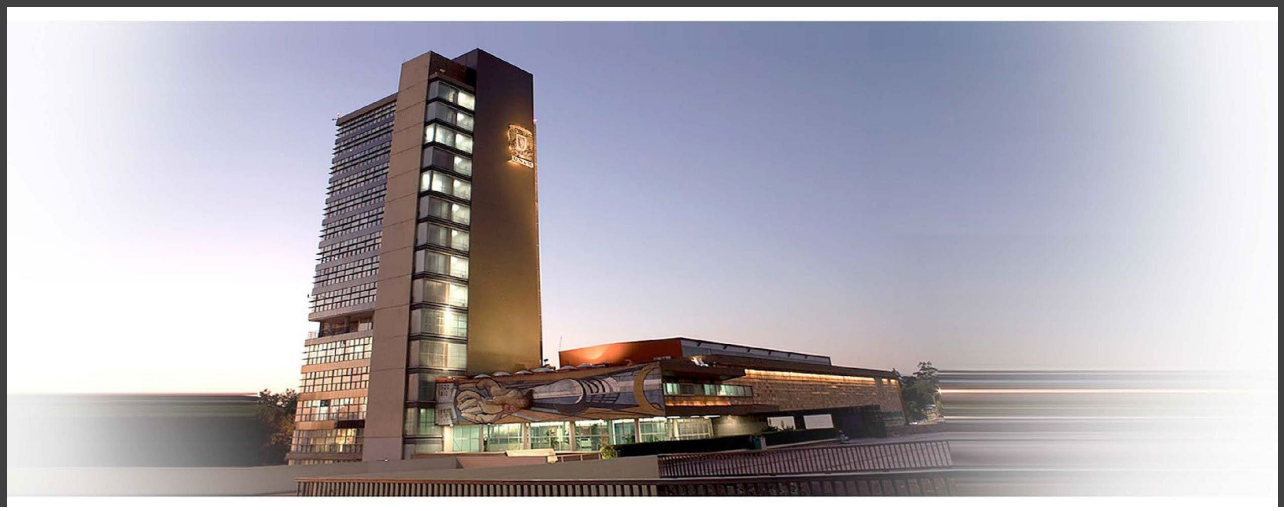
Universidad Nacional Autónoma de México



Universidad Nacional Autónoma de México

ANEXOS DE LAS NORMAS COMPLEMENTARIAS SOBRE MEDIDAS DE SEGURIDAD TÉCNICAS, ADMINISTRATIVAS Y FÍSICAS PARA LA PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE LA UNIVERSIDAD

ANEXO I: DOCUMENTO DE SEGURIDAD DE DATOS PERSONALES

ÍNDICE

Introducción

El presente documento de seguridad contiene las medidas de seguridad administrativa, física y técnica aplicables a los sistemas de tratamiento de datos personales de la esta área universitaria con el fin de asegurar la integridad, confidencialidad y disponibilidad de la información personal que éstos contienen.

Su propósito es identificar los sistemas de tratamiento de datos personales que posee esta área universitaria, el tipo de datos personales que contiene cada uno, los responsables, encargados, usuarios de cada sistema y las medidas de seguridad concretas implementadas.

Este modelo pretende brindar a las áreas universitarias homogeneidad en la redacción, organización y contenido para que elaboren su propio documento de seguridad en el que se describan las tres medidas de seguridad para la protección de los datos personales.

El marco jurídico del documento de seguridad se regula por el capítulo II de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, publicada el 26 de enero de 2017, que establece un conjunto mínimo de medidas de seguridad que cada dependencia o entidad universitaria deberá considerar al perfilar su estrategia de seguridad para la protección de los datos personales bajo su custodia, según el tipo de soportes —físicos, electrónicos o ambos— en los que residen dichos datos y dependiendo del nivel de protección que tales datos requieran.

Específicamente los artículos 31, 32 y 33 de la Ley General, del 55 al 72 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público, publicados en el Diario Oficial de la Federación el 26 de enero de 2018, así como del 20 al 31 de los Lineamientos para la protección de datos personales en posesión de la Universidad Nacional Autónoma de México, publicados en la Gaceta UNAM el 25 de febrero de 2019.

El cimiento del formato de documento de seguridad es la aplicación de un enfoque basado en los riesgos de los activos universitarios, específicamente los datos personales y los soportes que los resguardan. Además, el formato considera el tamaño y estructura de la institución, objetivos, clasificación de la información, requerimientos de seguridad y procesos que se precisan en razón de los activos que posee esta Máxima Casa de Estudios, lo cual se encuentran contemplado en el estándar internacional en materia de seguridad de la información ISO/IEC 27002:2013 "*Tecnología de la información - Técnicas de seguridad - Código de práctica para los controles de seguridad de la información".*

ÍNDICE

UNAM

CHICAGO

I. SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES A1. ADMINISTRACIÓN GENERAL

1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

DELEGACIÓN ADMINISTRATIVA	
Identificador único*	**UNAM CHICAGO**
(Nombre del sistema A1.1) *	**UNAM-CHICAGO-CÁMARAS DE SEGURIDAD**
Datos personales (sensibles o no) contenidos en el sistema*:	Imagen de las personas que ingresan y transitan a las instalaciones
Responsable/Encargado/Usuario	
Nombre*:	C.P. Mireya de Guadalupe Navarro González
Cargo*:	Delegada Administrativa
Funciones*:	Administrar el equipo. .
Obligaciones*:	No difundir información de los datos personales. No modificar la información almacenada en el servidor. Salvaguardar la información en el servidor. .
	Encargados / Usuario
(Nombre del Encargado 1*)	Ing. Ernesto González
Cargo*:	Ingeniero de Sistemas
Funciones*:	Mantener la seguridad de la información. Administrar los recursos del sistema.
Obligaciones*:	Mantener la confidencialidad de la información. Mantener operativo el sistema. No difundir información de los datos personales. No modificar la información almacenada en el servidor. No hacer respaldos en equipo personal de la información de datos personales.

Sistema (Nombre del A1.2)*:	**UNAM CHICAGO- PUMA (SERVIDOR)**
Datos personales contenidos en el sistema*:	1. Datos personales en general: Nombre, domicilio, teléfono celular, número de seguro social, estado civil, firma, lugar y fecha de nacimiento, nacionalidad, edad, nombre de beneficiarios, y su número de seguro social, documentos de reclutamiento, y selección de puesto, de incidencias, de capacitación, correo electrónico institucional, teléfono institucional, constancia de percepciones y retenciones, título, cédula profesional, certificados, reconocimientos, información migratoria. 2. Datos personales sensibles: Alergias, enfermedades, intervenciones quirúrgicas.
	Responsable:
Nombre*:	C.P. Mireya de Guadalupe Navarro González
Cargo*:	Delegada Administrativa
Funciones*:	Coordinar los servicios de mantenimiento del servidor para que esté operativo los 365 días del año.
Obligaciones*:	Mantener la confidencialidad de la documentación e información almacenada en el servidor. No difundir la información. No alterar los documentos.
	Encargados:
(Nombre del Encargado 1*)	Ing. Ernesto González
Cargo*:	Sistemas
Funciones*:	Mantener la seguridad de la información. Administrar los recursos del sistema. Hacer los respaldos de la información diariamente.
Obligaciones*:	Mantener la confidencialidad de la información. Mantener operativo el sistema. Hacer las actualizaciones cuando se requieran.
	Usuarios:
(Nombre del Usuario 1*)	Mtra. Claudia Rosa María Muñoz Cano
Cargo*:	Coordinadora de la Enseñanza del español y la cultura
Funciones*:	Compartir archivos y trabajar en red con otros profesores.
Obligaciones*:	Mantener la confidencialidad de la información almacenada en el servidor. No difundir la información. No alterar los documentos. No cambiar la configuración de los sistemas. No descargar la información o documentos de fuentes desconocidas.

(Nombre del Usuario 2*)	Mtra. Adriana Peguero Ceja
Cargo*:	Maestra de español
Funciones*:	Compartir archivos y trabajar en red con otros profesores.
Obligaciones*:	Mantener la confidencialidad de la información almacenada en el servidor. No difundir la información. No alterar los documentos. No cambiar la configuración de los sistemas. No descargar la información o documentos de fuentes desconocidas.
(Nombre del Usuario 3*)	Mtra. Carmen Martínez
Cargo*:	Maestra de español
Funciones*:	Compartir archivos y trabajar en red con otros profesores.
Obligaciones*:	Mantener la confidencialidad de la información almacenada en el servidor. No difundir la información. No alterar los documentos. No cambiar la configuración de los sistemas. No descargar la información o documentos de fuentes desconocidas.

(Nombre del sistema A1.3) *	**UNAM CHICAGO-EXPEDIENTES DE PERSONAL**
Datos personales (sensibles o no) contenidos en el sistema*:	1. Datos personales en general: Nombre, domicilio, teléfono celular, número de seguro social, estado civil, firma, lugar y fecha de nacimiento, nacionalidad, edad, nombre de beneficiarios y su número de seguro social, documentos de reclutamiento y selección de puesto, de incidencias, de capacitación, correo electrónico institucional, teléfono institucional, constancia de percepciones y retenciones, título, cédula profesional, certificados, reconocimientos, información migratoria. 2. Datos personales sensibles: Alergias, enfermedades, intervenciones quirúrgicas.
Responsable/ Encargado/Usuario	
Nombre*:	C.P. Mireya de Guadalupe Navarro González
Cargo*:	Delegada Administrativa
Funciones*:	Solicitar la información necesaria a quienes están siendo reclutados y a los empleados cuando la situación lo amerite. Supervisar el correcto llenado de los formatos de reclutamiento, incidencias, etc.
Obligaciones*:	Mantener la confidencialidad de la documentación e información recibida.

	No difundir la información. No alterar los documentos. Mantener todos los documentos a salvaguardo en el lugar designado para ese objetivo y bajo llave.

2. ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

DELEGACIÓN ADMINISTRATIVA	
Identificador único¨*	**UNAM CHICAGO**
(Nombre del sistema A1.1*)	**UNAM CHICAGO-CÁMARAS**
Tipo de soporte:*	Soporte físico
Descripción:*	El sistema posee un DVR (Digital Video Recorder), donde se almacenan las grabaciones hasta por un mes, dichas imágenes son obtenidas por las cámaras IP colocadas en el exterior y en el interior en cada piso del inmueble.
Características del lugar donde se resguardan los soportes:*	Se aloja en discos duros internos. Se encuentra dentro de un arnés para servidor con chapa y llave, dentro de un clóset con aire acondicionado, puerta de madera con chapa y llave
(Nombre del sistema A1.2*)	**UNAM CHICAGO- PUMA (SERVIDOR)**
Tipo de soporte*:	Técnico: Hardware y Software.
Descripción*:	Servidor de archivos y respaldos.
Características del lugar donde se resguardan los soportes*:	Se aloja en discos duros internos y externos. Se encuentra dentro de un arnés para servidor con chapa y llave; dentro de un clóset con aire acondicionado, puerta de madera con chapa y llave.
(Nombre del sistema A1.3*)	**UNAM CHICAGO-EXPEDIENTES DE PERSONAL**
Tipo de soporte*:	Físico
Descripción*:	Se cuenta con expedientes para cada empleado.
Características del lugar donde se resguardan los soportes*:	Se encuentran resguardados en un archivero de metal, con chapa y llave, en un área de la oficina de la Delegación Administrativa protegida por una cortina de acrílico que oculta el archivero. Dicha oficina tiene puerta de madera con chapa con acceso de huella digital.

3. ANÁLISIS DE RIESGOS

DELEGACIÓN ADMINISTRATIVA		
Identificador único*	**UNAM CHICAGO**	
(Nombre del sistema A1.1) *	**UNAM CHICAGO-CÁMARAS**	
Riesgo*	**Impacto***	**Mitigación***
Acceso no autorizado al sistema por un hacker. Catástrofe natural (una descarga eléctrica por un rayo). Vandalismo de las cámaras externas. Falla del DVR que no grabe.	Robo y/o eliminación de la información. Pérdida total de la información y del equipo. Pérdida total de la información. Pérdida total de la información.	Restablecer el sistema con un equipo nuevo.
(Nombre del sistema A1.2) *	**UNAM CHICAGO-PUMA (SERVIDOR)**	
Riesgo	**Impacto**	**Mitigación**
Acceso no autorizado al sistema por un hacker. Catástrofe natural (una descarga eléctrica por un rayo).	ALTO. Robo y/o modificación de la información. Pérdida total de la información y del equipo.	Restablecer un equipo nuevo y con los respaldos externos.
(Nombre del sistema A1.3) *	**UNAM CHICAGO-EXPEDIENTES DE PERSONAL**	
Riesgo	**Impacto**	**Mitigación**
Acceso no autorizado a la oficina de la Delegación Administrativa	BAJO. Robo, modificación y/o destrucción de los expedientes.	Reemplazar la cortina de acrílico por una puerta con chapa y llave.

4. ANÁLISIS DE BRECHA

DELEGACIÓN ADMINISTRATIVA		
Identificador único*	**UNAM CHICAGO**	
(Nombre del sistema A1.1) *	**UNAM CHICAGO-CÁMARAS**	
Medida de seguridad actual*	**Medida de seguridad necesaria***	**Acciones para remediación***
Contamos con credenciales de cada usuario para el acceso al DVR.	Respaldar los videos grabados en una nube.	*Reemplazo del equipo*
(Nombre del sistema A1.2) *	**UNAM CHICAGO-PUMA (SERVIDOR)**	
Medida de seguridad actual*	**Medida de seguridad necesaria***	**Acciones para remediación***
Contamos con un directorio activo que solicita las credenciales de cada usuario para el acceso al servidor. Contamos con una VPN (red virtual privada), para encriptar cualquier acceso remoto al servidor, con una configuración de Firewall.	Instalar un nuevo servidor espejo.	Adquirir un nuevo servidor. Instalar los programas y configuraciones de red. Restaurar los datos de los respaldos externos.
(Nombre del sistema A1.3) *	**UNAM CHICAGO-EXPEDIENTES DE PERSONAL**	
Medida de seguridad actual*	**Medida de seguridad necesaria***	**Acciones para remediación***
Se encuentran resguardados bajo llave y en una oficina que tiene acceso por medio de huella digital y sólo el responsable tiene acceso a esa oficina.	Tener un respaldo digital de los mismos.	Digitalizar los documentos y resguardarlos correctamente.

5. PLAN DE TRABAJO

DELEGACIÓN ADMINISTRATIVA			
Identificador único*	**UNAM CHICAGO**		
(Nombre del sistema A1.1) *	**UNAM CHICAGO-CÁMARAS**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Reemplazar el DVR	Instalación física del equipo. Configuración de red.	De una semana. (en la adquisición del equipo e instalación).	Iniciar de nuevo las grabaciones.
(Nombre del sistema A1.2) *	**UNAM CHICAGO-PUMA (SERVIDOR)**		
Actividad	**Descripción**	**Duración**	**Cobertura**
Restaurar el servidor con la información que fuera rescatable.	Instalación física del equipo. Configuración de red. Instalación de seguridad y antivirus. Pasar el periodo de pruebas de los sistemas.	De una a dos semanas.	El correo electrónico es de recuperación inmediata y total. Recuperación inmediata y total de los Programas de Office y Antivirus. (tenemos discos de instalación y licencias).
(Nombre del sistema A1.3) *			
Actividad	**Descripción**	**Duración**	**Cobertura**

6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

I. TRANSFERENCIAS DE DATOS PERSONALES

DELEGACIÓN ADMINISTRATIVA	
Identificador único*	**UNAM CHICAGO**
(Nombre del sistema A1.1)*	**UNAM CHICAGO - CAMARAS**
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	No aplica ya que las consultas son internas y de uso exclusivo de la Escuela y no se comparte la información con otras sedes.
Transferencias mediante el traslado de soportes electrónicos:	No aplica ya que las consultas son internas y de uso exclusivo de la Escuela y no se comparte la información con otras sedes.
Transferencias mediante el traslado sobre redes electrónicas:	No aplica ya que las consultas son internas y de uso exclusivo de la Escuela y no se comparte la información con otras sedes.
(Nombre del sistema A1.2)	**UNAM CHICAGO-PUMA (SERVIDOR)**
Transferencias mediante el traslado de soportes físicos:	No aplica ya que las consultas son internas y de uso exclusivo de la Escuela y no se comparte la información con otras sedes.
Transferencias mediante el traslado de soportes electrónicos:	No aplica ya que las consultas son internas y de uso exclusivo de la Escuela y no se comparte la información con otras sedes.
Transferencias mediante el traslado sobre redes electrónicas	No aplica ya que las consultas son internas y de uso exclusivo de la Escuela y no se comparte la información con otras sedes.
(Nombre del sistema A1.3)	**UNAM CHICAGO-EXPEDIENTES DE PERSONAL**
Transferencias mediante el traslado de soportes físicos:	Dado el caso, se envían por paquetería especializada (UPS, FEDEX, DHL) con destinatario primario y secundario con solicitud de firma de recibido y de identificación del destinatario con documento de identificación oficial. En caso de no encontrarse los destinatarios se solicita que se regrese al remitente.
Transferencias mediante el traslado de soportes electrónicos:	No aplica porque no los manejamos.
Transferencias mediante el traslado sobre redes electrónicas:	No aplica.

I. **RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS**

(Nombre del sistema A1.1) *	**UNAM CHICAGO-CÁMARAS**

1. Señalar las medidas de seguridad que ha implementado el área universitaria para el resguardo de los soportes físicos del sistema de manera que evite la alteración, pérdida o acceso no autorizado a los mismos.
No aplica.
2. Señalar en un listado las personas (nombre, cargo, funciones y obligaciones) que tienen acceso a los soportes físicos del sistema.
No aplica.

(Nombre del sistema A1.2)	**UNAM CHICAGO-PUMA (SERVIDOR)**

1. Señalar las medidas de seguridad que ha implementado el área universitaria para el resguardo de los soportes físicos del sistema de manera que evite la alteración, pérdida o acceso no autorizado.
Se basa en una plataforma de Windows con un directorio de acceso con credencialización de usuario y computadoras.
2. Señalar en un listado las personas (nombre, cargo, funciones y obligaciones) que tienen acceso a los soportes físicos del sistema.
Mireya Navarro González
Responsable de administrar el equipo.
No difundir la información de los datos personales.
No modificar la información almacenada en el servidor.
Salvaguardar la información almacenada en el servidor.

(Nombre del sistema A1.3)	**UNAM CHICAGO-EXPEDIENTES DE PERSONAL**

1. Señalar las medidas de seguridad que ha implementado el área universitaria para el resguardo de los soportes físicos del sistema de manera que evite la alteración, pérdida o acceso no autorizado.
Los expedientes se encuentran salvaguardados en un archivero bajo llave en la oficina de la Delegación Administrativa, cuyo acceso es mediante reconocimiento de huella digital y sólo la responsable tiene registrada la huella.
2. Señalar en un listado las personas (nombre, cargo, funciones y obligaciones) que tienen acceso a los soportes físicos del sistema. **Responsable: Mireya Navarro González. Delegada Administrativa.**

II. **BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA**

Sistema 1.1-UNAM CHICAGO-CÁMARAS

1. **Los datos que se registran en las bitácoras:**
   - **a)** Quién accede a los datos personales.
   - **b)** No se cuenta con una bitácora para estos propósitos. La única persona que accede a esa información es la responsable del sistema: Mireya Navarro González.
   - **c)** Para soportes físicos: La única bitácora que se tiene es sobre los mantenimientos y las actualizaciones y esa información está contenida en el sistema.
   - **d)** Para soportes electrónicos: Lo mismo que la anterior.

1. Si las bitácoras están en soporte físico o en soporte electrónico;
El DVR tiene su sistema de logs que se almacenan en el mismo equipo.

2. Lugar dónde almacena las bitácoras y por cuánto tiempo;
En el mismo DVR, hasta que se limpian cada mes.

3. La manera en que asegura la integridad de las bitácoras, y
El sistema no permite la alteración de los logs.

4. Respecto del análisis de las bitácoras:
No contamos con esa información.

Sistema 1. 2-UNAM CHICAGO-PUMA (SERVIDOR)

1.Los datos que se registran en las bitácoras:

a) Quién accede a los datos personales.

El acceso está basado en una plataforma de Windows con un directorio de acceso con credencialización de usuarios y computadoras.

a) Para soportes físicos: La única bitácora que se tiene es sobre los mantenimientos y las actualizaciones y esa información está contenida en el sistema.

b) Para soportes electrónicos: Lo mismo que la anterior.

2. Si las bitácoras están en soporte físico o en soporte electrónico;

Físico

3. Lugar dónde almacena las bitácoras y por cuánto tiempo;
En el mismo sistema.
4. La manera en que asegura la integridad de las bitácoras, y
El sistema no permite la alteración de los entradas.
5. Respecto del análisis de las bitácoras:
No contamos con esa información

Sistema 1. 3-UNAM CHICAGO-EXPEDIENTES DE PERSONAL

No contamos con bitácoras ya que el traslado, movimiento o consulta lo realiza solamente la responsable del sistema.

III. REGISTRO DE INCIDENTES:

Describir el procedimiento de atención de incidentes que tiene implementado el área universitaria y especificar si lleva registro de los incidentes relativos a soportes físicos, como lo son la pérdida o alteración no autorizada de expedientes, y para el caso de soportes electrónicos, ofrecer detalles sobre el registro de incidentes en el cual consigne los procedimientos realizados para la recuperación de los datos o para permitir la disponibilidad del proceso.

Sistema 1.1-UNAM CHICAGO-CÁMARAS

No contamos con registro de incidentes.

Sistema 1.2-UNAM CHICAGO-PUMA (SERVIDOR)

No contamos con registro de incidentes.

1. Los datos que registra:

a) La persona que resolvió el incidente;
b) La metodología aplicada;
c) Para soportes físicos: Los oficios, documentos, expedientes, estantes o archiveros, tanto los dañados como los recuperados, y
d) Para soportes electrónicos: Los campos, registros, tablas, bases de datos o archivos electrónicos, tanto dañados como recuperados, el nombre de los sistemas y la infraestructura afectada, indicar si el incidente afectó el servidor principal y los servidores de respaldo, etc.

2. Si el registro está en soporte físico o en soporte electrónico;
3. Cómo asegura la integridad de dicho registro, y
4. Para el caso de soportes electrónicos, quién autoriza la recuperación de datos.
5.

Sistema 1.3-UNAM CHICAGO-EXPEDIENTES DE PERSONAL

No contamos con registro de incidentes ya que no se han presentado.

V. ACCESO A LAS INSTALACIONES

1. Seguridad perimetral exterior (las instalaciones del área universitaria): **UNAM CHICAGO**

a) Se cuenta con un sistema de cámaras instaladas alrededor del edificio (puerta de entrada al edificio, entrada del área de carga y descarga en la parte de atrás del edificio, callejones laterales del inmueble). Se cuenta con un sistema de interfón para dar acceso solamente a las personas que tengan algún asunto relativo a la institución. En caso afirmativo se les da la entrada, en caso contrario no se da acceso. **Los empleados cuentan con una clave de acceso al edificio.**

2. Seguridad perimetral interior (oficina, almacén o bodega para soportes físicos, centro de datos para soportes electrónicos):

Se tienen cámaras instaladas en la entrada a la Escuela, en los pasillos de las oficinas administrativas, en el lobby, en el pasillo que lleva a los sanitarios, cocina, Galería 2, en las dos Galerías, en las escaleras que van al sótano, en el pasillo de las aulas. La información se almacena en el DVR máximo por un mes.
El sistema de cámaras se encuentra resguardado en un clóset localizado en el primer piso, con puerta de madera, chapa y llave. Las llaves de ese clóset se encuentran en un llavín con clave de acceso para abrirlo, en la oficina de la Delegación Administrativa y sólo la Delegada tiene acceso a ese llavín.
Las puertas de acceso a la Escuela y CIERTAS Áreas restringidas cuentan con dos chapas y llaves de seguridad. También, se cuenta con un sistema de alarma y solamente las personas autorizadas para abrir y cerrar la Escuela tienen llave de acceso y clave de alarma.
El tratamiento que se la da a los datos personales captados por las cámaras ya fue explicado en otra sección de este cuestionario.

VI. ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

Las medidas de seguridad previstas a continuación en los incisos VII al IX, sólo aplican para soportes electrónicos

VI. PERFILES DE USUARIO Y CONTRASEÑAS

Sistema 1.1-UNAM CHICAGO-CÁMARAS

1. Modelo de control de acceso (alguno de los siguientes):

a) ¿Es obligatorio (etiquetas para objetos y acreditación para sujetos)?
b) ¿Es discrecional (matriz de control de acceso)?
c) ¿Está basado en roles (perfiles) o grupos?
d) ¿Está basado en reglas?

No aplica ya que son grabaciones por cada piso del inmueble y por cada área de la Escuela.

2. Perfiles de usuario y contraseñas en el sistema operativo de red:

a) ¿Cuenta con un sistema operativo de red instalado en sus equipos?
b) ¿Proporciona dicho sistema operativo un manejo riguroso de perfiles de usuario y contraseñas?
c) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?

No aplica ya que son grabaciones por cada piso del inmueble y por cada área de la Escuela.

3. Perfiles de usuario y contraseñas manejados por el software aplicativo del sistema de tratamiento de datos personales:

a) ¿Ofrece dicho software un manejo riguroso de perfiles de usuario y contraseñas?
b) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?

No aplica ya que son grabaciones por cada piso del inmueble y por cada área de la Escuela.

4. Administración de perfiles de usuario y contraseñas:

a) ¿Quién da de alta nuevos perfiles?
b) ¿Quién autoriza la creación de nuevos perfiles?
c) ¿Se lleva registro de la creación de nuevos perfiles?

No aplica ya que son grabaciones por cada piso del inmueble y por cada área de la Escuela.

5. Acceso remoto al sistema de tratamiento de datos personales:

a) ¿Requieren los usuarios acceso remoto al equipo de cómputo que por lo general utilizan para trabajar con el sistema?
b) ¿Requiere el administrador acceso remoto al equipo donde reside el sistema para realizar tareas de mantenimiento?
c) ¿Cómo se evita el acceso remoto no autorizado?

No aplica ya que son grabaciones por cada piso del inmueble y por cada área de la Escuela.

Sistema 1.2-UNAM CHICAGO-PUMA (SERVIDOR)

1. Modelo de control de acceso:

Es por departamentos o grupos.

2. Perfiles de usuario y contraseñas en el sistema operativo de red

Es un sistema operativo de red. Todas las funciones son nativas del mismo.

3. Perfiles de usuario y contraseñas manejados por el software aplicativo del sistema de tratamiento de datos personales:

El software es instalado en un ambiente de red y solicita la credencialización de cada usuario.

4. Administración de perfiles de usuario y contraseñas:

El administrador de la red autoriza y tiene registro de nuevos perfiles.

5. Acceso remoto al sistema de tratamiento de datos personales:

El administrador de la red tiene implementado el VPN y tiene acceso remoto para solucionar problemas a distancia.

Se cuenta con un software para el acceso remoto encriptado.

Sistema 1.3-UNAM CHICAGO-EXPEDIENTES DE PERSONAL

1. Modelo de control de acceso:

Se necesita la llave del archivero para poder acceder a los expedientes. Y la llave la salvaguarda la responsable/encargada/usuaria.

2. Perfiles de usuario y contraseñas en el sistema operativo de red

No aplica.

3. Perfiles de usuario y contraseñas manejados por el software aplicativo del sistema de tratamiento de datos personales:

No aplica.

4. Administración de perfiles de usuario y contraseñas:

El administrador es el responsable/encargado/usuario. Son físicos.

5. Acceso remoto al sistema de tratamiento de datos personales:

No aplica

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

NO SE CUENTA CON RESPALDOS

3. **Cómo y dónde archiva esos medios, y**

NO APLICA

4. **Quién es el responsable de realizar estas operaciones (el área universitaria o un tercero).**

NO APLICA

Sistema 1.2-UNAM CHICAGO-PUMA (SERVIDOR)

1. **Señalar si realiza respaldos**

a) Completos_X_, diferenciales ___ o incrementales___;
b) De forma automática __X__ o Manual _____,
c) Periodicidad con que los realiza: ___DIARIO____

2. **El tipo de medios (por ejemplo: cintas magnéticas, discos duros, CD-ROM, entre otros) que utiliza para almacenar las copias de seguridad;[1]**

DISCOS DUROS

3. **Cómo y dónde archiva esos medios, y**

EN EL MISMO SERVIDOR EN DISCOS OCULTOS

4. **Quién es el responsable de realizar estas operaciones (el área universitaria o un tercero).**

UN TERCERO

Sistema 1.3-UNAM CHICAGO-EXPEDIENTES DE PERSONAL

1. **Señalar si realiza respaldos**

NO SE REALIZAN RESPALDOS

2. **El tipo de medios (por ejemplo: cintas magnéticas, discos duros, CD-ROM, entre otros) que utiliza para almacenar las copias de seguridad;**

N/A

1. **Cómo y dónde archiva esos medios, y**

N/A

4. **Quién es el responsable de realizar estas operaciones (el área universitaria o un tercero).**

N/A

IX. PLAN DE CONTINGENCIA

Sistema 1.1-UNAM CHICAGO-CÁMARAS

1. **Presentar el plan de contingencia con el cual garantiza la continuidad de la operación del sistema o informar si no lo tiene, pero se encuentra desarrollándolo.**

NO CONTAMOS CON UN PLAN Y NO SE HA DESARROLLADO.

2. **Si cuenta con plan de contingencia y lo ha implementado, deberá indicar si realiza pruebas de eficiencia de este.**

NO APLICA

3. Informar si cuenta con un sitio redundante (alterno) y señalar lo siguiente:

a) El tipo de sitio (caliente, tibio o frío);
b) Si el sitio es propio o subcontratado con un tercero;
c) Los procedimientos, el equipo y el personal que designa para poner en marcha tal sitio y
d) Tiempo que le lleva poner en marcha el sitio, según las pruebas de eficiencia.

NO APLICA

Sistema 1.2-UNAM CHICAGO-PUMA (SERVIDOR)

Presentar el plan de contingencia con el cual garantiza la continuidad de la operación del sistema o informar si no lo tiene, pero se encuentra desarrollándolo.

PLAN DE CONTINGENCIA: EN CASO DE DAÑO DEL SERVIDOR, REEMPLAZARLO POR UNO NUEVO Y RESTAURAR LOS RESPALDOS EN EL NUEVO SERVIDOR.

2. Si cuenta con plan de contingencia y lo ha implementado, deberá indicar si realiza pruebas de eficiencia de este.

NO HA HABIDO CONTINGENCIA POR LO TANTO NO SE HA APLICADO DICHO PLAN.

3. Informar si cuenta con un sitio redundante (alterno) y señalar lo siguiente:

NO APLICA

a) El tipo de sitio (caliente, tibio o frío);
b) Si el sitio es propio o subcontratado con un tercero;
c) Los procedimientos, el equipo y el personal que designa para poner en marcha tal sitio y
d) Tiempo que le lleva poner en marcha el sitio, según las pruebas de eficiencia.

Sistema 1.3-UNAM CHICAGO-EXPEDIENTES DE PERSONAL

Presentar el plan de contingencia con el cual garantiza la continuidad de la operación del sistema o informar si no lo tiene, pero se encuentra desarrollándolo.

NO SE CUENTA CON UN PLAN DE CONTINGENCIA.

2. Si cuenta con plan de contingencia y lo ha implementado, deberá indicar si realiza pruebas de eficiencia de este.

NO APLICA

3. **Informar si cuenta con un sitio redundante (alterno) y señalar lo siguiente:**

a) El tipo de sitio (caliente, tibio o frío);
b) Si el sitio es propio o subcontratado con un tercero;
c) Los procedimientos, el equipo y el personal que designa para poner en marcha tal sitio y
d) Tiempo que le lleva poner en marcha el sitio, según las pruebas de eficiencia.

NO APLICA

MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

7.1. Herramientas y recursos para monitoreo de la protección de datos personales

DELEGACIÓN ADMINISTRATIVA		
Identificador único*	**UNAM CHICAGO**	
(Nombre del sistema A1.1)*	**UNAM-CHICAGO-CÁMARAS**	
Recurso*	**Descripción***	**Control***
CÁMARAS DE ALTA DEFINICIÓN	**REVISIONES ALEATORIAS**	**SE VERIFICA EN UN MONITOR Y SE HACE SEMANALMENTE.** **NO SE NECESITA LICENCIA** **ES UN TERCERO EL RESPONSABLE.**

7.1. Herramientas y recursos para monitoreo de la protección de datos personales

DELEGACIÓN ADMINISTRATIVA		
Identificador único*	**UNAM CHICAGO**	
(Nombre del sistema A1.2)*	**UNAM CHICAGO-PUMA (SERVIDOR)**	
Recurso*	**Descripción***	**Control***
EL ACCESO REMOTO. UN SOFTWARE DE ALERTAS	**REVISIÓN ALEATORIA PERO EL SOFTWARE DE ALERTAS MONITOREA 24/7 .**	**ACCESO REMOTO Y LA LICENCIA ES ANUAL.** **ES UN TERCERO EL RESPONSABLE.**

7.1. Herramientas y recursos para monitoreo de la protección de datos personales

DELEGACIÓN ADMINISTRATIVA		
Identificador único*	**UNAM CHICAGO**	
(Nombre del sistema A1.3)*	**UNAM CHICAGO-EXPEDIENTE DE PERSONAL**	
Recurso*	**Descripción***	**Control***
VERIFICACIÓN FÍSICA	**PRUEBAS ALEATORIAS.**	**SE ENCUENTRAN SALVAGUARDADOS EN UN ARCHIVERO CON CERRADURA.** **LA ADMINISTRADORA ES LA RESPONSABLE.**

7.2. Procedimiento para la revisión de las medidas de seguridad

DELEGACIÓN ADMINISTRATIVA		
Identificador único*	**UNAM CHICAGO**	
(Nombre del sistema A1.1)*	**UNAM-CHICAGO-CÁMARAS**	
Medida de seguridad*	**Procedimiento***	**Responsable***
EL EQUIPO ESTÁ RESGUARDADO BAJO LLAVE EN UN CLÓSET CON CERRADURA Y TIENE CLAVE DE ACCESO	**COMPROBACIÓN DE ACTUALIZACIÓN Y MONITOREO VISUAL DE LAS MISMAS.**	**Indicar:** **a) ING. ERNESTO GONZÁLEZ** **b) UN DÍA**

7.2. Procedimiento para la revisión de las medidas de seguridad

DELEGACIÓN ADMINISTRATIVA		
Identificador único*	**UNAM CHICAGO**	
(Nombre del sistema A1.2)*	**UNAM CHICAGO-PUMA (SERVIDOR)**	
Medida de seguridad*	**Procedimiento***	**Responsable***
EL EQUIPO ESTÁ RESGUARDADO BAJO LLAVE EN UN CLÓSET CON CERRADURA Y TIENE CLAVE DE ACCESO	**COMPROBACIÓN DE ACTUALIZACIÓN Y EL SISTEMA DE ALERTAS ENVÍA CORREOS ELECTRÓNICOS CUANDO EL SISTEMA: ESTÁ ABAJO, LENTO, NECESITA ACTUALIZACIONES.**	***Indicar:*** ***a)*** **ING. ERNESTO GONZÁLEZ** ***b)*** **UN DÍA**

7.2. Procedimiento para la revisión de las medidas de seguridad

DELEGACIÓN ADMINISTRATIVA		
Identificador único*	**UNAM CHICAGO**	
(Nombre del sistema A1.3)*	**UNAM CHICAGO-EXPEDIENTE DE PERSONAL**	
Medida de seguridad*	**Procedimiento***	**Responsable***
MANTENER LA LLAVE DEL ARCHIVERO DONDE SE SALVAGUARDAN LOS EXPEDIENTES EN UN CAJÓN CON CERRADURA	***REVISAR QUE EL ARCHIVERO SE ENCUENTRE CERRADO CON LLAVE Y LA LLAVE ESTÉ TAMBIÉN EN EL CAJÓN CON CERRADURA.***	***Indicar:*** ***a)*** **C.P. MIREYA DE GPE. NAVARRO GONZÁLEZ** ***b)*** **MENOS DE UN DÍA**

7.3. Resultados de la evaluación y pruebas a las medidas de seguridad

DELEGACIÓN ADMINISTRATIVA		
Identificador único*	**UNAM CHICAGO**	
(Nombre del sistema A1.1)*	**UNAM-CHICAGO-CÁMARAS**	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***
REVISAR ALEATORIAMENTE GRABACIONES	***LA CERTIFICACIÓN DEL FUNCIONAMIENTO CORRECTO DEL SISTEMA***	***Indicar:*** ***a)*** **ING. ERNESTO GONZÁLEZ** ***b)*** **UN DÍA*a)* ING. ERNESTO GONZÁLEZ** ***b)*** **UN DÍA**

DELEGACIÓN ADMINISTRATIVA		
Identificador único*	**UNAM CHICAGO**	
(Nombre del sistema A1.2)*	**UNAM CHICAGO-PUMA (SERVIDOR)**	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***
EL SERVIDOR CUENTA CON HISTORIAL DE EVENTOS DONDE SE PUEDE VERIFICAR SI EXISTE ALGUNA FALLA Y TODOS LOS EVENTOS QUE HAN OCURRIDO.	***SE OBTIENE EL PORCENTAJE OPERATIVO DEL SERVIDOR.***	***Indicar:*** ***a)*** **ING. ERNESTO GONZÁLEZ** ***b)*** **UN DÍA**

DELEGACIÓN ADMINISTRATIVA		
Identificador único*	**UNAM CHICAGO**	
(Nombre del sistema A1.3)*	**UNAM CHICAGO-EXPEDIENTE DE PERSONAL**	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***
LA ENTRADA A LA OFICINA DONDE SE ENCUENTRAN LOS EXPEDIENTES ESTÁ RESTRINGIDA.	***SÓLO LA PERSONA AUTORIZADA TIENE ACCESO A ESA OFICINA.***	***a)* C.P. MIREYA DE GPE. NAVARRO GONZÁLEZ** ***b)* MENOS DE UN DÍA**

7.4. Acciones para la corrección y actualización de las medidas de seguridad

DELEGACIÓN ADMINISTRATIVA		
Identificador único*	**UNAM CHICAGO**	
(Nombre del sistema A1.1)*	**UNAM-CHICAGO-CÁMARAS**	
Medida de seguridad*	**Acciones***	**Responsable***
EN EL CASO DE DAÑOS, EL SISTEMA SE REEMPLAZARÍA YA SEA LAS CÁMARAS O EL SISTEMA DE VIDEO.	***Indique las acciones aplicables para corregir o actualizar la medida de seguridad.*** **a) REEMPLAZAR CÁMARAS O SISTEMA DE VIDEO.** **b) MANTENIMIENTO A LAS CÁMARAS Y AL SISTEMA DE VIDEO.**	***Indicar:*** ***a)* ING. ERNESTO GONZÁLEZ** ***b)* DOS DÍAS**

7.4. Acciones para la corrección y actualización de las medidas de seguridad

DELEGACIÓN ADMINISTRATIVA		
Identificador único*	**UNAM CHICAGO**	
(Nombre del sistema A1.2)*	**UNAM CHICAGO-PUMA (SERVIDOR)**	
Medida de seguridad*	**Acciones***	**Responsable***
EL SERVIDOR PERMITE FALLAS PARCIALES COMO DISCOS DUROS, MEMORIA Y FUENTE DE PODER.	***Indique las acciones aplicables para corregir o actualizar la medida de seguridad.*** **a) SE TIENE UN SISTEMA REDUNDANTE.** **b) LIMPIEZA Y MANTENIMIENTO.**	***Indicar:*** ***a)* ING. ERNESTO GONZÁLEZ** ***b)* DOS DÍAS**

7.4. Acciones para la corrección y actualización de las medidas de seguridad

DELEGACIÓN ADMINISTRATIVA		
Identificador único*	**UNAM CHICAGO**	
(Nombre del sistema A1.3)*	**UNAM CHICAGO-EXPEDIENTE DE PERSONAL**	
Medida de seguridad*	**Acciones***	**Responsable***
LA OFICINA DONDE SE ENCUENTRAN LOS EXPEDIENTES TIENE PUERTA CON CERRADURA Y SÓLO LA ADMINISTRADORA TIENE LLAVE.	***Indique las acciones aplicables para corregir o actualizar la medida de seguridad.*** **a) LOS EXPEDIENTES SE MANTIENEN EN EL ARCHIVERO BAJO LLAVE.** **b) MANTENER LA PUERTA CERRADA CON LLAVE CUANDO NO SE ENCUENTRE LA ADMINISTRADORA EN LA OFICINA**	***Indicar:*** ***a)* C.P. MIREYA DE GPE. NAVARRO GONZÁLEZ** ***b)* MENOS DE UN DÍA**

8. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

8.1. Programa de capacitación a los responsables de tratamiento de datos personales

DELEGACIÓN ADMINISTRATIVA			
Identificador único*	**UNAM CHICAGO**		
(Nombre del sistema A1.1)*	**UNAM-CHICAGO-CÁMARAS**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Taller	***Por Zoom***	***16/08/2022*** ***de 10 a 13 horas***	***Anual***

8.1. Programa de capacitación a los responsables de tratamiento de datos personales

DELEGACIÓN ADMINISTRATIVA			
Identificador único*	**UNAM CHICAGO**		
(Nombre del sistema A1.2)*	**UNAM CHICAGO-PUMA (SERVIDOR)**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Taller	***Por Zoom***	***16/08/2022*** ***de 10 a 13 horas***	***Anual***

8.1. Programa de capacitación a los responsables de tratamiento de datos personales

DELEGACIÓN ADMINISTRATIVA			
Identificador único*	**UNAM CHICAGO**		
(Nombre del sistema A1.3)*	**UNAM CHICAGO-EXPEDIENTE DE PERSONAL**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Taller	***Por Zoom***	***16/08/2022*** ***de 10 a 13 horas***	***Anual***

8.2. Programa de difusión de la protección a los datos personales

DELEGACIÓN ADMINISTRATIVA			
Identificador único*	**UNAM CHICAGO**		
(Nombre del sistema A1.1)* **(Nombre del sistema A1.2)*** **(Nombre del sistema A1.3)***	**UNAM-CHICAGO-CÁMARAS*** **UNAM CHICAGO-PUMA (SERVIDOR)** **UNAM CHICAGO-EXPEDIENTE DE PERSONAL**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Indique actividad, tema, recursos para la difusión. Agregar un renglón por cada elemento	***Describa el tipo de elemento, sus objetivos y forma de impartición, publicación o distribución***	***Indique duración del elemento en horas, días, meses, su fecha de inicio y de término***	***Mencione público objetivo, vigencia del elemento y frecuencia de actualización***

NO SE CUENTA CON UN PROGRAMA DE DIFUSIÓN DE LA PROTECCIÓN DE LOS DATOS PERSONALES.

9. MEJORA CONTINUA

9.1. Actualización y mantenimiento de sistemas de información

DELEGACIÓN ADMINISTRATIVA			
Identificador único*	**UNAM CHICAGO**		
(Nombre del sistema A1.1)* (Nombre del sistema A1.2)* (Nombre del sistema A1.3)*	**UNAM-CHICAGO-CÁMARAS* UNAM CHICAGO-PUMA (SERVIDOR) UNAM CHICAGO-EXPEDIENTE DE PERSONAL**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
.A1.1 CÁMARAS. SE ACTUALIZAN CADA 5 AÑOS. MANTTO. CADA AÑO. A1.2.SERVIDOR. SE ACTUALIZA LA MEMORIA Y LOS DISCOS DUROS CADA 2 AÑOS. Y MANTTO. ANUAL. A1.3 EXPEDIENTES..SE ACTUALIZAN POR LAS ALTAS, BAJAS Y CAMBIOS EN LOS DATOS PERSONALES DE LOS EMPLEADOS. MANTTO. CUANDO ES NECESARIO.	**A1.1.CÁMARAS. EL OBJETIVO ES PARA MANTENERLAS EN ESTADO OPERATIVO. A1.2.SERVIDOR. EL OBJETIVO ES PARA QUE SE PUEDA REPARAR EN CASO NECESARIO SIN INTERRUMPIR LA OPERACIÓN. A1.3.EXPEDIENTES. CONSERVAR EN BUEN ESTADO LOS DOCUMENTOS SALVAGUARDADOS.**	**A1.1.CÁMARAS. DURACIÓN UN DÍA. ANUAL. A.1.2. SERVIDOR DURACIÓN DOS DÍAS. ANUAL. A.1.3. EXPEDIENTES UN DÍA, CUANDO SE NECESITE.**	**A1.1.CÁMARAS. LA COMPATIBILIDAD ENTRE LAS CÁMARAS Y EL SISTEMA DE VIDEO. A.1.2 SERVIDOR. LA COMPATIBILIDAD DE LOS PROGRAMAS CON EL SERVIDOR. A.1.3. EXPEDIENTES. MANTENER EN ESTADO ÓPTIMO Y LEGIBLE TODOS LOS DOCUMENTOS RESGUARDADOS.**

9.2. Actualización y mantenimiento de equipo de cómputo

DELEGACIÓN ADMINISTRATIVA			
Identificador único*	**UNAM CHICAGO**		
(Nombre del sistema A1.1)* (Nombre del sistema A1.2)* (Nombre del sistema A1.3)*	**UNAM-CHICAGO-CÁMARAS* UNAM CHICAGO-PUMA (SERVIDOR) UNAM CHICAGO-EXPEDIENTE DE PERSONAL**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
A.1.1. CÁMARAS. **REVISIÓN DEL CABLEADO Y LA CAJA DE CONEXIONES.** **A.1.2. SERVIDOR** **LA REVISIÓN DE LAS FUENTES DE PODER, DE LA MEMORIA, DE LOS DISCOS DUROS Y EL SOFTWARE.** **A.1.3. EXPEDIENTES NO APLICA**	**A.1.1. CÁMARAS** **OBJETIVO MANTENER OPERATIVO EL SISTEMA DE GRABACIÓN Y REDUCIR LOS GASTOS DE REEMPLAZO DE EQUIPO.** **A.1.2.SERVIDOR** **OBJETIVO PRINCIPAL QUE PUEDAN TRABAJAR ININTERRUMPIDAMENTE LAS DIFERENTES ÁREAS.** **A.1.3. EXPEDIENTES** ***NO APLICA***	**A.1.1. CÁMARAS** **DURACIÓN: UN DÍA.** **A.1.2. SERVIDOR** **DURACIÓN: DOS DÍAS.** **A.1.3.EXPEDIENTES** **NO APLICA**	**A.1.1. CÁMARAS** **ASEGURAR QUE LAS CONEXIONES NO ESTÁN DETERIORADAS O DESGASTADAS POR EL CLIMA.** **A.1.2. SERVIDOR** **ASEGURAR QUE TODOS LOS COMPONENTES ESTÉN OPERATIVOS AL 100%.** **A.1.3.EXPEDIENTES** ***NO APLICA***

9.3. Procesos para la conservación, preservación y respaldos de información

DELEGACIÓN ADMINISTRATIVA		
Identificador único*	**UNAM CHICAGO**	
(Nombre del sistema A1.1)* (Nombre del sistema A1.2)* (Nombre del sistema A1.3)*	**UNAM-CHICAGO-CÁMARAS* UNAM CHICAGO-PUMA (SERVIDOR) UNAM CHICAGO-EXPEDIENTE DE PERSONAL**	
Proceso*	**Descripción***	**Responsable***
A.1.1. CÁMARAS ***GRABAR LA INFORMACIÓN EN UN DISCO DURO. NO SE CUENTA CON UN RESPALDO.*** ***A.1.2.SERVIDOR*** ***EL RESPALDO SE HACE EN UN DISCO DURO INTERNO Y EN OTRO EXTERNO.*** ***A.1.3.EXPEDIENTES*** ***NO APLICA***	***A.1.1. CÁMARAS*** ***SE GRABA EN UN DVR*** ***A.1.2. SERVIDOR*** ***SE HACE CON UN SOFTWARE DE RESPALDOS.*** ***A.1.3. EXPEDIENTES*** ***NO APLICA***	***A1.1.1 CÁMARAS Y A.1.2. SERVIDOR*** ***a) ING. ERNESTO GONZÁLEZ.*** ***b)* A.1.1 CÁMARAS- UN DÍA** **A.1.2. SERVIDOR DOS DÍAS** ***A.1.3.EXPEDIENTES*** ***NO APLICA***

9.4. Procesos de borrado seguro y disposición final de equipos y componentes informáticos

DELEGACIÓN ADMINISTRATIVA		
Identificador único*	**UNAM CHICAGO**	
(Nombre del sistema A1.1)* (Nombre del sistema A1.2)* (Nombre del sistema A1.3)*	**UNAM-CHICAGO-CÁMARAS* UNAM CHICAGO-PUMA (SERVIDOR) UNAM CHICAGO-EXPEDIENTE DE PERSONAL**	
Proceso*	**Descripción***	**Responsable***
A.1.1. CÁMARAS ***FORMATEO DE LOS DISCOS DUROS.*** ***A.1.2.SERVIDOR*** ***FORMATEO Y DESTRUCCIÓN DE LOS DISCOS DUROS.*** ***A.1.3.EXPEDIENTES*** ***SE TRITURAN***	***A.1.1. CÁMARAS*** ***CON UN SOFTWARE EN UNA COMPUTADORA*** ***A.1.2.SERVIDOR*** ***CON UN SOFTWARE EN UNA COMPUTADORA*** ***A.1.3.EXPEDIENTES*** ***SE UTILIZA UNA MÁQUINA TRITURADOR***	***Indicar:A.1.1. CÁMARAS Y*** ***A.1.2.SERVIDOR*** ***a) Nombre del responsable del proceso*** ***ING. ERNESTO GONZÁLEZ*** ***b) Tiempo máximo de ejecución en días*** ***DOS DÍAS*** ***A.1.3.EXPEDIENTES*** ***a) Nombre del responsable del proceso*** ***C.P. MIREYA DE GPE. NAVARRO GONZÁLEZ*** ***b) Tiempo máximo de ejecución en días*** ***DEPENDE DEL VOLUMEN DE DOCUMENTOS A TRITURAR.***

10. PROCEDIMIENTO PARA LA CANCELACIÓN DE UN SISTEMA DE TRATAMIENTO DE DATOS PERSONALES.

Sistema 1.1-UNAM CHICAGO-CÁMARAS

PROCEDIMIENTO:

1. LOS DATOS NO SE BORRAN SE SOBREESCRIBEN CADA TRES MESES AUTOMÁTICAMENTE.

Sistema 1.2-UNAM CHICAGO-PUMA (SERVIDOR)

PROCEDIMIENTO:

1. LA ELIMINACIÓN DE DATOS ES PERMANENTE E IRREVERSIBLE, CON LAS AUTORIZACIONES DEBIDAS Y NECESARIAS.

Sistema 1.3-UNAM CHICAGO-EXPEDIENTES DE PERSONAL

PROCEDIMIENTO:

1. AL MOMENTO DE QUE UNA PERSONA ES DADA DE BAJA POR RENUNCIA O DESPIDO, SU EXPEDIENTE ES REMOVIDO DE LOS ACTIVOS Y PASA AL ARCHIVO MUERTO.

A) DATOS DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES QUE SERÁ CANCELADO:

a) Denominación
b) Motivo de la cancelación

B) PLAZOS Y CONDICIONES PARA EL BLOQUEO DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES:[2]

C) MEDIDAS DE SEGURIDAD PARA EL BLOQUEO Y POSTERIOR SUPRESIÓN DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES:
NO APLICA

D) PROCEDIMIENTO PARA LA SUPRESIÓN DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

NO APLICA

E) MECANISMOS PARA LA SUPRESIÓN DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

NO APLICA

II. SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES A2. ADMINISTRACIÓN ESCOLAR

1. SISTEMA DE ADMINISTRACIÓN ESCOLAR

SECRETARÍA ACADÉMICA	
Identificador único*	**UNAM CHICAGO-ESCOLAR**
(Nombre del sistema A2) *	**Sistema de Administración Escolar**
Datos personales (sensibles o no) contenidos en el sistema*:	Nombre y Apellidos, correo electrónico, teléfono, género, fecha de nacimiento, país de nacimiento, máximo nivel de estudios.
Responsable:	Secretaría Académica
Nombre*:	Dra. Erika Erdely Ruiz
Cargo*:	Secretaria Académica
Funciones*:	Coadyuvar en el tratamiento automatizado de los datos personales, así como el contenido y uso del sistema.
Obligaciones*:	Supervisar que el sistema cumpla con las medidas para la protección de datos.
	Encargados:
(Nombre del Encargado 1*)	Mtra. Eréndira Sánchez Castañeda
Cargo*:	Coordinadora de Planeación y Desarrollo Institucional
Funciones*:	Asignar los permisos de acceso. Generar reportes de alumnos para la CRAI. Monitorear las bitácoras de acceso. Verificar que se hayan realizado los respaldos con el personal de informática de la CRAI.
Obligaciones*:	Proteger los datos personales de los alumnos y profesores. No modificar la información de datos personales. No difundir información de los datos personales. No compartir la contraseña de acceso al Sistema con usuarios no autorizados.
(Nombre del Encargado 2*)	Alejandra Nieto
Cargo*:	Servicios Escolares
Funciones*:	Brindar seguimiento al registro e inscripción de alumnos. Captura de datos personales del alumno para ciertos cursos y talleres. Inscribir a los alumnos en el grupo correspondiente. Contactar a alumnos para avisos e información. Envío de las boletas a los alumnos vía correo electrónico. Envío de avisos y las listas de grupos a los profesores. Enviar a la Delegación Administrativa datos solicitados para contactar a alumnos.

Obligaciones*:	Proteger los datos personales de los alumnos y profesores. No modificar la información de datos personales. No difundir información de los datos personales. No compartir la contraseña de acceso al Sistema con usuarios no autorizados.
(Nombre del Usuario 1*)	Mtra. Claudia Muñoz
Cargo*:	Coordinadora de Enseñanza de Español y Cultura
Funciones*:	Dar seguimiento a los procesos de registro de alumnos Contactar a los alumnos para enviar avisos e información relacionadas a los cursos. Contactar a los profesores para notificaciones o avisos.
Obligaciones*:	Proteger los datos personales de los alumnos y profesores. No modificar la información de datos personales. No difundir información de los datos personales. No compartir la contraseña de acceso al Sistema con usuarios no autorizados.
(Nombre del Usuario 2*)	Lic. Adriana Peguero
Cargo*:	Profesora de la Coordinación de Español y Cultura
Funciones*:	Dar seguimiento a los procesos de registro de alumnos Contactar a los alumnos para enviar avisos e información relacionadas a los cursos.
Obligaciones*:	Proteger los datos personales de los alumnos y profesores. No modificar la información de datos personales. No difundir información de los datos personales. No compartir la contraseña de acceso al Sistema con usuarios no autorizados.
(Nombre del Usuario 3*)	Lic. Paola Suyette Mendieta Verdejo
Cargo*:	Jefa del Departamento de Apoyo Académico a las sedes en el extranjero de la CRAI.
Funciones*:	Recibir y comprobar la información vertida en el formato de Actividades Académicas y Culturales.
Obligaciones*:	No difundir información de los datos personales. No modificar la información almacenada en el servidor. No hacer respaldos en equipo personal de la información de datos personales.
(**Nombre del Usuario 4*)**	Ing. Jorge Ángel Hernández López

Cargo*:	Jefe del Departamento de TIC´s de la CRAI.
Funciones*:	Salvaguardar la información en el servidor de la CRAI. Realizar los respaldos de la base de datos del Sistema. Corregir problemas técnicos del Sistema. Dar de alta las contraseñas de acceso solicitadas.
Obligaciones*:	No difundir información de los datos personales. No modificar la información almacenada en el servidor.

2. ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

SECRETARÍA ACADÉMICA	
Identificador único¨*	**UNAM CHICAGO-ESCOLAR**
(Nombre del sistema A2*)	**Sistema de Administración Escolar**
Tipo de soporte:*	Electrónico
Descripción:*	El registro de la información se almacena en una base de datos
Características del lugar donde se resguardan los soportes:*	El Sistema de Administración Escolar de UNAM Chicago está almacenado en el servidor de la Coordinación de Relaciones y Asuntos Internacionales.

3. ANÁLISIS DE RIESGOS

SECRETARÍA ACADÉMICA		
Identificador único*	**UNAM CHICAGO-ESCOLAR**	
(Nombre del sistema A2) *	**Sistema de Administración Escolar**	
Riesgo*	**Impacto***	**Mitigación***
Acceso no autorizado al Sistema Escolar.	Acceso a la información de datos personales para sustraerla, difundirla o modificarla.	Cambiar las contraseñas de acceso al sistema aplicando las "Políticas de contraseñas". Cambiar semestralmente las contraseñas de acceso al sistema aplicando las "Políticas de contraseñas". No almacenar la contraseña de acceso al Sistema en el equipo de cómputo del usuario.
Que los usuarios compartan su contraseña con usuarios no autorizados.	Personas no autorizadas tendrían acceso a la información de datos personales.	Firma de carta de confidencialidad.
Acceso no autorizado al servidor que alberga el sistema	Pérdida, robo o modificación no autorizada de la información	Mantener actualizado el servidor, contar con firewall, para evitar conexiones no autorizadas, políticas de seguridad para la infraestructura del servidor

4. ANÁLISIS DE BRECHA

SECRETARÍA ACADÉMICA		
Identificador único*	**UNAM CHICAGO-ESCOLAR**	
(Nombre del sistema A2) *	**Sistema de Administración Escolar**	
Medida de seguridad actual*	**Medida de seguridad necesaria***	**Acciones para remediación***
Acceso autorizado al Sistema Escolar con un usuario y contraseña.	Contraseñas robustas para usuarios autorizados que cumpla "Políticas de contraseñas".	Contar con un protocolo de contraseñas seguras y actualizarlas al menos cada semestre.

Cifrado de contraseñas de los usuarios	Asegurar que las contraseñas de los usuarios del sistema se almacenan de forma cifrada.	Protección de datos de acceso al sistema para evitar accesos no autorizados, minimizando el riesgo de robo o modificación no autorizada de la información

5. PLAN DE TRABAJO

SECRETARÍA ACADÉMICA			
Identificador único*	**UNAM CHICAGO-ESCOLAR**		
(Nombre del sistema A2) *	**Sistema de Administración Escolar**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Verificar el uso de contraseñas seguras para el acceso.	Actualizar las contraseñas de acceso con base en las “Políticas de contraseñas seguras”.	4 hrs	Se incrementa la seguridad en el acceso al sistema.
Firma de Carta de Confidencialidad	Elaborar una Carta de Confidencialidad para el manejo de datos personales que será firmada por los encargados y usuarios autorizados.	1 hr	Los usuarios formalizan por escrito su responsabilidad en el uso de datos personales.
Verificar políticas de seguridad del servidor	Establecer comunicación con el responsable del servidor para conocer las reglas de operación y seguridad sobre el servidor	6-8 hrs	Se minimiza el riesgo de una vulnerabilidad y que exista un acceso no autorizado y haya robo, pérdida o modificación de la información
Actualizar seguridad del servidor	En caso de que las políticas de seguridad, así como configuraciones no sean las correctas, generar un nuevo plan de trabajo para la correcta implementación de seguridad	Indefinido	Se minimiza el riesgo de una vulnerabilidad y que exista un acceso no autorizado y haya robo, pérdida o modificación de la información

6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

I. TRANSFERENCIAS DE DATOS PERSONALES

SECRETARÍA ACADÉMICA	
Identificador único*	**UNAM CHICAGO-ESCOLAR**
(Nombre del sistema A2)*	**Sistema de Administración Escolar**
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	No aplica
Transferencias mediante el traslado de soportes electrónicos:	Se realizan transferencias de datos personales mediante la nube privada de la cuenta Google creada por la CRAI a los usuarios autorizados.
Transferencias mediante el traslado sobre redes electrónicas:	Las conexiones se realizan por HTTP.

I. RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS

1. El Sistema de Administración Escolar (**UNAM CHICAGO-SE**) no realiza tratamiento de datos personales con soportes físicos, ya que se encuentra en soporte electrónico mediante el uso de una base de datos.

II. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

1 . L**os datos que se registran en las bitácoras:**
El mismo sistema cuenta, con una bitácora de registro de ingreso al sistema, se registra, la ip de conexión, nombre de usuario, hora de conexión y acción que realizó.

Las bitácoras se clasifican en personal de la sede y usuarios.

El responsable de la administración técnica del sistema las revisan aleatoriamente o en caso de alguna anomalía

III. REGISTRO DE INCIDENTES:

No se tiene un registro de incidentes

V. ACCESO A LAS INSTALACIONES

1. Seguridad perimetral exterior (las instalaciones del área universitaria):

El servidor se encuentra en las instalaciones de la coordinación de relaciones y asuntos internacionales, donde se utiliza un sistema de control de acceso en caso de trabajadores del edificio, cada perfil de usuario solo puede acceder a zonas autorizadas, según la dependencia de adscripción, así mismo, se tiene el sistema de CCTV; para visitantes mediante un videoportero en el cual se puede apreciar al visitante (dicha información no se guarda).

2. Seguridad perimetral interior (oficina, almacén o bodega para soportes físicos, centro de datos para soportes electrónicos):

El servidor se encuentra en el site de la CRAI, donde utilizan el sistema de control de acceso, sólo tiene acceso al site la tarjeta asignada al responsable de este, por otra parte, el responsable del site es el único que posee la llave de la puerta.

VI. ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

Los encargados del Sistema son los únicos autorizados para realizar la actualización de los datos personales de los Alumnos y Profesores, inicialmente se realizaban a petición del usuario, se validaba y se procedía al cambio.

Se propone modificar el procedimiento a:

Enviar vía electrónica el formato de "SOLICITUD DE EJERCICIO DE DERECHOS ARCO" al interesado.

Una vez recibida la solicitud, verificar si la información enviada en el formato es consistente con los documentos enviados previamente. De ser así, se procede a la solicitud de actualización de la información indicada

VII. PERFILES DE USUARIO Y CONTRASEÑAS

1. Modelo de control de acceso:

Está basado en roles.

1. Perfiles de usuario y contraseñas en el sistema operativo de red:
Los datos de usuario son almacenados por el aplicativo, no interviene el sistema operativo.

2. Perfiles de usuario y contraseñas manejados por el software aplicativo del sistema de tratamiento de datos personales:
El sistema guarda la contraseña del usuario.

3. Administración de perfiles de usuario y contraseñas:

La Coordinación de Planeación y Desarrollo Institucional autoriza los nuevos perfiles con privilegios de administrador y solicita la creación del usuario y contraseña al Responsable de TIC´s de la CRAI.

Los Encargados crean el perfil y contraseña de los profesores.

4. Acceso remoto al sistema de tratamiento de datos personales:
Los usuarios acceden al sistema mediante el uso de usuario y contraseña.

a) ¿Requiere el administrador acceso remoto al equipo donde reside el sistema para realizar tareas de mantenimiento? El responsable de TICs accede de forma remota al Servidor mediante conexiones cifradas por protocolo SSH, así mismo cuenta con un usuario y contraseña para el servidor.

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

1. Señalar si realiza respaldos
Se realiza un respaldo completo de forma automatizada de la base de datos del Sistema de manera diaria, dichos archivos se almacenan en el mismo equipo, posteriormente el responsable de TICs, almacena el ultimo respaldo en el servidor de archivos de la CRAI.

2. El tipo de medios (por ejemplo: cintas magnéticas, discos duros, CD-ROM, entre otros) que utiliza para almacenar las copias de seguridad
Los respaldos se almacenan en los servidores de la CRAI

3. Cómo y dónde archiva esos medios:
Se realizan mediante la herramienta del gestor de la BD, dejando una copia en una ruta específica del servidor, distinta al del aplicativo, posteriormente mediante una conexión cifrada de SSH se envían al servidor de respaldos.

4. Quién es el responsable de realizar estas operaciones (el área universitaria o un tercero).
El Ing. Jorge Hernández, Jefe de Departamento de TIC´s de la CRAI, ya que el Sistema se encuentra alojado en un servidor de esta Coordinación.

IX. PLAN DE CONTINGENCIA

1. Presentar el plan de contingencia con el cual garantiza la continuidad de la operación del sistema o informar si no lo tiene, pero se encuentra desarrollándose.

Se cuenta con algunas medidas como las medidas de seguridad en los periodos de inactividad o mantenimiento, pero no se tiene desarrollado el plan de contingencia

2. Si cuenta con plan de contingencia y lo ha implementado, deberá indicar si realiza pruebas de eficiencia de este.

No se cuenta con plan de contingencia

7. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

7.1. Herramientas y recursos para monitoreo de la protección de datos personales

SECRETARÍA ACADÉMICA		
Identificador único*	**UNAM CHICAGO-ESCOLAR**	
(Nombre del sistema A2)*	**Sistema de Administración Escolar**	
Recurso*	**Descripción***	**Control***
Bitácora del sistema	Revisión aleatoria	El responsable de la administración técnica del sistema las revisa aleatoriamente o en caso de alguna anomalía CRAI en coordinación con UNAM Chicago

7.1. Programa de capacitación a los responsables de tratamiento de datos personales

SECRETARÍA ACADÉMICA			
Identificador único A2*	**UNAM CHICAGO-ESCOLAR**		
(Nombre del sistema A2)*	**Sistema de Administración Escolar**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Taller	Virtual por zoom	16/08/22 10am a 1 pm.	Staff UNAM Chicago Anual

7.2. Procedimiento para la revisión de las medidas de seguridad

SECRETARÍA ACADÉMICA		
Identificador único*	**UNAM CHICAGO-ESCOLAR**	
(Nombre del sistema A2)*	**Sistema de Administración Escolar**	
Medida de seguridad*	**Procedimiento***	**Responsable***
Plan de respaldos de información.	Revisión y validación del historial de respaldos del sistema.	El responsable de realizar la revisión es el Ing. Jorge. Hernández, CRAI. La duración de la revisión es un día hábil.
Instalar y mantener actualizado el software antimalware.	Revisión y actualización de la versión del software antivirus y de la base de datos.	El responsable de realizar la revisión es el IT de UNAM Chicago. La duración de la revisión es un día hábil.

7.3. Resultados de la evaluación y pruebas a las medidas de seguridad

SECRETARÍA ACADÉMICA		
Identificador único*	**UNAM CHICAGO-ESCOLAR**	
(Nombre del sistema A2)*	**Sistema de Administración Escolar**	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***
Plan de respaldos de información.	Se cuenta con respaldos actualizados de la información del sistema.	El responsable de realizar la revisión es el Ing. Jorge Hernández, CRAI.
Instalar y mantener actualizado el software antimalware.	El Software antivirus está actualizado.	El responsable de realizar la revisión es el IT de UNAM Chicago.

7.4. Acciones para la corrección y actualización de las medidas de seguridad

SECRETARÍA ACADÉMICA		
Identificador único*	**UNAM CHICAGO-ESCOLAR**	
(Nombre del sistema A2)*	**Sistema de Administración Escolar**	
Medida de seguridad*	**Acciones***	**Responsable***
Uso de certificados SSL	Implementación del certificado SSL.	UNAM Chicago en coordinación con la CRAI.
Cambio del módulo de contraseñas.	Cambiar las contraseñas de los usuarios actualizados de manera semestral.	UNAM Chicago en coordinación con la CRAI.

8. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

8.1. Programa de capacitación a los responsables de tratamiento de datos personales

SECRETARÍA ACADÉMICA			
Identificador único*	**UNAM CHICAGO-ESCOLAR**		
(Nombre del sistema A2)*	**Sistema de Administración Escolar**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Elaboración del Documento de Seguridad y Sistema de Gestió de Seguridad de Datos Personales de las áreas universitarias.	Taller vía zoom	16/08/22 10am a 1 pm.	Staff UNAM Chicago Anual

8.2. Programa de difusión de la protección a los datos personales

No se cuenta con un programa de difusión de la protección de datos personales.

9. MEJORA CONTINUA

9.1. Actualización y mantenimiento de sistemas de información

SECRETARÍA ACADÉMICA			
Identificador único*	**UNAM CHICAGO-ESCOLAR**		
(Nombre del sistema A2)*	**Sistema de Administración Escolar**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Actualización del manejador de BD	Actualización de la versión del manejador de BD.	2-4 hrs	Actualización de la versión del gestor de base de datos.
Actualización del servicio web	Actualizar el servicio web de forma constante para evitar huecos de seguridad en el aplicativo.	2-4 hrs	Actualización del servicio web que usa el servidor.

9.2. Actualización y mantenimiento de equipo de cómputo

SECRETARÍA ACADÉMICA			
Identificador único*	**UNAM CHICAGO-ESCOLAR**		
(Nombre del sistema A2)*	**Sistema de Administración Escolar**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Actualización del antivirus del servidor Mantenimiento preventivo lógico	Actualización de versión del sistema operativo	4-6 horas	Actualización del sistema operativo, así como paquetes correspondientes para el correcto funcionamiento de este.

Actualización del antivirus del servidor Mantenimiento preventivo físico	Limpieza y verificación del correcto funcionamiento de los componentes del servidor	8-10 horas	Limpieza del servidor, pruebas de desempeño y de estado de memorias RAM, procesador, discos duros, para garantizar el correcto funcionamiento de éste.

9.3. Procesos para la conservación, preservación y respaldos de información

SECRETARÍA ACADÉMICA		
Identificador único*	**UNAM CHICAGO-ESCOLAR**	
(Nombre del sistema A2)*	**Sistema de Administración Escolar**	
Proceso*	**Descripción***	**Responsable***
Plan de respaldos de información.	Se realiza un respaldo completo de forma automatizada de la base de datos del Sistema de manera diaria, dichos archivos se almacenan en el mismo equipo, posteriormente el responsable de TICs, almacena el último respaldo en el servidor de archivos de la CRAI. Los respaldos se hacen mediante la herramienta del gestor de la BD, dejando una copia en una ruta específica del servidor, distinta al del aplicativo, posteriormente mediante una conexión cifrada de SSH se envían al servidor de respaldos.	El Ing. Jorge Hernández, Jefe de Departamento de TIC´s de la CRAI, ya que el Sistema se encuentra alojado en un servidor de esta dependencia.

9.4. Procesos de borrado seguro y disposición final de equipos y componentes informáticos
No aplica para UNAM Chicago. Este sistema está alojado en el servidor de CRAI.

10. PROCEDIMIENTO PARA LA CANCELACIÓN DE UN SISTEMA DE TRATAMIENTO DE DATOS PERSONALES. No aplica para UNAM Chicago.
Este sistema está alojado en el servidor de CRAI.

III. SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES A3. ENSEÑANZA DE ESPAÑOL Y CULTURA

1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

SECRETARÍA ACADÉMICA	
Identificador único*	UNAM Chicago-Colocación
(Nombre del sistema A3.1) *	**Base de datos de aplicación de exámenes de colocación**
Datos personales (sensibles o no) contenidos en el sistema*:	Nombre(s), apellido(s), teléfono (particular, celular y/o institucional), correo electrónico (personal o institucional), correo electrónico, nacionalidad y ocupación.
Responsable*:	Coordinación de enseñanza de español y cultura
Nombre:	Claudia Muñoz Cano
Cargo*:	Coordinadora
Funciones*:	Llevar el registro de los alumnos que requieren examen de colocación
Obligaciones*:	No difundir los datos personales de los estudiantes
	Encargados:
(Nombre del Encargado 1*)	Adriana Peguero Ceja
Cargo	Profesora de tiempo completo
Funciones*:	Llevar el registro de los alumnos que requieren examen de colocación
Obligaciones*:	No difundir los datos personales de los estudiantes
	Usuarios:
(Nombre del Usuario 1*)	Carmen Martínez
Cargo*:	Profesora de medio tiempo
Funciones*:	Apoyar en el registro de los alumnos que requieren examen de colocación
Obligaciones*:	No difundir los datos personales de los estudiantes
Identificador único*	UNAM Chicago-PreT
Sistema (Nombre del A3.2)*:	**Base de datos de pre-registro a talleres de español y cultura**
Datos personales contenidos en el sistema*:	Nombre(s), apellido(s), teléfono (particular, celular y/o institucional), correo electrónico (personal o institucional), correo electrónico, edad y género.

Responsable:	Coordinación de enseñanza de español y cultura
Nombre*:	Claudia Muñoz Cano
Cargo*:	Coordinadora
Funciones*:	Llevar el registro de los alumnos inscritos en los talleres de cultura y español.
Obligaciones*:	No difundir los datos personales de los estudiantes
	Encargados:
(Nombre del Encargado 1*)	Adriana Peguero Ceja
Cargo*:	Profesora de tiempo completo
Funciones*:	Llevar el registro de los alumnos inscritos en los talleres de cultura y español.
Obligaciones*:	No difundir los datos personales de los estudiantes
	Usuarios:
(Nombre del Usuario 1*)	Carmen Martínez
Cargo*:	Profesora de medio tiempo
Funciones*:	Apoyar en el registro de los alumnos inscritos en los talleres de cultura y español.
Obligaciones*:	No difundir los datos personales de los estudiantes

2. ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

SECRETARÍA ACADÉMICA	
Identificador único¨*	UNAM Chicago-Colocación
(Nombre del sistema A3.1)	**Base de datos de aplicación de exámenes de colocación**
Tipo de soporte:*	Electrónico
Descripción:*	Base de datos
Características del lugar donde se resguardan los soportes:*	Alojamiento en la plataforma Moodle creada por la CUAIEED para UNAM Chicago. Los estudiantes ingresan a la plataforma con un nombre de usuario y una contraseña generados por la Coordinación de enseñanza de español y cultura
(Nombre del sistema A3.2)	**Base de datos de pre-registro a talleres de lengua y cultura**
Tipo de soporte*:	Electrónico
Descripción*:	Base de datos
Características del lugar donde se resguardan los soportes*:	Alojamiento en la nube de la cuenta Google creada por la CRAI para la Coordinación de enseñanza y de español y cultura de UNAM Chicago

3. ANÁLISIS DE RIESGOS

SECRETARÍA ACADÉMICA		
Identificador único*	UNAM Chicago-Colocación	
(Nombre del sistema A3.1) *	Base de datos de aplicación de exámenes de colocación	
Riesgo*	**Impacto***	**Mitigación***
Acceso a la plataforma Moodle.	Alteración de información personal	Aplicar correctamente las medidas para crear contraseñas más seguras.

SECRETARÍA ACADÉMICA		
Identificador único*	UNAM Chicago-Colocación	
(Nombre del sistema A3.2) *	Base de datos pre- registro para talleres de lengua y cultura	
Riesgo*	**Impacto***	**Mitigación***
Acceso al Drive de Google	Alteración de información personal	Cambiar contraseña de acceso a Google Drive

4. ANÁLISIS DE BRECHA

SECRETARÍA ACADÉMICA		
Identificador único*	UNAM Chicago-Colocación	
(Nombre del sistema A3.1) *	Base de datos de aplicación de exámenes de colocación	
Medida de seguridad actual*	**Medida de seguridad necesaria***	**Acciones para remediación***
Acceso autorizado a la plataforma Moodle con un usuario y contraseña.	Actualizar contraseñas de acceso del responsable, encargado y usuario del sistema	Actualizar contraseñas cada seis meses

SECRETARÍA ACADÉMICA		
Identificador único*	UNAM Chicago-Colocación	
(Nombre del sistema A3.2) *	Base de datos pre- registro para talleres de lengua y cultura	
Medida de seguridad actual*	**Medida de seguridad necesaria***	**Acciones para remediación***
Acceso autorizado a la cuenta de Google Drive donde se alojan los formularios.	Actualizar contraseñas de acceso del responsable, encargado y usuario del sistema	Actualizar contraseñas cada seis meses

5. PLAN DE TRABAJO

SECRETARÍA ACADÉMICA			
Identificador único*	UNAM Chicago-Colocación		
(Nombre del sistema A3.1) *	Base de datos de aplicación de exámenes de colocación		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Actualizar los datos de acceso del responsable, encargado y usuario del sistema	Actualizar las contraseñas asignadas al responsable, encargado y usuario del sistema	A partir del 15 de septiembre de 2022 se empezará a hacer cada trimestre.	Al actualizar los datos de acceso se incrementa la protección de los datos personales.

SECRETARÍA ACADÉMICA			
Identificador único*	UNAM Chicago-PreT		
(Nombre del sistema A3.2) *	Base de datos pre- registro para talleres de lengua y cultura		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Bajar los formularios de la nube al Servidor de UNAM Chicago	Convertir los formularios de Google en archivos excel para bajarlos de la nube y guardarlos en el servidor de la sede .	A partir del 15 de septiembre de 2022 se empezará a hacer cada trimestre.	Al bajar los formularios se incrementa la protección de los datos personales

6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

I.TRANSFERENCIAS DE DATOS PERSONALES

SECRETARÍA ACADÉMICA	
Identificador único*	UNAM Chicago-Colocación
(Nombre del sistema A3.1)*	Base de datos de aplicación de exámenes de colocación
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	.No se realizan transferencias de datos personales mediante el traslado de soportes físicos.
Transferencias mediante el traslado de soportes electrónicos:	No se realizan transferencias de datos personales mediante el traslado de soportes electrónicos.
Transferencias mediante el traslado sobre redes electrónicas:	No se realizan transferencias de datos personales mediante el traslado sobre redes electrónicas.
Identificador único*	UNAM Chicago-PreT
(Nombre del sistema A3.2)	Base de datos pre- registro para talleres de lengua y cultura
Transferencias mediante el traslado de soportes físicos:	No se realizan transferencias de datos personales mediante el traslado de soportes físicos.
Transferencias mediante el traslado de soportes electrónicos:	La transferencia de datos se hace desde la nube privada de la cuenta Google creada por la CRAI para la Coordinación.
Transferencias mediante el traslado sobre redes electrónicas:	No se realizan transferencias de datos personales mediante el traslado sobre redes electrónicas.

II. RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS

El Examen de colocación y el registro a talleres de lengua y cultura no realizan tratamiento de datos personales con soportes físicos, ya que se encuentran en soporte electrónico mediante el uso de una base de datos.

III. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

La plataforma Moodle donde se aloja el Examen de colocación (Sistema A3.1) proporciona la bitácora de accesos de los profesores y alumnos a este sistema.

La Base de datos pre- registro para talleres de lengua y cultura (Sistema A3.2) es un formulario de Google alojado en el drive, por lo que se puede ver el historial de acceso del responsable, encargado y usuario de este sistema.

Responsable, encargado y usuario tienen acceso a los datos personales en ambos sistemas. Ambos sistemas tienen historial por lo que se pueden consultar las bitácoras de acceso del responsable, el encargado y el usuario.

IV. REGISTRO DE INCIDENTES:

No se tiene registro de incidentes.

V. ACCESO A LAS INSTALACIONES

Seguridad perimetral exterior (las instalaciones del área universitaria): UNAM CHICAGO

Se cuenta con un sistema de cámaras instaladas alrededor del edificio (puerta de entrada al edificio, entrada del área de carga y descarga en la parte de atrás del edificio, callejones laterales del inmueble). Se cuenta con un sistema de interfón para dar acceso solamente a las personas que tengan algún asunto relativo a la institución. En caso afirmativo se les da la entrada, en caso contrario no se da acceso.

Los empleados cuentan con una clave de acceso al edificio.

Seguridad perimetral interior (oficina, almacén o bodega para soportes físicos, centro de datos para soportes electrónicos):

Se tienen cámaras instaladas en la entrada a la Escuela, en los pasillos de las oficinas administrativas, en el lobby, en el pasillo que lleva a los sanitarios, cocina, Galería 2, en las dos Galerías, en las escaleras que van al sótano, en el pasillo de las aulas. La información se almacena en el DVR máximo por un mes.

El sistema de cámaras se encuentra resguardado en un clóset localizado en el primer piso, con puerta de madera, chapa y llave. Las llaves de ese clóset se encuentran en un llavín con clave de acceso para abrirlo, en la oficina de la Delegación Administrativa y sólo la Delegada tiene acceso a ese llavín.

Las puertas de acceso a la Escuela y CIERTAS Áreas restringidas cuentan con dos chapas y llaves de seguridad. También, se cuenta con un sistema de alarma y solamente las personas autorizadas para abrir y cerrar la Escuela tienen llave de acceso y clave de alarma.

El tratamiento que se la da a los datos personales captados por las cámaras ya fue explicado en la sección correspondiente al Sistema A1.1

VI. ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

En este apartado se deberá establecer un mecanismo o procedimiento institucional para la actualización de la información personal contenida en el sistema, en donde se establezca la frecuencia con la que se efectúa y la forma en que se está solicitando al titular acreditar de manera idónea sus requerimientos de rectificación de datos inexactos.

Para el sistema A3.1, los usuarios pueden realizar la actualización de sus datos personales una vez que han ingresado al sistema mediante sus códigos de acceso, en el apartado “Actualizar mis datos”.

Para el sistema A3.2 no es necesario hacer actualización de datos, pues es solo un pre-registro de estudiantes interesados en los cursos de lengua y cultura.

Las medidas de seguridad previstas a continuación en los incisos VII al IX, sólo aplican para soportes electrónicos

VII. PERFILES DE USUARIO Y CONTRASEÑAS

En este rubro el área universitaria deberá describir el esquema de perfiles de usuario y contraseñas que tiene implementado para control de acceso mediante una red electrónica.

1. Modelo de control de acceso (alguno de los siguientes):
Está basado en roles

2. Perfiles de usuario y contraseñas en el sistema operativo de red:

a) ¿Cuenta con un sistema operativo de red instalado en sus equipos? **No**
b) ¿Proporciona dicho sistema operativo un manejo riguroso de perfiles de usuario y contraseñas? **No se cuenta con un sistema operativo**
c) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena? **No se cuenta con un sistema operativo**

3. Perfiles de usuario y contraseñas manejados por el software aplicativo del sistema de tratamiento de datos personales:

a) ¿Ofrece dicho software un manejo riguroso de perfiles de usuario y contraseñas? No se cuenta con un sistema operativo
b) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena? No se cuenta con un sistema operativo

4. Administración de perfiles de usuario y contraseñas:

- **a)** ¿Quién da de alta nuevos perfiles? La Coordinación de enseñanza de lengua y cultura (Responsable y Encargado)
- **b)** ¿Quién autoriza la creación de nuevos perfiles? La Coordinación de enseñanza de lengua y cultura (Responsable y Encargado)
- **c)** ¿Se lleva registro de la creación de nuevos perfiles? Sí

5. Acceso remoto al sistema de tratamiento de datos personales:

- **a)** ¿Requieren los usuarios acceso remoto al equipo de cómputo que por lo general utilizan para trabajar con el sistema? No
- **b)** ¿Requiere el administrador acceso remoto al equipo donde reside el sistema para realizar tareas de mantenimiento? No
- **c)** ¿Cómo se evita el acceso remoto no autorizado? No se necesita acceso remoto al sistema de tratamiento de datos personales

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

Para el sistema A3.1:

Los respaldos se realizan de forma completa y automatizada, el sitio público una vez por mes, carpeta de persistencia (moodledata) lunes y sábado, base de datos todos los días. Se almacenan de forma permanente en cintas magnéticas para su resguardo almacenados en la oficina del departamento de operaciones y seguridad informática los cuales son los responsables de todo el procedimiento.

Para el sistema A3.2:

1. Señalar si realiza respaldos
   - **a)** Completos_X_, diferenciales ___ o incrementales___;
   - **b)** De forma automática ____ o Manual __X___,
   - **c)** Periodicidad con que los realiza: __Semestralmente_____
2. El tipo de medios (por ejemplo: cintas magnéticas, discos duros, CD-ROM, entre otros) que utiliza para almacenar las copias de seguridad:
   Disco duro
3. Cómo y dónde archiva esos medios, y
   El respaldo se almacena en el servidor de UNAM Chicago en discos ocultos
4. Quién es el responsable de realizar estas operaciones (el área universitaria o un tercero).
   Un tercero

IX. PLAN DE CONTINGENCIA

1. Presentar el plan de contingencia con el cual garantiza la continuidad de la operación del sistema o informar si no lo tiene, pero se encuentra desarrollándose.

Se cuenta con algunas medidas como las medidas de seguridad en los periodos de inactividad o mantenimiento, pero no se tiene desarrollado el plan de contingencia

2. Si cuenta con plan de contingencia y lo ha implementado, deberá indicar si realiza pruebas de eficiencia de este.

No se cuenta con plan de contingencia

3. Informar si cuenta con un sitio redundante (alterno) y señalar lo siguiente:

a) El tipo de sitio (caliente, tibio o frío);
b) Si el sitio es propio o subcontratado con un tercero;
c) Los procedimientos, el equipo y el personal que designa para poner en marcha tal sitio y
d) Tiempo que le lleva poner en marcha el sitio, según las pruebas de eficiencia.

7. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

7.1. Herramientas y recursos para monitoreo de la protección de datos personales

SECRETARÍA ACADÉMICA		
Identificador único*	UNAM Chicago-Colocación	
(Nombre del sistema A3.1)*	Base de datos de aplicación de exámenes de colocación	
Recurso*	**Descripción***	**Control***
Bitácora del sistema	Revisión aleatoria	CUAIEED. Departamento de operaciones y seguridad informática

UNAM CHICAGO		
Identificador único*	UNAM Chicago-PreT	
(Nombre del sistema A3.2)*	Base de datos de pre-registro a talleres de español y cultura	
Recurso*	**Descripción***	**Control***
Bitácora manual	Revisión aleatoria	El responsable de la administración técnica del sistema las revisa aleatoriamente o en caso de alguna anomalía

7.2. Procedimiento para la revisión de las medidas de seguridad

SECRETARÍA ACADÉMICA		
Identificador único*	UNAM Chicago-Colocación	
(Nombre del sistema A3.1)*	Base de datos de aplicación de exámenes de colocación	
Medida de seguridad*	**Procedimiento***	**Responsable***
Análisis de configuraciones del sistema operativo y aplicación.	Se realiza una revisión de las actualizaciones del servidor y la aplicación LMS Moodle una vez cada treinta días validando si existen nuevas actualizaciones tanto en versiones del aplicativo como del sistema operativo y su paquetería.	CUAIEED. Departamento de operaciones y seguridad informática, 1 día.

SECRETARÍA ACADÉMICA		
Identificador único*	UNAM Chicago-PreT	
(Nombre del sistema A3.2)*	Base de datos de pre-registro a talleres de español y cultura	
Medida de seguridad*	**Procedimiento***	**Responsable***
Instalar y mantener actualizado el software antimalware.	Revisión y actualización de la versión del software antivirus y de la base de datos.	El responsable de realizar la revisión es el IT de UNAM Chicago. La duración de la revisión es un día hábil.

7.3. Resultados de la evaluación y pruebas a las medidas de seguridad

SECRETARÍA ACADÉMICA		
Identificador único*	UNAM Chicago-Colocación	
(Nombre del sistema A3.1)*	Base de datos de aplicación de exámenes de colocación	
Medida de seguridad*	**Procedimiento***	**Responsable***
Plan de respaldos de información.	Revisión y validación del historial de respaldos del sistema.	CUAIEED. Departamento de operaciones y seguridad informática, 1 día.
Instalar y mantener actualizado el software antimalware.	Revisión y actualización de la versión del software antivirus y de la base de datos.	CUAIEED. Departamento de operaciones y seguridad informática, 1 día.

SECRETARÍA ACADÉMICA		
Identificador único*	UNAM Chicago-PreT	
(Nombre del sistema A3.2)*	Base de datos de pre-registro a talleres de español y cultura	
Medida de seguridad*	**Procedimiento***	**Responsable***
Instalar y mantener actualizado el software antimalware.	Revisión y actualización de la versión del software antivirus y de la base de datos.	El responsable de realizar la revisión es el IT de UNAM Chicago. La duración de la revisión es un día hábil.

7.4. Acciones para la corrección y actualización de las medidas de seguridad

SECRETARÍA ACADÉMICA		
Identificador único*	UNAM Chicago-Colocación	
(Nombre del sistema A3.1)*	Base de datos de aplicación de exámenes de colocación	
Medida de seguridad*	**Acciones***	**Responsable***
Actualización de la paquetería del sistema operativo y/o la aplicación.	Se realiza la actualización del sistema operativo junto con sus dependencias así como de existir alguna actualización del aplicativo.	CUAIEED. Departamento de operaciones y seguridad informática, 1 día.

SECRETARÍA ACADÉMICA		
Identificador único*	UNAM Chicago-PreT	
(Nombre del sistema A3.2)*	Base de datos de pre-registro a talleres de español y cultura	
Medida de seguridad*	**Acciones***	**Responsable***
Cambio del módulo de contraseñas.	Cambiar las contraseñas del personal que tiene acceso a los equipos de cómputo los usuarios actualizados de manera semestral.	El responsable de realizar la revisión es el IT de UNAM Chicago.
El servidor permite fallas parciales como discos duros, memoria y fuente de poder.	a) Se tiene un sistema redundante. b) Limpieza y mantenimiento.	El responsable de realizar la revisión es el IT de UNAM Chicago. La duración de la revisión son dos días hábiles.

8. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

8.1. Programa de capacitación a los responsables de tratamiento de datos personales

SECRETARÍA ACADÉMICA			
Identificador único*	UNAM Chicago-Colocación		
(Nombre del sistema A3.1)*	Base de datos de aplicación de exámenes de colocación		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Taller	Virtual por zoom	16/08/22 de 10am a 1pm.	Staff UNAM Chicago Actualización anual

SECRETARÍA ACADÉMICA			
Identificador único*	UNAM Chicago-PreT		
(Nombre del sistema A3.2)*	Base de datos de pre-registro a talleres de español y cultura		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Taller	Virtual por zoom	16/08/22 de 10am a 1pm.	Staff UNAM Chicago Actualización anual

8.2. Programa de difusión de la protección a los datos personales

SECRETARÍA ACADÉMICA			
Identificador único*	UNAM Chicago-Colocación		
(Nombre del sistema A3.1)*	Base de datos de aplicación de exámenes de colocación		
Actividad*	**Descripción***	**Duración***	**Cobertura***
No se cuenta con un programa de difu sión de la protección de datos personales			

SECRETARÍA ACADÉMICA			
Identificador único*	UNAM Chicago-PreT		
(Nombre del sistema A3.2)*	Base de datos de pre-registro a talleres de español y cultura		
Actividad*	**Descripción***	**Duración***	**Cobertura***
No se cuenta con un programa de difusión de la protección de datos personales.			

9. MEJORA CONTINUA

9.1. Actualización y mantenimiento de sistemas de información

SECRETARÍA ACADÉMICA			
Identificador único*	UNAM Chicago-Colocación		
(Nombre del sistema A3.1)*	Base de datos de aplicación de exámenes de colocación		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Actualización del aplicativo LMS Moodle.	Se realiza la revisión y actualización a la última versión estable de la plataforma	Permanente	Completa

SECRETARÍA ACADÉMICA			
Identificador único*	UNAM Chicago-PreT		
(Nombre del sistema A3.2)*	Base de datos de pre-registro a talleres de español y cultura		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Como la base de datos se respalda en el Servidor, se actualiza la memoria y los discos duros cada 2 años, y se le da un mantenimiento anual.	Actualizar el servicio web de forma constante para evitar huecos de seguridad en el aplicativo.	2-4 hrs	Actualización del servicio web que usa el servidor.

9.2. Actualización y mantenimiento de equipo de cómputo

SECRETARÍA ACADÉMICA			
Identificador único*	UNAM Chicago-Colocación		
(Nombre del sistema A3.1)*	Base de datos de aplicación de exámenes de colocación		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Actualización del antivirus del servidor Mantenimiento preventivo lógico	Actualización de versión del sistema operativo	4-6 horas	Actualización del sistema operativo, así como paquetes correspondientes para el correcto funcionamiento de éste.

SECRETARÍA ACADÉMICA			
Identificador único*	UNAM Chicago-PreT		
(Nombre del sistema A3.2)*	Base de datos de pre-registro a talleres de español y cultura		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Como la base de datos se respalda en el Servidor, se hace una actualización del antivirus del mismo. Además, se realiza un mantenimiento preventivo físico que consiste en la revisión de las fuentes de poder, de la memoria, de los discos duros y el software.	Limpieza y verificación del correcto funcionamiento de los componentes del servidor.	Dos días	Limpieza del servidor, pruebas de desempeño y de estado de memorias RAM, procesador, discos duros, para garantizar el correcto funcionamiento de éste.

9.3. Procesos para la conservación, preservación y respaldos de información

SECRETARÍA ACADÉMICA		
Identificador único*	UNAM Chicago-Colocación	
(Nombre del sistema A3.1)*	Base de datos de aplicación de exámenes de colocación	
Proceso*	**Descripción***	**Responsable***
Almacenamiento y preservación de los respaldos.	Los respaldos obtenidos de la plataforma son grabados en cintas magnéticas para su protección y almacenamiento.	CUAIEED Departamento de operaciones y seguridad informática. Tiempo de ejecución: 1 día

SECRETARÍA ACADÉMICA		
Identificador único*	UNAM Chicago-PreT	
(Nombre del sistema A3.2)*	Base de datos de pre-registro a talleres de español y cultura	
Proceso*	**Descripción***	**Responsable***
El respaldo se hace en un disco duro interno y en otro externo.	Se hace con un software de respaldos.	El responsable de realizar la revisión es el IT de UNAM Chicago. La duración de la revisión son dos días hábiles.

9.4. PROCESOS DE BORRADO SEGURO Y DISPOSICIÓN FINAL DE EQUIPOS Y COMPONENTES INFORMÁTICOS

SECRETARÍA ACADÉMICA		
Identificador único*	UNAM Chicago-Colocación	
(Nombre del sistema A3.1)*	Base de datos de aplicación de exámenes de colocación	
Proceso*	**Descripción***	**Responsable***
Eliminación del equipo físico (hardware del servidor y sistema de almacenamiento).	El equipo físico es entregado al área de Servicios Universitarios para su baja definitiva y posterior destrucción, los datos almacenados en medios físicos son borrados de forma permanente mediante un borrado de bajo nivel.	CUAIEED, UNAM Departamento de operaciones y seguridad informática, borrado seguro, tiempo 1 día. La baja del equipo depende de otra área universitaria donde el proceso puede tardar de 6 meses a 1 año.

SECRETARÍA ACADÉMICA		
Identificador único*	UNAM Chicago-PreT	
(Nombre del sistema A3.2)*	Base de datos de pre-registro a talleres de español y cultura	
Proceso*	**Descripción***	**Responsable***
Como la base de datos se respalda en el servidor, se hace el formateo y destrucción de los discos duros.	Todo el proceso se realiza con un software en una computadora.	El responsable es el IT de UNAM Chicago. La ejecución del proceso se realiza en dos días hábiles.

10. PROCEDIMIENTO PARA LA CANCELACIÓN DE UN SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

A) DATOS DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES QUE SERÁ CANCELADO:

Sistema A3.1: Base de datos de aplicación de exámenes de colocación **Procedimiento:** **La eliminación de datos es permanente e irreversible, con las autorizaciones debidas y necesarias.**

Sistema A3.2: Base de datos de pre-registro a talleres de español y cultura **Procedimiento:** **La eliminación de datos es permanente e irreversible, con las autorizaciones debidas y necesarias.**

B) PLAZOS Y CONDICIONES PARA EL BLOQUEO DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES:

No aplica

C) MEDIDAS DE SEGURIDAD PARA EL BLOQUEO Y POSTERIOR SUPRESIÓN DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES:

No aplica

D) PROCEDIMIENTO PARA LA SUPRESIÓN DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

No aplica

E) MECANISMOS PARA LA SUPRESIÓN DEL SISTEMA DE TRATAMIENTO DE DATOS PERSON

No aplica

IV. SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES A4. MOVILIDAD

1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

SECRETARÍA ACADÉMICA	
Identificador único*	UNAM Chicago - Movilidad.
(Nombre del sistema A4) *	Base de Datos de estudiantes de Servicio Social y Prácticas Profesionales.
Datos personales (sensibles o no) contenidos en el sistema*:	**1.** Datos personales en general: . Datos de identificación: Nombre completo, correo electrónico. **2.** Datos académicos: No. de cuenta del estudiante, Nombre Facultad o Escuela, Programa asignado, historial académico. **3.** Datos laborales: Curriculum Vitae.
Responsable*:	Secretaría Académica.
Nombre*:	Erika Erdely Ruiz.
Cargo*:	Secretaría Académica.
Funciones:	Coadyuvar en el contenido y uso de la base de datos.
Obligaciones:	Supervisar que la base de datos cumpla con las medidas para la protección de datos.
Encargado:	Marco Antonio Fuentes Tamayo.
Cargo:	Coordinador de Movilidad y Servicios Académicos.
Funciones*:	Llevar un registro de estudiantes que prestan su servicio social a través de los programas de Servicio Social y/o realizan prácticas profesionales en la UNAM Chicago; recibir solicitudes de prácticas profesionales y de Servicio Social, dar seguimiento desde la petición inicial hasta la conclusión de la misma.
Obligaciones*:	● Guardar confidencialidad respecto a los datos personales, académicos y laborales de los estudiantes. ● Mantener la información dentro del Departamento de Movilidad y Servicios Académicos. ● Hacer uso de la información únicamente para los fines especificados. ● Vigilar que el sistema cumpla con todas las medidas de seguridad técnicas y administrativas. ● Resguardar la información almacenada en la base de datos. ● No difundir la información de los datos personales.

2. ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

SECRETARÍA ACADÉMICA	
Identificador único¨*	UNAM Chicago - Movilidad.
(Nombre del sistema A4*)	Base de Datos de estudiantes de Servicio Social y Prácticas Profesionales.
Tipo de soporte:*	Soporte electrónico.
Descripción:*	Hoja de cálculo.
Características del lugar donde se resguardan los soportes:*	Alojamiento en Google Drive.

3. ANÁLISIS DE RIESGOS

SECRETARÍA ACADÉMICA		
Identificador único*	UNAM Chicago - Movilidad.	
(Nombre del sistema A4) *	Base de Datos de estudiantes de Servicio Social y Prácticas Profesionales.	
Riesgo*	**Impacto***	**Mitigación***
Acceso al equipo de cómputo que resguarda y mediante el cual se puede acceder directamente a la cuenta y los archivos de Google.	Acceso ilimitado a la información y datos personales, así como su modificación y divulgación.	Construir una contraseña compleja y de alto nivel de seguridad, de tal manera que, los datos e información se mantengan protegidos aun y cuando se acceda físicamente al equipo de cómputo.

4. ANÁLISIS DE BRECHA

SECRETARÍA ACADÉMICA		
Identificador único*	UNAM Chicago - Movilidad.	
(Nombre del sistema A4) *	Base de Datos de estudiantes de Servicio Social y Prácticas Profesionales	
Medida de seguridad actual*	**Medida de seguridad necesaria***	**Acciones para remediación***
Usuarios autorizados para el monitoreo.	Mejorar la calidad y complejidad de las contraseñas para usuarios autorizados por la Secretaría Académica.	Actualizar las contraseñas cada seis meses.

5. PLAN DE TRABAJO

SECRETARÍA ACADÉMICA			
Identificador único*	UNAM Chicago - Movilidad.		
(Nombre del sistema A4) *	Base de Datos de estudiantes de Servicio Social y Prácticas Profesionales		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Implementación de contraseñas de alta seguridad en las cuentas que tienen acceso a la base de datos.	Utilizar contraseñas robustas y de alta seguridad para acceder a las cuentas que tienen acceso a los datos personales. El objetivo es brindar mayor seguridad y limitar la accesibilidad a la información personal para que solo tengan acceso personal autorizado.	Las contraseñas robustas y de alta seguridad serán actualizadas por lo menos una vez al semestre durante un periodo indeterminado.	Incremento en la protección a los datos personales.

6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS
I.TRANSFERENCIAS DE DATOS PERSONALES

SECRETARÍA ACADÉMICA	
Identificador único*	UNAM Chicago - Movilidad.
(Nombre del sistema A4)*	Base de Datos de estudiantes de Servicio Social y Prácticas Profesionales
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	No se realizan transferencias mediante el traslado de soportes físicos.
Transferencias mediante el traslado de soportes electrónicos:	La transferencia de datos se hace desde la nube privada de la cuenta Google creada por la CRAI la coordinación de movilidad transfiere a la coordinación de planeación y desarrollo y Secretaría Académica.
Transferencias mediante el traslado sobre redes electrónicas:	No se realizan transferencias mediante el traslado de redes electrónicas.

II. **RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS**

1. La base de datos de información personal no cuenta con soportes físicos, ya que se encuentran en soporte electrónico.

III. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

No se lleva bitácora.

IV. REGISTRO DE INCIDENTES:

No se cuenta con procedimientos para atender incidentes.

V. ACCESO A LAS INSTALACIONES

1. **Seguridad perimetral exterior** (las instalaciones del área universitaria): **UNAM CHICAGO**

a) Se cuenta con un sistema de cámaras instaladas alrededor del edificio (puerta de entrada al edificio, entrada del área de carga y descarga en la parte de atrás del edificio, callejones laterales del inmueble). Se cuenta con un sistema de interfón para dar acceso solamente a las personas que tengan algún asunto relativo a la institución. En caso afirmativo se les da la entrada, en caso contrario no se da acceso.

Los empleados cuentan con una clave de acceso al edificio.

2. Seguridad perimetral interior (oficina, almacén o bodega para soportes físicos, centro de datos para soportes electrónicos):

Se tienen cámaras instaladas en la entrada a la Escuela, en los pasillos de las oficinas administrativas, en el lobby, en el pasillo que lleva a los sanitarios, cocina, Galería 2, en las dos Galerías, en las escaleras que van al sótano, en el pasillo de las aulas. La información se almacena en el DVR máximo por un mes.

El sistema de cámaras se encuentra resguardado en un clóset localizado en el primer piso, con puerta de madera, chapa y llave. Las llaves de ese clóset se encuentran en un llavín con clave de acceso para abrirlo, en la oficina de la Delegación Administrativa y sólo la Delegada tiene acceso a ese llavín.

Las puertas de acceso a la Escuela y CIERTAS Áreas restringidas cuentan con dos chapas y llaves de seguridad. También, se cuenta con un sistema de alarma y solamente las personas autorizadas para abrir y cerrar la Escuela tienen llave de acceso y clave de alarma. El tratamiento que se le da a los datos personales captados por las cámaras ya fue explicado en otra sección de este cuestionario.

VI. ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

La actualización de la información contenida en el sistema de tratamiento de datos personales será de manera manual, a cargo del coordinador del área, o la secretaría académica, siempre y cuando consideren que la información debe ser actualizada y bajo el consentimiento de los titulares de los datos personales.

Las medidas de seguridad previstas a continuación en los incisos VII al IX, sólo aplican para soportes electrónicos

VII. PERFILES DE USUARIO Y CONTRASEÑAS

1. Modelo de control de acceso:

Está basado en roles.

1. Perfiles de usuario y contraseñas en el sistema operativo de red:
Los perfiles de usuario y contraseñas son almacenados por gmail. El acceso lo concede la secretaría académica o el coordinador de movilidad y servicios académicos.

2. Perfiles de usuario y contraseñas manejados por el software aplicativo del sistema de tratamiento de datos personales:

El sistema aplicativo almacena la información de usuarios y contraseñas.

1. Administración de perfiles de usuario y contraseñas:

La Secretaría Académica y el coordinador de movilidad y servicios académicos pueden conceder o restringir a los perfiles de acuerdo a su rol.

2. Acceso remoto al sistema de tratamiento de datos personales:

A través de su usuario y contraseña, los usuarios pueden acceder de manera remota al sistema siempre y cuando tengan acceso concedido por secretaría académica o el coordinador del área.

a) ¿Requiere el administrador acceso remoto al equipo donde reside el sistema para realizar tareas de mantenimiento?
No.

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

1. Señalar si realiza respaldos

El sistema realiza respaldo diario de la información contenida en el mismo, el coordinador del área es responsable de guardar este respaldo en el equipo de cómputo de la sede.

2. El tipo de medios (por ejemplo: cintas magnéticas, discos duros, CD-ROM, entre otros) que utiliza para almacenar las copias de seguridad

Los respaldos se almacenan en los servidores de gmail.

3. Cómo y dónde archiva esos medios:

Se archivan en el perfil del usuario donde está almacenada la información.

4. Quién es el responsable de realizar estas operaciones (el área universitaria o un tercero).

Area universitaria.

IX. PLAN DE CONTINGENCIA

1. Presentar el plan de contingencia con el cual garantiza la continuidad de la operación del sistema o informar si no lo tiene, pero se encuentra desarrollándose.

Se cuenta con algunas medidas como las medidas de seguridad en los periodos de inactividad o mantenimiento, pero no se tiene desarrollado el plan de contingencia.

2. Si cuenta con plan de contingencia y lo ha implementado, deberá indicar si realiza pruebas de eficiencia de este.

No se cuenta con plan de contingencia.

3. Informar si cuenta con un sitio redundante (alterno) y señalar lo siguiente:

No aplica.

7. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

7.1. Herramientas y recursos para monitoreo de la protección de datos personales

SECRETARÍA ACADÉMICA		
Identificador único*	UNAM Chicago - Movilidad.	
(Nombre del sistema A4)*	Base de Datos de estudiantes de Servicio Social y Prácticas Profesionales	
Recurso*	**Descripción***	**Control***
Bitácora del sistema	Revisión aleatoria	El responsable de la administración técnica del sistema las revisa aleatoriamente o en caso de alguna anomalía CRAI en coordinación con UNAM Chicago

7.1. Programa de capacitación a los responsables de tratamiento de datos personales

SECRETARÍA ACADÉMICA			
Identificador único A4*	UNAM Chicago - Movilidad.		
(Nombre del sistema A4)*	Base de Datos de estudiantes de Servicio Social y Prácticas Profesionales		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Taller	Virtual por zoom	16/08/22 10am a 1 pm.	Staff UNAM Chicago Anual

7.2. Procedimiento para la revisión de las medidas de seguridad

SECRETARÍA ACADÉMICA		
Identificador único*	UNAM Chicago - Movilidad.	
(Nombre del sistema A4)*	Base de Datos de estudiantes de Servicio Social y Prácticas Profesionales	
Medida de seguridad*	**Procedimiento***	**Responsable***
Plan de respaldos de información.	Revisión y validación del historial de respaldos del sistema.	El responsable de realizar la revisión es el Ing. Jorge. Hernández, CRAI. La duración de la revisión es un día hábil.
Instalar y mantener actualizado el software antimalware.	Revisión y actualización de la versión del software antivirus y de la base de datos.	El responsable de realizar la revisión es el IT de UNAM Chicago. La duración de la revisión es un día hábil.

7.3. Resultados de la evaluación y pruebas a las medidas de seguridad

SECRETARÍA ACADÉMICA		
Identificador único*	UNAM Chicago - Movilidad.	
(Nombre del sistema A4)*	Base de Datos de estudiantes de Servicio Social y Prácticas Profesionales	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***
Respaldar la información.	Se cuenta con respaldos actualizados y protegidos de la información del sistema.	El responsable de realizar la revisión es el responsable del área.
Descargar, instalar y actualizar el software antimalware más reciente en los ordenadores.	El Software antivirus se encuentra instalado, y actualizado en su última versión.	El responsable de realizar la revisión es el IT de la UNAM Chicago.

7.4. Acciones para la corrección y actualización de las medidas de seguridad

SECRETARÍA ACADÉMICA		
Identificador único*	UNAM Chicago - Movilidad.	
(Nombre del sistema A4)*	Base de Datos de estudiantes de Servicio Social y Prácticas Profesionales	
Medida de seguridad*	**Acciones***	**Responsable***
Revisar las últimas actualizaciones del software de protección	Actualizar constantemente el software.	UNAM Chicago.
Cambio de contraseñas.	Cambiar las contraseñas de los usuarios actualizados de manera semestral.	UNAM Chicago

8. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

8.1. Programa de capacitación a los responsables de tratamiento de datos personales

SECRETARÍA ACADÉMICA			
Identificador único*	UNAM Chicago - Movilidad.		
(Nombre del sistema A4)*	Base de Datos de estudiantes de Servicio Social y Prácticas Profesionales		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Elaboración del Documento d Seguridad y Sistema de Gest de Seguridad de Datos Personales de las áreas universitarias.	Taller vía zoom	16/08/22 10am a 1 pm.	Staff UNAM Chicago Anual

8.2. Programa de difusión de la protección a los datos personales

SECRETARÍA ACADÉMICA			
Identificador único*	UNAM Chicago - Movilidad.		
(Nombre del sistema A4)*	Base de Datos de estudiantes de Servicio Social y Prácticas Profesionales		
Actividad*	**Descripción***	**Duración***	**Cobertura***
No aplica	No aplica	No aplica	No aplica

9. MEJORA CONTINUA

9.1. Actualización y mantenimiento de sistemas de información

SECRETARÍA ACADÉMICA			
Identificador único*	UNAM Chicago - Movilidad.		
(Nombre del sistema A4)*	Base de Datos de estudiantes de Servicio Social y Prácticas Profesionales		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Actualización del servicio web	Actualizar el servicio web de forma constante para evitar huecos de seguridad en el aplicativo.	2-4 hrs	Actualización del servicio web que usa el servidor.

9.2. Actualización y mantenimiento de equipo de cómputo

SECRETARÍA ACADÉMICA			
Identificador único*	UNAM Chicago - Movilidad.		
(Nombre del sistema A4)*	Base de Datos de estudiantes de Servicio Social y Prácticas Profesionales		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Actualización del antivirus del servidor Mantenimiento preventivo lógico	Actualización de versión del sistema operativo	4-6 horas	Actualización del sistema operativo, así como paquetes correspondientes para el correcto funcionamiento de este.
Actualización del antivirus del servidor Mantenimiento preventivo físico	Limpieza y verificación del correcto funcionamiento de los componentes del servidor	8-10 horas	Limpieza del servidor, pruebas de desempeño y de estado de memorias RAM, procesador, discos duros, para garantizar el correcto funcionamiento de éste.

9.3. Procesos para la conservación, preservación y respaldos de información

SECRETARÍA ACADÉMICA		
Identificador único*	UNAM Chicago - Movilidad.	
(Nombre del sistema A4)*	Base de Datos de estudiantes de Servicio Social y Prácticas Profesionales	
Proceso*	**Descripción***	**Responsable***
Respaldar la información en los equipos de cómputo de la sede.	Se realiza un respaldo completo de forma periódica y manual, donde se almacena la información respaldada en el disco duro del equipo de cómputo donde no se tiene acceso de manera remota.. .	Responsable del área.

9.4. Procesos de borrado seguro y disposición final de equipos y componentes informáticos

SECRETARÍA ACADÉMICA		
Identificador único*	UNAM Chicago - Movilidad.	
(Nombre del sistema A4)*	Base de Datos de estudiantes de Servicio Social y Prácticas Profesionales	
Proceso*	**Descripción***	**Responsable***
Se realiza un respaldo total de toda lai información almacenada en el equipo de cómputo a desechar. Posteriormente, se realiza un formateo total de la unidad para dejarla en estado de fabrica. Por último, se resguarda físicamente en la sede o se desecha el equipo.	A través del formateo general del ordenador, se realiza un respaldo de seguridad en una unidad USB o disco duro externo, se procede al borrado seguro de toda la información y se dispone del equipo de cómputo según su estado físico.	*IT de UNAM Chicago. Un proceso que dura 24 horas aproximadamente.*

10. PROCEDIMIENTO PARA LA CANCELACIÓN DE UN SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

A) DATOS DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES QUE SERÁ CANCELADO:

a) Base de Datos de estudiantes de Servicio Social y Prácticas Profesionales
b) Motivo de la cancelación

1. La Secretaría Académica deberá solicitar la cancelación por escrito al encargado del sistema explicando los motivos y tiempo que deberá permanecer disponible para consulta.

2. El responsable del sistema deberá realizar la suspensión de las contraseñas de acceso al sistema.

3. El responsable del sistema deberá notificar a la Secretaría Académica de las acciones realizadas para lograr la cancelación temporal del sistema.

4. Una vez transcurrida la temporalidad en que el sistema quedó bloqueado, el encargado del sistema iniciará la eliminación segura del mismo.

5. El responsable del sistema notificará a la Secretaría Académica de que el sistema ha sido cancelado

B) PLAZOS Y CONDICIONES PARA EL BLOQUEO DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

Señalar el periodo de bloqueo, considerando los plazos de prescripción para el ejercicio de algún derecho por parte de los titulares de conformidad con la normatividad de cada área universitaria. Asimismo, se debe señalar las condiciones y el procedimiento que se seguirá para realizar el bloqueo)

C) MEDIDAS DE SEGURIDAD PARA EL BLOQUEO Y POSTERIOR SUPRESIÓN DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES:

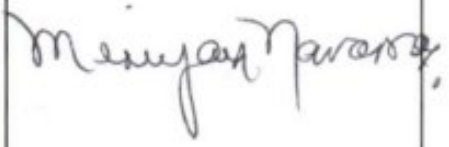
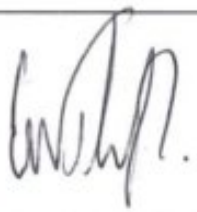
D) PROCEDIMIENTO PARA LA SUPRESIÓN DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

Una vez transcurrida la temporalidad en que el sistema quedó bloqueado, el encargado del sistema iniciará la eliminación segura del mismo.

E) MECANISMOS PARA LA SUPRESIÓN DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

El encargado del área, previo notificación a secretaría académica, le proporciona acceso al IT de UNAM Chicago para que pueda acceder al sistema y pueda modificarlo de manera directa.

APROBACIÓN DEL DOCUMENTO DE SEGURIDAD

		Nombre y firma de quienes revisaron el presente documento:
Responsables del desarrollo:	Mireya Navarro, delegada administrativa. (312) 573-1347 mnavarro@unam.mx Eréndira Sánchez, coordinadora de planeación y desarrollo. (312) 573-1347 erendira.sanchez@unam.mx Claudia Muñoz, coordinadora de enseñanza de español y cultura. (312) 573-1347 claudia.munoz@chicago.unam.mx Marco Antonio Fuentes, coordinador de movilidad, (312) 573-1347 marcofuentes@chicago.unam.mx	
Revisó:	Erika Erdely, secretaria académica, (312) 573-1347 erika@chicago.unam.mx	
Autorizó:	Guillermo Pulido, director, (312) 573-1347 gpulido@chicago.unam.mx	
Fecha de aprobación:	04/11/2022	
Fecha de actualización:	Primera versión: 03/11/2022	

UNAM

SAN ANTONIO

1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Servicios Escolares / Administración	
Identificador único*	UNAM San Antonio
(Nombre del sistema A1) *	**Sistema Escolar**
Datos personales (sensibles o no) contenidos en el sistema*:	Nombre, domicilio, teléfono celular, correo electrónico, firma electrónica, nacionalidad, edad, fecha de nacimiento, grado escolar, estatus migratorio.
Responsable*:	Servicios Escolares
Nombre*:	**Ligia Corral**
Cargo*:	**Student Affairs & Registrar - DSO**
Funciones*:	Registrar a los usuarios en el control de acceso
Obligaciones*:	Conocer la privacidad de los datos que se manejan y mantener el secreto de dicha información. Hacer uso de los datos únicamente para los fines para los que han sido recabados.
Identificador único*	UNAM San Antonio
(Nombre del sistema A2) *	**Sistema Jotform**
Datos personales (sensibles o no) contenidos en el sistema*:	Trayectoria educativa, Nombre, domicilio, teléfono celular, correo electrónico, firma electrónica, nacionalidad, edad, fecha de nacimiento, grado escolar, estatus migratorio, número de pasaporte, número de visa, nombres de dependientes.
Responsable*:	Servicios Escolares
Nombre*:	**Ligia Corral**
Cargo*:	**Student Affairs & Registrar - DSO**
Funciones*:	Registrar a los usuarios en el control de acceso
Obligaciones*:	Conocer la privacidad de los datos que se manejan y mantener el secreto de dicha información. Hacer uso de los datos únicamente para los fines para los que han sido recabados.
Identificador único*	UNAM San Antonio
(Nombre del sistema A3) *	**Sistemas Jotform, Sistema Escolar, Quickbooks**
Datos personales (sensibles o no) contenidos en el sistema*:	Trayectoria educativa, Nombre, domicilio, teléfono celular, correo electrónico, firma electrónica, nacionalidad, edad, fecha de nacimiento, grado escolar, estatus migratorio, número de pasaporte, número de visa, nombres de dependientes.
Responsable*:	IT
Nombre*:	**Orlando Gonzalez**
Cargo*:	**IT Coordinator**
Funciones*:	Dar mantenimiento al sistema aplicando actualizaciones operativas para garantizar el correcto funcionamiento de los sistemas y mantener respaldos.
Obligaciones*:	Proteger y mantener de forma segura y privada la información en general, así como los datos personales almacenados.

Identificador único*	UNAM San Antonio
(Nombre del sistema A4) *	**Quickbooks**
Datos personales (sensibles o no) contenidos en el sistema*:	Nombre, domicilio, teléfono celular, correo electrónico.
Responsable*:	Departamento de Administración
Nombre*:	**Antonio Huereca**
Cargo*:	**Business Manager**
Funciones*:	Autorizar y supervisar pagos a proveedores, atender las necesidades administrativas con la finalidad de brindar apoyo administrativo a los responsables de procesos de registro en las diferentes áreas de la institución.
Obligaciones*:	Procurar la protección de los datos personales contenidos en el sistema.
	Usuarios:
(Nombre del Usuario A4.1*)	**Laura Carreón**
Cargo*:	**Executive Assistant to the Director**
Funciones*:	Registrar a los usuarios en el control de acceso
Obligaciones*:	Procurar la protección de los datos personales contenidos en el sistema
Identificador único*	UNAM San Antonio
(Nombre del sistema A5) *	**Sistema Exel**
Datos personales (sensibles o no) contenidos en el sistema*:	Nombre, domicilio, teléfono celular, correo electrónico, firma electrónica, nacionalidad, edad, fecha de nacimiento, grado escolar, estatus migratorio, lugar de residencia, domicilio trabajo.
Responsable*:	Administración
Nombre*:	**Antonio Huereca**
Cargo*:	**Business Manager**
Funciones*:	Registrar a los usuarios en el control de acceso
Obligaciones*:	Conocer la privacidad de los datos que se manejan y mantener el secreto de dicha información. Hacer uso de los datos únicamente para los fines para los que han sido recabados.
	Usuarios:
(Nombre del Usuario A5.1*)	**Laura Carreón**
Cargo*:	**Executive Assistant to the Director**
Funciones*:	Registrar a los usuarios en el control de acceso
Obligaciones*:	Conocer la privacidad de los datos que se manejan y mantener el secreto de dicha información. Hacer uso de los datos únicamente para los fines para los que han sido recabados.

2. ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Servicios Escolares / Administración	
Identificador único¨*	UNAM San Antonio
(Nombre del sistema A1*)	**Sistema Escolar**
Tipo de soporte:*	Electrónico
Descripción:*	Base de datos
Características del lugar donde se resguardan los soportes:*	Información reservada
(Nombre del sistema A2*)	**Sistema Jotform**
Tipo de soporte:*	Electrónico
Descripción:*	Base de datos
Características del lugar donde se resguardan los soporte:*	Información reservada
(Nombre del sistema A4*)	**Sistema Quickbooks**
Tipo de soporte:*	Electrónico
Descripción:*	Base de datos
Características del lugar donde se resguardan los soporte:*	Información reservada
(Nombre del sistema A5*)	**Sistema Exel**
Tipo de soporte*:	El sistema se encuentra en soporte físico
Descripción*:	Expedientes
Características del lugar donde se resguardan los soportes*:	Oficina con ventilación artificial, puerta de acceso de madera y chapa, aislada de humedad, con archiveros y libreros que permiten la conservación adecuada de los documentos.

3. ANÁLISIS DE RIESGOS

Servicios Escolares / Administración	
Identificador único*	UNAM San Antonio
(Nombre del sistema) * -Sistema Escolar A1 -Sistema Jotform A2 -Sistema Quickbooks A4 -Sistema Excel A5	***INFORMACIÓN RESERVADA***

4. ANÁLISIS DE BRECHA

Servicios Escolares / Administración	
Identificador único*	UNAM San Antonio
(Nombre del sistema) * -Sistema Escolar A1 -Sistema Jotform A2 -Sistema Quickbooks A4 -Sistema Excel A5	***INFORMACIÓN RESERVADA***

5. PLAN DE TRABAJO

Servicios Escolares / Administración	
Identificador único*	*UNAM San Antonio*
(Nombre del sistema) * -Sistema Escolar A1 -Sistema Jotform A2 -Sistema Quickbooks A4 -Sistema Excel A5	***INFORMACIÓN RESERVADA***

6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

I. TRANSFERENCIAS DE DATOS PERSONALES

Servicios Escolares / Administración	
Identificador único*	*UNAM San Antonio*
(Nombre del sistema A1/2)*	**Sistema Escolar / Quickbooks**
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:[1]	No se realizan transferencias de datos personales mediante el traslado de soportes físicos.
Transferencias mediante el traslado de soportes electrónicos:	No se realizan transferencias de datos personales mediante el traslado de soportes electrónicos.
Transferencias mediante el traslado sobre redes electrónicas:	No se realizan transferencias de datos personales mediante el traslado sobre redes electrónicas

II. RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS

1. Señalar las medidas de seguridad que ha implementado el área universitaria para el resguardo de los soportes físicos del sistema de manera que evite la alteración, pérdida o acceso no autorizado a los mismos.

- **Oficina con ventilación artificial, puerta de acceso de madera y chapa, aislada de humedad, con archiveros y libreros que permiten la conservación adecuada de los documentos.**
- **Respaldo de data de los sistemas**

2. Señalar en un listado las personas (nombre, cargo, funciones y obligaciones) que tienen acceso a los soportes físicos del sistema.[3]

-Antonio Huereca – Business Manager
-Ligia Corral – Student Services & Registar
-Laura Carreon – Executive Assistant to the Director
-Orlando González – IT Coordinator

III. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

La información correspondiente a bitácoras (acceso y operación) se encuentra en el archivo .log almacenado en ubicación del sistema escolar.

1. Los datos que se registran en las bitácoras:

a) Quién accede a los datos personales, fecha y hora en la que se realiza el acceso o se intenta el mismo, propósito del acceso, así como fecha y hora de salida;
b) Para soportes físicos: Número o clave del expediente utilizado, y
c) Para soportes electrónicos: Operaciones o acciones llevadas a cabo y registros utilizados de la base de datos.

1. Si las bitácoras están en soporte físico o en soporte electrónico
2. Lugar dónde almacena las bitácoras y por cuánto tiempo;
3. La manera en que asegura la integridad de las bitácoras, y
4. Respecto del análisis de las bitácoras:

a) Quién es el responsable de analizarlas (si es el área universitaria o si es un tercero) y cada cuándo las analiza, y

b) Para el caso de que las bitácoras estén en soporte electrónico: las herramientas de análisis utilizadas.

IV. REGISTRO DE INCIDENTES:

Describir el procedimiento de atención de incidentes que tiene implementado el área universitaria y especificar si lleva registro de los incidentes relativos a soportes físicos, como lo son la pérdida o alteración no autorizada de expedientes, y para el caso de soportes electrónicos, ofrecer detalles sobre el registro de incidentes en el cual consigne los procedimientos realizados para la recuperación de los datos o para permitir la disponibilidad del proceso.

N/A

V. ACCESO A LAS INSTALACIONES

1. Seguridad perimetral exterior (las instalaciones del área universitaria):

Para las personas que acceden a sus instalaciones:

a) ¿Cómo las identifica? **N/A**
b) ¿Cómo las autentifica? **N/A**
c) ¿Cómo les autoriza el acceso? **N/A**

Seguridad perimetral interior (oficina, almacén o bodega para soportes físicos, centro de datos

Para las personas que acceden a dichos espacios interiores:

a) ¿Cómo las identifica? **N/A**
b) ¿Cómo las autentifica? **N/A**
c) ¿Cómo les autoriza el acceso? **N/A**

VI. ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

En este apartado se deberá establecer un mecanismo o procedimiento institucional para la actualización de la información personal contenida en el sistema, en donde se establezca la frecuencia con la que se efectúa y la forma en que se está solicitando al titular acreditar de manera idónea sus requerimientos de rectificación de datos inexactos).

Las medidas de seguridad previstas a continuación en los incisos VII al IX, sólo aplican para soportes electrónicos

VII. PERFILES DE USUARIO Y CONTRASEÑAS

En este rubro el área universitaria deberá describir el esquema de perfiles de usuario y contraseñas que tiene implementado para control de acceso mediante una red electrónica.

-Modelo de control de acceso (alguno de los siguientes):

a) ¿Es obligatorio (etiquetas para objetos y acreditación para sujetos)?
b) ¿Es discrecional (matriz de control de acceso)?
c) ¿Está basado en roles (perfiles) o grupos? **Está basado en roles**
d) ¿Está basado en reglas?

- Perfiles de usuario y contraseñas en el sistema operativo de red:
  a) ¿Cuenta con un sistema operativo de red instalado en sus equipos? **Si**
  b) ¿Proporciona dicho sistema operativo un manejo riguroso de perfiles de usuario y contraseñas? **SI**
  c) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena? **SI**

- Perfiles de usuario y contraseñas manejados por el software aplicativo del sistema de tratamiento de datos personales:
  a) ¿Ofrece dicho software un manejo riguroso de perfiles de usuario y contraseñas? **SI**
  b) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena? **SI**

- Administración de perfiles de usuario y contraseñas:
  a) ¿Quién da de alta nuevos perfiles? **Los alumnos y usuarios pueden darse de alta con el fin de registro para eventos académicos y culturales.**
  b) ¿Quién autoriza la creación de nuevos perfiles? **El sistema automáticamente captura la información.**
  c) ¿Se lleva registro de la creación de nuevos perfiles? **Sí, el mismo sistema lleva el registro de los nuevos usuarios**

- Acceso remoto al sistema de tratamiento de datos personales:

a) ¿Requieren los usuarios acceso remoto al equipo de cómputo que por lo general utilizan para trabajar con el sistema? **No, cada usuario puede acceder al sistema desde cualquier equipo con conexión a internet.**

b) ¿Requiere el administrador acceso remoto al equipo donde reside el sistema para realizar tareas de mantenimiento? **Sí**

c) ¿Cómo se evita el acceso remoto no autorizado? **Únicamente el administrador de sistemas tiene el acceso y se cuenta con mecanismos como el captcha y conexiones especiales.**

VIII. ROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

- Señalar si realiza respaldos
  - **a)** Completos_X_, diferenciales o incrementales
  - **b)** De forma automática _X o Manual
  - **c)** Periodicidad con que los realiza: _diario
  - **d)** El tipo de medios (por ejemplo: cintas magnéticas, discos duros, CD-ROM, entre otros) que utiliza para almacenar las copias de seguridad: Disco Duro externo
  - **e)** Cómo y dónde archiva esos medios, y local
  - **f)** Quién es el responsable de realizar estas operaciones (el área universitaria o un tercero). Área Universitaria

IX. PLAN DE CONTINGENCIA

a) Presentar el plan de contingencia con el cual garantiza la continuidad de la operación del sistema o informar si no lo tiene, pero se encuentra desarrollándolo. **N/A**

Continuar los mismos pasos con el siguiente SISTEMA A2. (Nombre del sistema A2)[8], B1. (Nombre del sistema B1), etc. N/A

7. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

7.1. Herramientas y recursos para monitoreo de la protección de datos personales

Servicios Escolares / Administración	
Identificador único*	*UNAM San Antonio*
(Nombre del sistema) * -Sistema Escolar A1 -Sistema Jotform A2 -Sistema Quickbooks A4 -Sistema Excel A5	***Firewall / INFORMACIÓN RESERVADA***

7.2. Procedimiento para la revisión de las medidas de seguridad

Servicios Escolares / Administración	
Identificador único*	*UNAM San Antonio*
(Nombre del sistema) * -Sistema Escolar A1 -Sistema Jotform A2 -Sistema Quickbooks A4 -Sistema Excel A5	***Departamento IT / INFORMACIÓN RESERVADA***

i) El **sitio alterno frío** cuenta con un ambiente mínimo de infraestructura y no cuenta con el equipo. Este tipo de sitios alternos es el menos costoso, pero supone demora de algunos días para restablecer operaciones.

7.3. Resultados de la evaluación y pruebas a las medidas de seguridad

Servicios Escolares / Administración	
Identificador único*	*UNAM San Antonio*
(Nombre del sistema) * -Sistema Escolar A1 -Sistema Jotform A2 -Sistema Quickbooks A4 -Sistema Excel A5	***Departamento IT / INFORMACIÓN RESERVADA***

7.4. Acciones para la corrección y actualización de las medidas de seguridad

Servicios Escolares / Administración	
Identificador único*	*UNAM San Antonio*
(Nombre del sistema) * -Sistema Escolar A1 -Sistema Jotform A2 -Sistema Quickbooks A4 -Sistema Excel A5	***Departamento IT / INFORMACIÓN RESERVADA***

8. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

8.1. Programa de capacitación a los responsables de tratamiento de datos personales

Servicios Escolares / Administración			
Identificador único*	*UNAM San Antonio*		
Nombre del sistema A1 / A4	**Sistema Escolar / Sistema Quickbooks**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Capacitación para la Protección de Datos Personales	Curso presencial c/videos informativos	2 hrs por día, 2 veces por año	Personal que maneja datos personales y responsable de IT de la información. Actualizaciones 2 veces por año con frecuencia por año.

8.2. Programa de difusión de la protección a los datos personales

N/A

9. MEJORA CONTINUA

9.1. Actualización y mantenimiento de sistemas de información

Servicios Escolares / Administración			
Identificador único*	*UNAM San Antonio*		
Nombre del sistema A1/A4	**Sistema Escolar / Quickbooks**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Actualización de los sistemas	Updates vigentes	Depende del mismo software	Total

9.2. Actualización y mantenimiento de equipo de cómputo

Servicios Escolares / Administración			
Identificador único*	*UNAM San Antonio*		
Nombre del sistema A1 / A4	**Sistema Escolar / Quickbooks**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Actualización de los sistemas	Updates vigentes	Depende del mismo software	Total y/o parcial dependiendo del update del software.

9.3. Procesos para la conservación, preservación y respaldos de información

Servicios Escolares / Administración		
Identificador único*	*UNAM San Antonio*	
Nombre del sistema A1 / A4	**Sistema Escolar / Quickbooks**	
Proceso*	**Descripción***	**Responsable***
Respaldo de la base de datos	Respaldo en disco externo	IT Department

9.4. Procesos de borrado seguro y disposición final de equipos y componentes informáticos

N/A

10. PROCEDIMIENTO PARA LA CANCELACIÓN DE UN SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

N/A

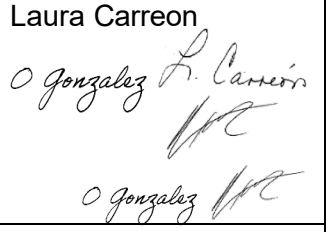
A) DATOS DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES QUE SERÁ CANCELADO: **N/A**

B) PLAZOS Y CONDICIONES PARA EL BLOQUEO DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES:[9] **N/A**

C) PROCEDIMIENTO PARA LA SUPRESIÓN DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES **N/A**

D) MECANISMOS PARA LA SUPRESIÓN DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES **N/A**

11. APROBACIÓN DEL DOCUMENTO DE SEGURIDAD

		Nombre y firma de quienes revisaron el presente documento:
Responsable del desarrollo:	IT Department / Director's office	Orlando González / Laura Carreon 
Revisó:	Departamento Administrativo	Antonio Huereca
Autorizó:	Departamento IT / Administrativo	Orlando González / Antonio Huereca
Fecha de aprobación:		11/4/2022
Fecha de actualización:		11/4/2022

UNAM

LOS ÁNGELES

SISTEMA REGISTRO ALUMNOS CURSOS ESPAÑOL

1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

UNAM - Los Ángeles (Centro de Estudios Mexicanos)	
Identificador único*	**UNAM-LA Spanish Course Registration**
(Nombre del sistema A1) *	**Registro alumnos cursos español**
Datos personales (sensibles o no) contenidos en el sistema*:	Correo electrónico, tipo de registro (nuevo o reingreso), nombre, apellido, teléfono, dirección (número, calle, suite, ciudad, estado, país, código postal), fecha de nacimiento, género, nacionalidad, estudios realizados.
Responsable: *	
Nombre*:	Alfredo Fernández Carmona
Cargo*:	Coordinador de relaciones y gestión
Funciones*:	Administrar acceso a responsables y usuarios. Actualizar campos de datos personales, cuando se requiera.
Obligaciones*:	No difundir información de los datos personales. Resguardar el sistema.
	Encargados:
(Nombre del Encargado 1*)	Fernando Pérez Rodríguez
Cargo*:	Coordinador de Español
Funciones*:	Dar seguimiento a los registros de nuevos alumnos y alumnos de reingreso para asignar grupo.
Obligaciones*:	Mantener actualizado el estatus de los registros
	Usuarios:
(Nombre del Usuario 1*)	Fernando Pérez Rodríguez
Cargo*:	Coordinador de español
Funciones*:	Preparar información para reportes de matriz de indicadores trimestralmente
Obligaciones*:	No modificar información de los registros de alumnos inscritos.

2. ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

UNAM - Los Ángeles (Centro de Estudios Mexicanos)	
Identificador único¨*	**UNAM-LA Spanish Course Registration**
(Nombre del sistema A1*)	**Registro alumnos cursos español**
Tipo de soporte: *	Soporte Electrónico
Descripción: *	Base de Datos
Características del lugar donde se resguardan los soportes: *	Alojamiento en la nube privada de Google Drive

3. ANÁLISIS DE RIESGOS

UNAM - Los Ángeles (Centro de Estudios Mexicanos)		
Identificador único*	**UNAM-LA Spanish Course Registration**	
(Nombre del sistema A1) *	**Registro alumnos cursos español**	
Riesgo*	**Impacto***	**Mitigación***
No se cuenta soporte físico	Pérdida de la información en caso de no poder acceder a la nube que aloja la información.	Realizar respaldo en soporte físico.

4. ANÁLISIS DE BRECHA

UNAM - Los Ángeles (Centro de Estudios Mexicanos)		
Identificador único*	**UNAM-LA Spanish Course Registration**	
(Nombre del sistema A1) *	**Registro alumnos cursos español**	
Medida de seguridad actual*	**Medida de seguridad necesaria***	**Acciones para remediación***
El acceso al sistema solo para responsable, encargado y usuario mediante correo electrónico y contraseña asignados por la G Suite for Education.	Establecer periodos para cambio de contraseñas.	Definir periodicidad para el cambio de contraseñas.

5. PLAN DE TRABAJO

UNAM - Los Ángeles (Centro de Estudios Mexicanos)			
Identificador único*	**UNAM-LA Spanish Course Registration**		
(Nombre del sistema A1) *	**Registro alumnos cursos español**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Respaldo en soporte físico	Realizar respaldo en un medio de almacenamiento físico del soporte electrónico.	Realizar respaldo mensual.	Respaldo del total de sistema de Registro alumnos cursos español

6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

I. TRANSFERENCIAS DE DATOS PERSONALES

UNAM - Los Ángeles (Centro de Estudios Mexicanos)	
Identificador único*	**UNAM-LA Spanish Course Registration**
(Nombre del sistema A1)*	**Registro alumnos cursos español**
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	No se realiza transferencia de datos personales mediante el traslado de soportes físicos.
Transferencias mediante el traslado de soportes electrónicos:	No se realiza transferencia de datos personales mediante el traslado de soportes electrónicos.
Transferencias mediante el traslado sobre redes electrónicas:	No se realiza transferencia de datos personales mediante el traslado sobre redes electrónicas.

II. RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS

NO SE REALIZAN RESGURADOS CON SOPORTES FÍSICOS

i. Señalar las medidas de seguridad que ha implementado el área universitaria para el resguardo de los soportes físicos del sistema de manera que evite la alteración, pérdida o acceso no autorizado a los mismos.
ii. Señalar en un listado las personas (nombre, cargo, funciones y obligaciones) que tienen acceso a los soportes físicos del sistema.

III. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

LA INFORMACIÓN DE ACCESO Y OPERACIÓN SE EN CUENTRA EN EL PROPIO SISTEMA COMO PANEL DE ACTIVIDAD

IV. REGISTRO DE INCIDENTES:

NO SE CUENTA CON UN PROCEDIMIENTO DE ATENCIÓN A INCIDENTES

Describir el procedimiento de atención de incidentes que tiene implementado el área universitaria y especificar si lleva registro de los incidentes relativos a soportes físicos, como lo son la pérdida o alteración no autorizada de expedientes, y para el caso de soportes electrónicos, ofrecer detalles sobre el registro de incidentes en el cual consigne los procedimientos realizados para la recuperación de los datos o para permitir la disponibilidad del proceso.

V. ACCESO A LAS INSTALACIONES

1. **Seguridad perimetral exterior** (las instalaciones del área universitaria):

¿Qué medidas ha implementado para controlar el acceso de personas a sus instalaciones? Por ejemplo, se espera que describa si cuenta con uno o más puntos de control de acceso y quienes los operan, si tiene vigilancia las 24 horas, si ha levantado bardas o cercas, si existe un sistema de tratamiento de datos personales de videovigilancia, entre otras posibles medidas.

Para las personas que acceden a sus instalaciones:

b) ¿Cómo las identifica? No se cuenta con mecanismos de identificación.
c) ¿Cómo las autentifica? No se cuenta con mecanismos de autentificación.
d) ¿Cómo les autoriza el acceso? No se cuenta con mecanismos de control de acceso.

2. **Seguridad perimetral interior** (oficina, almacén o bodega para soportes físicos, centro de datos para soportes electrónicos):

¿Qué medidas de seguridad ha implementado para controlar el acceso a los espacios donde almacena los soportes físicos o electrónicos del sistema? Por ejemplo, se espera que precise el tipo de puertas y cerraduras instaladas, si tiene instalados controles biométricos, si administra la asignación de llaves y/o claves de acceso para abrir puertas y/o estantería, si cuenta con vigilancia las 24 horas, si hay un sistema de tratamiento de datos personales de videovigilancia, entre otras medidas.

Para las personas que acceden a dichos espacios interiores:

1. ¿Cómo las identifica? Solo el personal tiene acceso.
2. ¿Cómo las autentifica? Con identificación oficial.
3. ¿Cómo les autoriza el acceso? Se les asigna llave para ingreso a la oficina.

VI.ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

En este apartado se deberá establecer un mecanismo o procedimiento institucional para la actualización de la información personal contenida en el sistema, en donde se establezca la frecuencia con la que se efectúa y la forma en que se está solicitando al titular acreditar de manera idónea sus requerimientos de rectificación de datos inexactos).

No se cuenta con un apartado de actualización de información en el sistema, en caso necesario los datos se ingresan nuevamente.

Las medidas de seguridad previstas a continuación en los incisos VII al IX, sólo aplican para soportes electrónicos

VII. PERFILES DE USUARIO Y CONTRASEÑAS

En este rubro el área universitaria deberá describir el esquema de perfiles de usuario y contraseñas que tiene implementado para control de acceso mediante una red electrónica.

1. Modelo de control de acceso (alguno de los siguientes):

a) ¿Es obligatorio (etiquetas para objetos y acreditación para sujetos)? No
b) ¿Es discrecional (matriz de control de acceso)? No
c) ¿Está basado en roles (perfiles) o grupos? Si
d) ¿Está basado en reglas? No

2. Perfiles de usuario y contraseñas en el sistema operativo de red:

a) ¿Cuenta con un sistema operativo de red instalado en sus equipos? Si
b) ¿Proporciona dicho sistema operativo un manejo riguroso de perfiles de usuario y contraseñas? Si
c) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena? Si

3. Perfiles de usuario y contraseñas manejados por el software aplicativo del sistema de tratamiento de datos personales:

a) ¿Ofrece dicho software un manejo riguroso de perfiles de usuario y contraseñas? Si
b) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena? Solo las contraseñas.

4. Administración de perfiles de usuario y contraseñas:

a) ¿Quién da de alta nuevos perfiles? Delegado Administrativo.
b) ¿Quién autoriza la creación de nuevos perfiles? Delegado Administrativo
c) ¿Se lleva registro de la creación de nuevos perfiles? Si, en el mismo sistema.

5. Acceso remoto al sistema de tratamiento de datos personales:

a) ¿Requieren los usuarios acceso remoto al equipo de cómputo que por lo general utilizan para trabajar con el sistema? No, cada usuario puede acceder al sistema desde cualquier equipo con conexión a internet.

b) ¿Requiere el administrador acceso remoto al equipo donde reside el sistema para realizar tareas de mantenimiento? No

c) ¿Cómo se evita el acceso remoto no autorizado? El sistema no se aloja en un equipo, por lo que no habría acceso remoto a dicho equipo.

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

1. Señalar si realiza respaldos

1. Completos_X, diferenciales ___ o incrementales___;
2. De forma automática ____ o Manual __X___,
3. Periodicidad con que los realiza: _Anual_____

2. El tipo de medios (por ejemplo: cintas magnéticas, discos duros, CD-ROM, entre otros) que utiliza para almacenar las copias de seguridad; Disco duro

3. Cómo y dónde archiva esos medios, Se archiva en archivero bajo llave.

4. Quién es el responsable de realizar estas operaciones (el área universitaria o un tercero). El área universitaria.

IX. PLAN DE CONTINGENCIA

NO SE CUENTA CON UN PLAN DE CONTIGENCIA NI EN DESARROLLO.

1. Presentar el plan de contingencia con el cual garantiza la continuidad de la operación del sistema o informar si no lo tiene, pero se encuentra desarrollándolo.

2. Si cuenta con plan de contingencia y lo ha implementado, deberá indicar si realiza pruebas de eficiencia de este.

3. Informar si cuenta con un sitio redundante (alterno) y señalar lo siguiente:

a) El tipo de sitio (caliente, tibio o frío);

b) Si el sitio es propio o subcontratado con un tercero;

c) Los procedimientos, el equipo y el personal que designa para poner en marcha tal sitio y

d) Tiempo que le lleva poner en marcha el sitio, según las pruebas de eficiencia.

7. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

7.1. Herramientas y recursos para monitoreo de la protección de datos personales

UNAM - Los Ángeles (Centro de Estudios Mexicanos)		
Identificador único*	**UNAM-LA Spanish Course Registration**	
(Nombre del sistema A1)*	**Registro alumnos cursos español**	
Recurso*	**Descripción***	**Control***
Panel de actividad	Revisión aleatoria	Revisión de manera regular para supervisar el uso del sistema e identificar un posible uso inusual. Responsable: Alfredo Fernández Carmona

7.2. Procedimiento para la revisión de las medidas de seguridad

UNAM - Los Ángeles (Centro de Estudios Mexicanos)		
Identificador único*	**UNAM-LA Spanish Course Registration**	
(Nombre del sistema A1)*	**Registro alumnos cursos español**	
Medida de seguridad*	**Procedimiento***	**Responsable***
Principio del menor privilegio	Revisión de configuración de las cuentas de usuarios del sistema	Responsable de la revisión Alfredo Fernández Carmona. Duración de la revisión un día hábil.
Revisión de respaldos de la información	Revisar realización y ubicación de los respaldos realizados	Responsable de la revisión Alfredo Fernández Carmona Duración de la revisión un día hábil.

7.3. Resultados de la evaluación y pruebas a las medidas de seguridad

UNAM - Los Ángeles (Centro de Estudios Mexicanos)		
Identificador único*	**UNAM-LA Spanish Course Registration**	
(Nombre del sistema A1)*	**Registro alumnos cursos español**	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***
Principio del menor privilegio	Se encontró que todas las cuentas de usuarios del sistema cuentan con los privilegios correspondientes.	Responsable de realizar la revisión Alfredo Fernández Carmona Revisión realizada el 2 de noviembre de 2022.
Revisión de respaldos de la información	Se cuentan con respaldo realizados y en la ubicación correspondiente.	Responsable de realizar la revisión Alfredo Fernández Carmona Revisión realizada el 2 de noviembre de 2022.

7.4. Acciones para la corrección y actualización de las medidas de seguridad

UNAM - Los Ángeles (Centro de Estudios Mexicanos)		
Identificador único*	**UNAM-LA Spanish Course Registration**	
(Nombre del sistema A1)*	**Registro alumnos cursos español**	
Medida de seguridad*	**Acciones***	**Responsable***
Programa anual para evaluar medidas de seguridad.	Se revisaron las medidas implantadas. No se requirieron medidas correctivas.	Responsable de las acciones Alfredo Fernández Carmona. Fecha de conclusión de 02 de noviembre de 2022.

8. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

8.1. Programa de capacitación a los responsables de tratamiento de datos personales

UNAM - Los Ángeles (Centro de Estudios Mexicanos)			
Identificador único*	**UNAM-LA Spanish Course Registration**		
(Nombre del sistema A1)*	**Registro alumnos cursos español**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Programa de capacitación que se relaciona con las medidas de seguridad técnica para la protección de datos personales en posesión de la UNAM, elaborado por DGETIC	Cursos en video que contribuyen a la formación y capacitación del personal a cargo de la protección de los datos personales en la UNAM en las entidades y dependencias	fecha de inicio 01 de diciembre de 2022 fecha de término 31 de enero de 2023	Responsable del sistema. Sin Vigencia. Sin frecuencia de actualización.

8.2. Programa de difusión de la protección a los datos personales

UNAM - Los Ángeles (Centro de Estudios Mexicanos)			
Identificador único*	**UNAM-LA Spanish Course Registration**		
(Nombre del sistema A1)*	**Registro alumnos cursos español**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
No se cuenta con un programa de difusión de la protección de datos personales.			

9. MEJORA CONTINUA

9.1. Actualización y mantenimiento de sistemas de información

UNAM - Los Ángeles (Centro de Estudios Mexicanos)			
Identificador único*	**UNAM-LA Spanish Course Registration**		
(Nombre del sistema A1)*	**Registro alumnos cursos español**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
N/A	N/A	N/A	N/A

9.2. Actualización y mantenimiento de equipo de cómputo

UNAM - Los Ángeles (Centro de Estudios Mexicanos)			
Identificador único*	**UNAM-LA Spanish Course Registration**		
(Nombre del sistema A1)*	**Registro alumnos cursos español**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Mantenimiento preventivo	Realizar el mantenimiento preventivo del equipo de cómputo tanto a nivel hardware como software para su funcionamiento óptimo.	1 vez por año	Equipos de cómputo de los usuarios del sistema.

9.3. Procesos para la conservación, preservación y respaldos de información

UNAM - Los Ángeles (Centro de Estudios Mexicanos)		
Identificador único*	**UNAM-LA Spanish Course Registration**	
(Nombre del sistema A1)*	**Registro alumnos cursos español**	
Proceso*	**Descripción***	**Responsable***
Respaldos periódicos de información	De manera anual se genera una copia de todos los archivos del sistema en un disco duro externo	Responsable de realizar respaldo Alfredo Fernández Carmona. Se lleva a cabo en 1 día hábil.

Por el momento no se cuenta con procesos de conservación y preservación de la información distintos a la generación de respaldos informáticos.

9.4. Procesos de borrado seguro y disposición final de equipos y componentes informáticos

UNAM - Los Ángeles (Centro de Estudios Mexicanos)		
Identificador único*	**UNAM-LA Spanish Course Registration**	
(Nombre del sistema A1)*	**Registro alumnos cursos español**	
Proceso*	**Descripción***	**Responsable***
Borrado seguro de información	Borrado seguro de información Con base en la circular DGTIC/003/2017, utilizando la herramienta de borrado seguro SDelete.	Responsable del proceso de borrado seguro Alfredo Fernández Carmona Tiempo máximo de ejecución 1 día hábil.

El sistema no se aloja en equipos informáticos, por lo que no aplica el proceso de disposición final de equipos.

10. PROCEDIMIENTO PARA LA CANCELACIÓN DE UN SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

1. Titular de la sede deberá solicitar la cancelación por escrito al encargado del sistema explicando los motivos y tiempo que deberá permanecer disponible para consulta.
2. El responsable del sistema deberá realizar la suspensión de las credenciales de acceso al sistema o en su caso, bloquear el apartado inicio de sesión del mismo.
3. El responsable del sistema deberá notificar al Titilar de la sede de las acciones realizadas para lograr la cancelación temporal del sistema.
4. Una vez transcurrida la temporalidad en que el sistema quedó bloqueado, el encargado del sistema iniciará la eliminación segura del mismo siguiendo el procedimiento establecido de Borrado seguro.
5. El responsable del sistema notificará al Titular de la sede de que el sistema ha sido cancelado.

Así mismo en el momento de la cancelación del sistema se deberán definir los siguientes puntos:

A) DATOS DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES QUE SERÁ CANCELADO:

a) Denominación
b) Motivo de la cancelación

B) PLAZOS Y CONDICIONES PARA EL BLOQUEO DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES:
(Señalar el periodo de bloqueo, considerando los plazos de prescripción para el ejercicio de algún derecho por parte de los titulares de conformidad con la normatividad de cada área universitaria. Asimismo, se debe señalar las condiciones y el procedimiento que se seguirá para realizar el bloqueo)

C) MEDIDAS DE SEGURIDAD PARA EL BLOQUEO Y POSTERIOR SUPRESIÓN DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES:
D) PROCEDIMIENTO PARA LA SUPRESIÓN DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES
(Describir el procedimiento para suprimir el sistema, una vez cumplido el plazo de bloqueo)

E) MECANISMOS PARA LA SUPRESIÓN DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

(Describir las técnicas para la eliminación física del sistema)

SISTEMA REGISTRO ALUMNOS CURSOS INGLÉS

1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

UNAM - Los Ángeles (Centro de Estudios Mexicanos)	
Identificador único*	**Registro a inglés en línea (Zlingo, TOEFL, Pronunciación)**
(Nombre del sistema A2) *	**Registro alumnos cursos inglés**
Datos personales (sensibles o no) contenidos en el sistema*:	Correo electrónico, nombre, apellido, fecha de nacimiento, género, país de origen, dirección (número, calle, suite, ciudad, estado, país, código postal), teléfono, nivel de estudios alcanzados.
Responsable: *	
Nombre*:	Alfredo Fernández Carmona
Cargo*:	Coordinador de relaciones y gestión
Funciones*:	Administrar acceso a responsables y usuarios. Actualizar campos de datos personales, cuando se requiera.
Obligaciones*:	No difundir información de los datos personales. Resguardar el sistema.
	Encargados:
(Nombre del Encargado 1*)	Vicente Ibarra Vázquez
Cargo*:	Asistente académico/administrativo
Funciones*:	Dar seguimiento a los registros de nuevos alumnos y alumnos de reingreso para asignar grupo.
Obligaciones*:	Mantener actualizado el estatus de los registros
	Usuarios:
(Nombre del Usuario 1*)	Vicente Ibarra Vázquez
Cargo*:	Asistente académico/administrativo
Funciones*:	Preparar información para reportes de matriz de indicadores trimestralmente
Obligaciones*:	No modificar información de los registros de alumnos inscritos.

2. ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

UNAM - Los Ángeles (Centro de Estudios Mexicanos)	
Identificador único¨*	**Registro a inglés en línea (Zlingo, TOEFL, Pronunciación)**
(Nombre del sistema A2*)	**Registro alumnos cursos inglés**
Tipo de soporte: *	Soporte Electrónico
Descripción: *	Base de Datos
Características del lugar donde se resguardan los soportes: *	Alojamiento en la nube privada de Google Drive

3. ANÁLISIS DE RIESGOS

UNAM - Los Ángeles (Centro de Estudios Mexicanos)		
Identificador único*	**Registro a inglés en línea (Zlingo, TOEFL, Pronunciación)**	
(Nombre del sistema A2) *	**Registro alumnos cursos inglés**	
Riesgo*	**Impacto***	**Mitigación***
No se cuenta soporte físico	Pérdida de la información en caso de no poder acceder a la nube que aloja la información.	Realizar respaldo en soporte físico.

4. ANÁLISIS DE BRECHA

UNAM - Los Ángeles (Centro de Estudios Mexicanos)		
Identificador único*	**Registro a inglés en línea (Zlingo, TOEFL, Pronunciación)**	
(Nombre del sistema A2) *	**Registro alumnos cursos inglés**	
Medida de seguridad actual*	**Medida de seguridad necesaria***	**Acciones para remediación***
El acceso al sistema solo para responsable, encargado y usuario mediante correo electrónico y contraseña asignados por la G Suite for Education.	Establecer periodos para cambio de contraseñas.	Definir periodicidad para el cambio de contraseñas.

5. PLAN DE TRABAJO

UNAM - Los Ángeles (Centro de Estudios Mexicanos)			
Identificador único*	**Registro a inglés en línea (Zlingo, TOEFL, Pronunciación)**		
(Nombre del sistema A2) *	**Registro alumnos cursos inglés**		
Actividad*	**Descripción***	**Duración***	**Cobertura ***
Respaldo en soporte físico	Realizar respaldo en un medio de almacenamiento físico del soporte electrónico.	Realizar respaldo mensual.	Respaldo del total de sistema de Registro alumnos cursos inglés

6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

X. TRANSFERENCIAS DE DATOS PERSONALES

UNAM - Los Ángeles (Centro de Estudios Mexicanos)	
Identificador único*	**Registro a inglés en línea (Zlingo, TOEFL, Pronunciación)**
(Nombre del sistema A2)*	**Registro alumnos cursos inglés**
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	No se realiza transferencia de datos personales mediante el traslado de soportes físicos.
Transferencias mediante el traslado de soportes electrónicos:	No se realiza transferencia de datos personales mediante el traslado de soportes electrónicos.
Transferencias mediante el traslado sobre redes electrónicas:	No se realiza transferencia de datos personales mediante el traslado sobre redes electrónicas.

XI. RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS

NO SE REALIZAN RESGURADOS CON SOPORTES FÍSICOS

i. Señalar las medidas de seguridad que ha implementado el área universitaria para el resguardo de los soportes físicos del sistema de manera que evite la alteración, pérdida o acceso no autorizado a los mismos.
ii. Señalar en un listado las personas (nombre, cargo, funciones y obligaciones) que tienen acceso a los soportes físicos del sistema.

XII. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

LA INFORMACIÓN DE ACCESO Y OPERACIÓN SE EN CUENTRA EN EL PROPIO SISTEMA COMO PANEL DE ACTIVIDAD

5. Los datos que se registran en las bitácoras:

- **a)** Quién accede a los datos personales, fecha y hora en la que se realiza el acceso o se intenta el mismo, propósito del acceso, así como fecha y hora de salida;
- **b)** Para soportes físicos: Número o clave del expediente utilizado, y
- **c)** Para soportes electrónicos: Operaciones o acciones llevadas a cabo y registros utilizados de la base de datos.

6. Si las bitácoras están en soporte físico o en soporte electrónico;
7. Lugar dónde almacena las bitácoras y por cuánto tiempo;
8. La manera en que asegura la integridad de las bitácoras, y
9. Respecto del análisis de las bitácoras:

- **a)** Quién es el responsable de analizarlas (si es el área universitaria o si es un tercero) y cada cuándo las analiza, y
- **b)** Para el caso de que las bitácoras estén en soporte electrónico: las herramientas de análisis utilizadas.

XIII. REGISTRO DE INCIDENTES:

NO SE CUENTA CON UN PROCEDIMIENTO DE ATENCIÓN A INCIDENTES

Describir el procedimiento de atención de incidentes que tiene implementado el área universitaria y especificar si lleva registro de los incidentes relativos a soportes físicos, como lo son la pérdida o alteración no autorizada de expedientes, y para el caso de soportes electrónicos, ofrecer detalles sobre el registro de incidentes en el cual consigne los procedimientos realizados para la recuperación de los datos o para permitir la disponibilidad del proceso.

i. Los datos que registra:

1. La persona que resolvió el incidente;
2. La metodología aplicada;
3. Para soportes físicos: Los oficios, documentos, expedientes, estantes o archiveros, tanto los dañados como los recuperados, y
4. Para soportes electrónicos: Los campos, registros, tablas, bases de datos o archivos electrónicos, tanto dañados como recuperados, el nombre de los sistemas y la infraestructura afectada, indicar si el incidente afectó el servidor principal y los servidores de respaldo, etc.

ii. Si el registro está en soporte físico o en soporte electrónico;
iii. Cómo asegura la integridad de dicho registro, y
iv. Para el caso de soportes electrónicos, quién autoriza la recuperación de datos.

XIV. ACCESO A LAS INSTALACIONES

3. Seguridad perimetral exterior (las instalaciones del área universitaria):

¿Qué medidas ha implementado para controlar el acceso de personas a sus instalaciones? Por ejemplo, se espera que describa si cuenta con uno o más puntos de control de acceso y quienes los operan, si tiene vigilancia las 24 horas, si ha levantado bardas o cercas, si existe un sistema de tratamiento de datos personales de videovigilancia, entre otras posibles medidas.

Para las personas que acceden a sus instalaciones:

a) ¿Cómo las identifica? No se cuenta con mecanismos de identificación.
b) ¿Cómo las autentifica? No se cuenta con mecanismos de autentificación.
c) ¿Cómo les autoriza el acceso? No se cuenta con mecanismos de control de acceso.

4. Seguridad perimetral interior (oficina, almacén o bodega para soportes físicos, centro de datos para soportes electrónicos):

¿Qué medidas de seguridad ha implementado para controlar el acceso a los espacios donde almacena los soportes físicos o electrónicos del sistema? Por ejemplo, se espera que precise el tipo de puertas y cerraduras instaladas, si tiene instalados controles biométricos, si administra la asignación de llaves y/o claves de acceso para abrir puertas y/o estantería, si cuenta con vigilancia las 24 horas, si hay un sistema de tratamiento de datos personales de videovigilancia, entre otras medidas.

Para las personas que acceden a dichos espacios interiores:

1. ¿Cómo las identifica? Solo el personal tiene acceso.
2. ¿Cómo las autentifica? Con identificación oficial.
3. ¿Cómo les autoriza el acceso? Se les asigna llave para ingreso a la oficina.

XV. ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

En este apartado se deberá establecer un mecanismo o procedimiento institucional para la actualización de la información personal contenida en el sistema, en donde se establezca la

frecuencia con la que se efectúa y la forma en que se está solicitando al titular acreditar de manera idónea sus requerimientos de rectificación de datos inexactos).

No se cuenta con un apartado de actualización de información en el sistema, en caso necesario los datos se ingresan nuevamente.

Las medidas de seguridad previstas a continuación en los incisos VII al IX, sólo aplican para soportes electrónicos

XVI. PERFILES DE USUARIO Y CONTRASEÑAS

En este rubro el área universitaria deberá describir el esquema de perfiles de usuario y contraseñas que tiene implementado para control de acceso mediante una red electrónica.

1. Modelo de control de acceso (alguno de los siguientes):

- **a)** ¿Es obligatorio (etiquetas para objetos y acreditación para sujetos)? No
- **b)** ¿Es discrecional (matriz de control de acceso)? No
- **c)** ¿Está basado en roles (perfiles) o grupos? Si
- **d)** ¿Está basado en reglas? No

2. Perfiles de usuario y contraseñas en el sistema operativo de red:

- **a)** ¿Cuenta con un sistema operativo de red instalado en sus equipos? Si
- **b)** ¿Proporciona dicho sistema operativo un manejo riguroso de perfiles de usuario y contraseñas? Si
- **c)** ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena? Si

3. Perfiles de usuario y contraseñas manejados por el software aplicativo del sistema de tratamiento de datos personales:

- **a)** ¿Ofrece dicho software un manejo riguroso de perfiles de usuario y contraseñas? Si
- **b)** ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena? Solo las contraseñas.

5. Administración de perfiles de usuario y contraseñas:

- **a)** ¿Quién da de alta nuevos perfiles? Delegado Administrativo.
- **b)** ¿Quién autoriza la creación de nuevos perfiles? Delegado Administrativo
- **c)** ¿Se lleva registro de la creación de nuevos perfiles? Si, en el mismo sistema.

6. Acceso remoto al sistema de tratamiento de datos personales:

- **a)** ¿Requieren los usuarios acceso remoto al equipo de cómputo que por lo general utilizan para trabajar con el sistema? No, cada usuario puede acceder al sistema desde cualquier equipo con conexión a internet.
- **b)** ¿Requiere el administrador acceso remoto al equipo donde reside el sistema para realizar tareas de mantenimiento? No
- **c)** ¿Cómo se evita el acceso remoto no autorizado? El sistema no se aloja en un equipo, por lo que no habría acceso remoto a dicho equipo.

XVII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

5. Señalar si realiza respaldos

1. Completos_X, diferenciales ___ o incrementales___;
2. De forma automática ____ o Manual __X___,
3. Periodicidad con que los realiza: _Anual_____

6. El tipo de medios (por ejemplo: cintas magnéticas, discos duros, CD-ROM, entre otros) que utiliza para almacenar las copias de seguridad: Disco duro

7. Cómo y dónde archiva esos medios, Se archiva en archivero bajo llave.

8. Quién es el responsable de realizar estas operaciones (el área universitaria o un tercero). El área universitaria.

XVIII. PLAN DE CONTINGENCIA

NO SE CUENTA CON UN PLAN DE CONTIGENCIA NI EN DESARROLLO.

4. Presentar el plan de contingencia con el cual garantiza la continuidad de la operación del sistema o informar si no lo tiene, pero se encuentra desarrollándolo.

5. Si cuenta con plan de contingencia y lo ha implementado, deberá indicar si realiza pruebas de eficiencia de este.

6. Informar si cuenta con un sitio redundante (alterno) y señalar lo siguiente:

a) El tipo de sitio (caliente, tibio o frío);
b) Si el sitio es propio o subcontratado con un tercero;
c) Los procedimientos, el equipo y el personal que designa para poner en marcha tal sitio y
d) Tiempo que le lleva poner en marcha el sitio, según las pruebas de eficiencia.

7. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

10.1. Herramientas y recursos para monitoreo de la protección de datos personales

UNAM - Los Ángeles (Centro de Estudios Mexicanos)		
Identificador único*	**Registro a inglés en línea (Zlingo, TOEFL, Pronunciación)**	
(Nombre del sistema A2)*	**Registro alumnos cursos inglés**	
Recurso*	**Descripción***	**Control***
Panel de actividad	Revisión aleatoria	Revisión de manera regular para supervisar el uso del sistema e identificar un posible uso inusual. Responsable: Alfredo Fernández Carmona

10.2. Procedimiento para la revisión de las medidas de seguridad

UNAM - Los Ángeles (Centro de Estudios Mexicanos)		
Identificador único*	**Registro a inglés en línea (Zlingo, TOEFL, Pronunciación)**	
(Nombre del sistema A2)*	**Registro alumnos cursos inglés**	
Medida de seguridad*	**Procedimiento***	**Responsable***
Principio del menor privilegio	Revisión de configuración de las cuentas de usuarios del sistema	Responsable de la revisión Alfredo Fernández Carmona. Duración de la revisión un día hábil.
Revisión de respaldos de la información	Revisar realización y ubicación de los respaldos realizados	Responsable de la revisión Alfredo Fernández Carmona Duración de la revisión un día hábil.

10.3. Resultados de la evaluación y pruebas a las medidas de seguridad

UNAM - Los Ángeles (Centro de Estudios Mexicanos)		
Identificador único*	**Registro a inglés en línea (Zlingo, TOEFL, Pronunciación)**	
(Nombre del sistema A2)*	**Registro alumnos cursos inglés**	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***
Principio del menor privilegio	Se encontró que todas las cuentas de usuarios del sistema cuentan con los privilegios correspondientes.	Responsable de realizar la revisión Alfredo Fernández Carmona Revisión realizada el 2 de noviembre de 2022.
Revisión de respaldos de la información	Se cuentan con respaldo realizados y en la ubicación correspondiente.	Responsable de realizar la revisión Alfredo Fernández Carmona Revisión realizada el 2 de noviembre de 2022.

10.4. Acciones para la corrección y actualización de las medidas de seguridad

UNAM - Los Ángeles (Centro de Estudios Mexicanos)		
Identificador único*	**Registro a inglés en línea (Zlingo, TOEFL, Pronunciación)**	
(Nombre del sistema A2)*	**Registro alumnos cursos inglés**	
Medida de seguridad*	**Acciones***	**Responsable***
Programa anual para evaluar medidas de seguridad.	Se revisaron las medidas implantadas. No se requirieron medidas correctivas.	Responsable de las acciones Alfredo Fernández Carmona. Fecha de conclusión de 02 de noviembre de 2022.

11. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

11.1. Programa de capacitación a los responsables de tratamiento de datos personales

UNAM - Los Ángeles (Centro de Estudios Mexicanos)			
Identificador único*	**Registro a inglés en línea (Zlingo, TOEFL, Pronunciación)**		
(Nombre del sistema A2)*	**Registro alumnos cursos inglés**		
Actividad*	**Descripción***	**Duración***	**Cobertura ***
Programa de capacitación que se relaciona con las medidas de seguridad técnica para la protección de datos personales en posesión de la UNAM, elaborado por DGETIC	Cursos en video que contribuyen a la formación y capacitación del personal a cargo de la protección de los datos personales en la UNAM en las entidades y dependencias	fecha de inicio 01 de diciembre de 2022 fecha de término 31 de enero de 2023	Responsable del sistema. Sin Vigencia. Sin frecuencia de actualización.

11.2. Programa de difusión de la protección a los datos personales

UNAM - Los Ángeles (Centro de Estudios Mexicanos)			
Identificador único*	**Registro a inglés en línea (Zlingo, TOEFL, Pronunciación)**		
(Nombre del sistema A2)*	**Registro alumnos cursos inglés**		
Actividad*	**Descripción***	**Duración***	**Cobertura+**
No se cuenta con un programa de difusión de la protección de datos personales.			

12. MEJORA CONTINUA

12.1. Actualización y mantenimiento de sistemas de información

UNAM - Los Ángeles (Centro de Estudios Mexicanos)			
Identificador único*	**Registro a inglés en línea (Zlingo, TOEFL, Pronunciación)**		
(Nombre del sistema A2)*	**Registro alumnos cursos inglés**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
N/A	N/A	N/A	N/A

12.2. Actualización y mantenimiento de equipo de cómputo

UNAM - Los Ángeles (Centro de Estudios Mexicanos)			
Identificador único*	**Registro a inglés en línea (Zlingo, TOEFL, Pronunciación)**		
(Nombre del sistema A2)*	**Registro alumnos cursos inglés**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Mantenimiento preventivo	Realizar el mantenimiento preventivo del equipo de cómputo tanto a nivel hardware como software para su funcionamiento óptimo.	1 vez por año	Equipos de cómputo de los usuarios del sistema.

12.3. Procesos para la conservación, preservación y respaldos de información

UNAM - Los Ángeles (Centro de Estudios Mexicanos)		
Identificador único*	**Registro a inglés en línea (Zlingo, TOEFL, Pronunciación)**	
(Nombre del sistema A2)*	**Registro alumnos cursos inglés**	
Proceso*	**Descripción***	**Responsable***
Respaldos periódicos de información	De manera anual se genera una copia de todos los archivos del sistema en un disco duro externo	Responsable de realizar respaldo Alfredo Fernández Carmona. Se lleva a cabo en 1 día hábil.

Por el momento no se cuenta con procesos de conservación y preservación de la información distintos a la generación de respaldos informáticos.

12.4. Procesos de borrado seguro y disposición final de equipos y componentes informáticos

UNAM - Los Ángeles (Centro de Estudios Mexicanos)		
Identificador único*	**Registro a inglés en línea (Zlingo, TOEFL, Pronunciación)**	
(Nombre del sistema A2)*	**Registro alumnos cursos inglés**	
Proceso*	**Descripción***	**Responsable***
Borrado seguro de información	Borrado seguro de información Con base en la circular DGTIC/003/2017, utilizando la herramienta de borrado seguro SDelete.	Responsable del proceso de borrado seguro Alfredo Fernández Carmona Tiempo máximo de ejecución 1 día hábil.

El sistema no se aloja en equipos informáticos, por lo que no aplica el proceso de disposición final de equipos.

13. PROCEDIMIENTO PARA LA CANCELACIÓN DE UN SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

1. Titular de la sede deberá solicitar la cancelación por escrito al encargado del sistema explicando los motivos y tiempo que deberá permanecer disponible para consulta.
2. El responsable del sistema deberá realizar la suspensión de las credenciales de acceso al sistema o en su caso, bloquear el apartado inicio de sesión del mismo.
3. El responsable del sistema deberá notificar al Titilar de la sede de las acciones realizadas para lograr la cancelación temporal del sistema.
4. Una vez transcurrida la temporalidad en que el sistema quedó bloqueado, el encargado del sistema iniciará la eliminación segura del mismo siguiendo el procedimiento establecido de Borrado seguro.
5. El responsable del sistema notificará al Titular de la sede de que el sistema ha sido cancelado.

Así mismo en el momento de la cancelación del sistema se deberán definir los siguientes puntos:

F) DATOS DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES QUE SERÁ CANCELADO:

a) Denominación
b) Motivo de la cancelación

G) PLAZOS Y CONDICIONES PARA EL BLOQUEO DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES:

(Señalar el periodo de bloqueo, considerando los plazos de prescripción para el ejercicio de algún derecho por parte de los titulares de conformidad con la normatividad de cada área universitaria. Asimismo, se debe señalar las condiciones y el procedimiento que se seguirá para realizar el bloqueo)

H) MEDIDAS DE SEGURIDAD PARA EL BLOQUEO Y POSTERIOR SUPRESIÓN DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES:

(Describir las medidas de seguridad aplicables al periodo de bloqueo y la supresión del sistema, considerando el nivel de protección requerido en virtud del tipo de datos personales contenidos en el sistema)

I) PROCEDIMIENTO PARA LA SUPRESIÓN DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

(Describir el procedimiento para suprimir el sistema, una vez cumplido el plazo de bloqueo)

J) MECANISMOS PARA LA SUPRESIÓN DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES
(Describir las técnicas para la eliminación física del sistema)

SISTEMA REGISTRO ASISTENTES A ACTIVIDADES ACADÉMICO/CULTURALES

1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

UNAM - Los Ángeles (Centro de Estudios Mexicanos)	
Identificador único*	**Registro Asistencia Acad/Cult.**
(Nombre del sistema A3) *	**Registro asistentes a actividades académico/culturales**
Datos personales (sensibles o no) contenidos en el sistema*:	Correo electrónico, nombre, apellido, género
Responsable: *	
Nombre*:	Alfredo Fernández Carmona
Cargo*:	Coordinador de relaciones y gestión
Funciones*:	Administrar acceso a responsables y usuarios. Actualizar campos de datos personales, cuando se requiera. Crear registros físicos.
Obligaciones*:	No difundir información de los datos personales. Resguardar el sistema.
	Encargados:
(Nombre del Encargado 1*)	Ricardo de Rosenzweig Díaz
Cargo*:	Encargado área comunicación
Funciones*:	Dar seguimiento a los registros de asistentes
Obligaciones*:	Almacenar registros físicos
	Usuarios:
(Nombre del Usuario 1*)	Vicente Ibarra Vázquez
Cargo*:	Asistente académico/administrativo
Funciones*:	Preparar información para reportes de matriz de indicadores trimestralmente
Obligaciones*:	No modificar información de los registros de alumnos inscritos.

2. ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

UNAM - Los Ángeles (Centro de Estudios Mexicanos)	
Identificador único¨*	**Registro Asistencia Acad/Cult.**
(Nombre del sistema A3*)	**Registro asistentes a actividades académico/culturales**
Tipo de soporte: *	Soporte Electrónico y soporte físico
Descripción: *	Base de Datos, registros impresos
Características del lugar donde se resguardan los soportes: *	Alojamiento en la nube privada de Google Drive Carpeta con los registros impresos en oficina de administración.

3. ANÁLISIS DE RIESGOS

UNAM - Los Ángeles (Centro de Estudios Mexicanos)		
Identificador único*	**Registro Asistencia Acad/Cult.**	
(Nombre del sistema A3) *	**Registro asistentes a actividades académico/culturales**	
Riesgo*	**Impacto***	**Mitigación***
No se cuenta soporte físico en el caso de registros electrónicos.	Pérdida de la información en caso de no poder acceder a la nube que aloja la información.	Realizar respaldo en soporte físico.
No se cuenta con soporte electrónico en el caso de registros físicos	Pérdida de la información en caso de extravío de la carpeta del soporte físico.	Realizar respaldo en soporte electrónico.

4. ANÁLISIS DE BRECHA

UNAM - Los Ángeles (Centro de Estudios Mexicanos)		
Identificador único*	**Registro Asistencia Acad/Cult.**	
(Nombre del sistema A3) *	**Registro asistentes a actividades académico/culturales**	
Medida de seguridad actual*	**Medida de seguridad necesaria***	**Acciones para remediación***
El acceso al sistema solo para responsable, encargado y usuario mediante correo electrónico y contraseña asignados por la G Suite for Education.	Establecer periodos para cambio de contraseñas.	Definir periodicidad para el cambio de contraseñas.

5. PLAN DE TRABAJO

UNAM - Los Ángeles (Centro de Estudios Mexicanos)			
Identificador único*		**Registro Asistencia Acad/Cult.**	
(Nombre del sistema A3) *		**Registro asistentes a actividades académico/culturales**	
Actividad*	**Descripción***	**Duración***	**Cobertura***
Respaldo en soporte físico	**Realizar respaldo en un medio de almacenamiento físico del soporte electrónico.**	**Realizar respaldo mensual.**	**Respaldo del total del sistema de Registro físico de asistentes a actividades académico/culturales.**
Respaldo en soporte electrónico.	**Realizar respaldo en medio de almacenamiento electrónico del soporte físico.**	**Realizar respaldo mensualmente.**	**Respaldo del total del sistema de Registro electrónico de asistentes a actividades académico/culturales**

6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

XIX. TRANSFERENCIAS DE DATOS PERSONALES

UNAM - Los Ángeles (Centro de Estudios Mexicanos)	
Identificador único*	**Registro Asistencia Acad/Cult.**
(Nombre del sistema A3)*	**Registro asistentes a actividades académico/culturales**
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	No se realiza transferencia de datos personales mediante el traslado de soportes físicos.
Transferencias mediante el traslado de soportes electrónicos:	No se realiza transferencia de datos personales mediante el traslado de soportes electrónicos.
Transferencias mediante el traslado sobre redes electrónicas:	No se realiza transferencia de datos personales mediante el traslado sobre redes electrónicas.

XX. RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS

NO SE REALIZAN RESGURADOS CON SOPORTES FÍSICOS

i. Señalar las medidas de seguridad que ha implementado el área universitaria para el resguardo de los soportes físicos del sistema de manera que evite la alteración, pérdida o acceso no autorizado a los mismos.

ii. Señalar en un listado las personas (nombre, cargo, funciones y obligaciones) que tienen acceso a los soportes físicos del sistema.

XXI. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

LA INFORMACIÓN DE ACCESO Y OPERACIÓN SE EN CUENTRA EN EL PROPIO SISTEMA COMO PANEL DE ACTIVIDAD

10. Los datos que se registran en las bitácoras:

- **a)** Quién accede a los datos personales, fecha y hora en la que se realiza el acceso o se intenta el mismo, propósito del acceso, así como fecha y hora de salida;
- **b)** Para soportes físicos: Número o clave del expediente utilizado, y
- **c)** Para soportes electrónicos: Operaciones o acciones llevadas a cabo y registros utilizados de la base de datos.

11. Si las bitácoras están en soporte físico o en soporte electrónico;

12. Lugar dónde almacena las bitácoras y por cuánto tiempo;

13. La manera en que asegura la integridad de las bitácoras, y

14. Respecto del análisis de las bitácoras:

- **a)** Quién es el responsable de analizarlas (si es el área universitaria o si es un tercero) y cada cuándo las analiza, y
- **b)** Para el caso de que las bitácoras estén en soporte electrónico: las herramientas de análisis utilizadas.

XXII. REGISTRO DE INCIDENTES:

NO SE CUENTA CON UN PROCEDIMIENTO DE ATENCIÓN A INCIDENTES

Describir el procedimiento de atención de incidentes que tiene implementado el área universitaria y especificar si lleva registro de los incidentes relativos a soportes físicos, como lo son la pérdida o alteración no autorizada de expedientes, y para el caso de soportes electrónicos, ofrecer detalles sobre el registro de incidentes en el cual consigne los procedimientos realizados para la recuperación de los datos o para permitir la disponibilidad del proceso.

i. Los datos que registra:

1. La persona que resolvió el incidente;
2. La metodología aplicada;
3. Para soportes físicos: Los oficios, documentos, expedientes, estantes o archiveros, tanto los dañados como los recuperados, y
4. Para soportes electrónicos: Los campos, registros, tablas, bases de datos o archivos electrónicos, tanto dañados como recuperados, el nombre de los sistemas y la infraestructura afectada, indicar si el incidente afectó el servidor principal y los servidores de respaldo, etc.

ii. Si el registro está en soporte físico o en soporte electrónico;
iii. Cómo asegura la integridad de dicho registro, y
iv. Para el caso de soportes electrónicos, quién autoriza la recuperación de datos.

XXIII. ACCESO A LAS INSTALACIONES

7. Seguridad perimetral exterior (las instalaciones del área universitaria):

¿Qué medidas ha implementado para controlar el acceso de personas a sus instalaciones? Por ejemplo, se espera que describa si cuenta con uno o más puntos de control de acceso y quienes los operan, si tiene vigilancia las 24 horas, si ha levantado bardas o cercas, si existe un sistema de tratamiento de datos personales de videovigilancia, entre otras posibles medidas.

Para las personas que acceden a sus instalaciones:

a) ¿Cómo las identifica? No se cuenta con mecanismos de identificación.
b) ¿Cómo las autentifica? No se cuenta con mecanismos de autentificación.
c) ¿Cómo les autoriza el acceso? No se cuenta con mecanismos de control de acceso.

8. Seguridad perimetral interior (oficina, almacén o bodega para soportes físicos, centro de datos para soportes electrónicos):

¿Qué medidas de seguridad ha implementado para controlar el acceso a los espacios donde almacena los soportes físicos o electrónicos del sistema? Por ejemplo, se espera que precise el tipo de puertas y cerraduras instaladas, si tiene instalados controles biométricos, si administra la asignación de llaves y/o claves de acceso para abrir puertas y/o estantería, si cuenta con vigilancia las 24 horas, si hay un sistema de tratamiento de datos personales de videovigilancia, entre otras medidas.

Para las personas que acceden a dichos espacios interiores:

1. ¿Cómo las identifica? Solo el personal tiene acceso.
2. ¿Cómo las autentifica? Con identificación oficial.
3. ¿Cómo les autoriza el acceso? Se les asigna llave para ingreso a la oficina.

XXIV.ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

En este apartado se deberá establecer un mecanismo o procedimiento institucional para la actualización de la información personal contenida en el sistema, en donde se establezca la frecuencia con la que se efectúa y la forma en que se está solicitando al titular acreditar de manera idónea sus requerimientos de rectificación de datos inexactos).

No se cuenta con un apartado de actualización de información en el sistema, en caso necesario los datos se ingresan nuevamente.

Las medidas de seguridad previstas a continuación en los incisos VII al IX, sólo aplican para soportes electrónicos

XXV. PERFILES DE USUARIO Y CONTRASEÑAS

En este rubro el área universitaria deberá describir el esquema de perfiles de usuario y contraseñas que tiene implementado para control de acceso mediante una red electrónica.

1. Modelo de control de acceso (alguno de los siguientes):

- **a)** ¿Es obligatorio (etiquetas para objetos y acreditación para sujetos)? No
- **b)** ¿Es discrecional (matriz de control de acceso)? No
- **c)** ¿Está basado en roles (perfiles) o grupos? Si
- **d)** ¿Está basado en reglas? No

2. Perfiles de usuario y contraseñas en el sistema operativo de red:

- **a)** ¿Cuenta con un sistema operativo de red instalado en sus equipos? Si
- **b)** ¿Proporciona dicho sistema operativo un manejo riguroso de perfiles de usuario y contraseñas? Si
- **c)** ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena? Si

3. Perfiles de usuario y contraseñas manejados por el software aplicativo del sistema de tratamiento de datos personales:

- **a)** ¿Ofrece dicho software un manejo riguroso de perfiles de usuario y contraseñas? Si
- **b)** ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena? Solo las contraseñas.

4. Administración de perfiles de usuario y contraseñas:

- **a)** ¿Quién da de alta nuevos perfiles? Delegado Administrativo.
- **b)** ¿Quién autoriza la creación de nuevos perfiles? Delegado Administrativo
- **c)** ¿Se lleva registro de la creación de nuevos perfiles? Si, en el mismo sistema.

5. Acceso remoto al sistema de tratamiento de datos personales:

- **a)** ¿Requieren los usuarios acceso remoto al equipo de cómputo que por lo general utilizan para trabajar con el sistema? No, cada usuario puede acceder al sistema desde cualquier equipo con conexión a internet.
- **b)** ¿Requiere el administrador acceso remoto al equipo donde reside el sistema para realizar tareas de mantenimiento? No
- **c)** ¿Cómo se evita el acceso remoto no autorizado? El sistema no se aloja en un equipo, por lo que no habría acceso remoto a dicho equipo.

XXVI. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

9. Señalar si realiza respaldos

1. Completos_X, diferenciales ___ o incrementales___;
2. De forma automática ____ o Manual __X___,
3. Periodicidad con que los realiza: _Anual_____

10. El tipo de medios (por ejemplo: cintas magnéticas, discos duros, CD-ROM, entre otros) que utiliza para almacenar las copias de seguridad; Disco duro

11.Cómo y dónde archiva esos medios, Se archiva en archivero bajo llave.

12. Quién es el responsable de realizar estas operaciones (el área universitaria o un tercero). El área universitaria.

XXVII. PLAN DE CONTINGENCIA

NO SE CUENTA CON UN PLAN DE CONTIGENCIA NI EN DESARROLLO.

7. Presentar el plan de contingencia con el cual garantiza la continuidad de la operación del sistema o informar si no lo tiene, pero se encuentra desarrollándolo.

8. Si cuenta con plan de contingencia y lo ha implementado, deberá indicar si realiza pruebas de eficiencia de este.

9. Informar si cuenta con un sitio redundante (alterno) y señalar lo siguiente:

a) El tipo de sitio (caliente, tibio o frío);
b) Si el sitio es propio o subcontratado con un tercero;
c) Los procedimientos, el equipo y el personal que designa para poner en marcha tal sitio y
d) Tiempo que le lleva poner en marcha el sitio, según las pruebas de eficiencia.

7. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

13.1. Herramientas y recursos para monitoreo de la protección de datos personales

UNAM - Los Ángeles (Centro de Estudios Mexicanos)		
Identificador único*	**Registro Asistencia Acad/Cult.**	
(Nombre del sistema A3)*	**Registro asistentes a actividades académico/culturales**	
Recurso*	**Descripción***	**Control***
Panel de actividad	Revisión aleatoria	Revisión de manera regular para supervisar el uso del sistema e identificar un posible uso inusual. Responsable: Alfredo Fernández Carmona

13.2. Procedimiento para la revisión de las medidas de seguridad

UNAM - Los Ángeles (Centro de Estudios Mexicanos)		
Identificador único*	**Registro Asistencia Acad/Cult.**	
(Nombre del sistema A3)*	**Registro asistentes a actividades académico/culturales**	
Medida de seguridad*	**Procedimiento***	**Responsable***
Principio del menor privilegio	Revisión de configuración de las cuentas de usuarios del sistema	Responsable de la revisión Alfredo Fernández Carmona. Duración de la revisión un día hábil.
Revisión de respaldos de la información	Revisar realización y ubicación de los respaldos realizados	Responsable de la revisión Alfredo Fernández Carmona Duración de la revisión un día hábil.

13.3. Resultados de la evaluación y pruebas a las medidas de seguridad

UNAM - Los Ángeles (Centro de Estudios Mexicanos)		
Identificador único*	**Registro Asistencia Acad/Cult.**	
(Nombre del sistema A3)*	**Registro asistentes a actividades académico/culturales**	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***
Principio del menor privilegio	Se encontró que todas las cuentas de usuarios del sistema cuentan con los privilegios correspondientes.	Responsable de realizar la revisión Alfredo Fernández Carmona Revisión realizada el 2 de noviembre de 2022.
Revisión de respaldos de la información	Se cuentan con respaldo realizados y en la ubicación correspondiente.	Responsable de realizar la revisión Alfredo Fernández Carmona Revisión realizada el 2 de noviembre de 2022.

13.4. Acciones para la corrección y actualización de las medidas de seguridad

UNAM - Los Ángeles (Centro de Estudios Mexicanos)		
Identificador único*	**Registro Asistencia Acad/Cult.**	
(Nombre del sistema A3)*	**Registro asistentes a actividades académico/culturales**	
Medida de seguridad*	**Acciones***	**Responsable***
Programa anual para evaluar medidas de seguridad.	Se revisaron las medidas implantadas. No se requirieron medidas correctivas.	Responsable de las acciones Alfredo Fernández Carmona. Fecha de conclusión de 02 de noviembre de 2022.

14. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

14.1. Programa de capacitación a los responsables de tratamiento de datos personales

UNAM - Los Ángeles (Centro de Estudios Mexicanos)			
Identificador único*	**Registro Asistencia Acad/Cult.**		
(Nombre del sistema A3)*	**Registro asistentes a actividades académico/culturales**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Programa de capacitación que se relaciona con las medidas de seguridad técnica para la protección de datos personales en posesión de la UNAM, elaborado por DGETIC	Cursos en video que contribuyen a la formación y capacitación del personal a cargo de la protección de los datos personales en la UNAM en las entidades y dependencias	fecha de inicio 01 de diciembre de 2022 fecha de término 31 de enero de 2023	Responsable del sistema. Sin Vigencia. Sin frecuencia de actualización.

14.2. Programa de difusión de la protección a los datos personales

UNAM - Los Ángeles (Centro de Estudios Mexicanos)			
Identificador único*	**Registro Asistencia Acad/Cult.**		
(Nombre del sistema A3)*	**Registro asistentes a actividades académico/culturales**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
No se cuenta con un programa de difusión de la protección de datos personales.			

15. MEJORA CONTINUA

15.1. Actualización y mantenimiento de sistemas de información

UNAM - Los Ángeles (Centro de Estudios Mexicanos)			
Identificador único*	**Registro Asistencia Acad/Cult.**		
(Nombre del sistema A3)*	**Registro asistentes a actividades académico/culturales**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
N/A	N/A	N/A	N/A

15.2. Actualización y mantenimiento de equipo de cómputo

UNAM - Los Ángeles (Centro de Estudios Mexicanos)			
Identificador único*	**Registro Asistencia Acad/Cult.**		
(Nombre del sistema A3)*	**Registro asistentes a actividades académico/culturales**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Mantenimiento preventivo	Realizar el mantenimiento preventivo del equipo de cómputo tanto a nivel hardware como software para su funcionamiento óptimo.	1 vez por año	Equipos de cómputo de los usuarios del sistema.

15.3. Procesos para la conservación, preservación y respaldos de información

UNAM - Los Ángeles (Centro de Estudios Mexicanos)		
Identificador único*	**Registro Asistencia Acad/Cult.**	
(Nombre del sistema A3)*	**Registro asistentes a actividades académico/culturales**	
Proceso*	**Descripción***	**Responsable***
Respaldos periódicos de información	De manera anual se genera una copia de todos los archivos del sistema en un disco duro externo	Responsable de realizar respaldo Alfredo Fernández Carmona. Se lleva a cabo en 1 día hábil.

Por el momento no se cuenta con procesos de conservación y preservación de la información distintos a la generación de respaldos informáticos.

15.4. Procesos de borrado seguro y disposición final de equipos y componentes informáticos

UNAM - Los Ángeles (Centro de Estudios Mexicanos)		
Identificador único*	**Registro Asistencia Acad/Cult.**	
(Nombre del sistema A3)*	**Registro asistentes a actividades académico/culturales**	
Proceso*	**Descripción***	**Responsable***
Borrado seguro de información	Borrado seguro de información Con base en la circular DGTIC/003/2017, utilizando la herramienta de borrado seguro SDelete.	Responsable del proceso de borrado seguro Alfredo Fernández Carmona Tiempo máximo de ejecución 1 día hábil.

El sistema no se aloja en equipos informáticos, por lo que no aplica el proceso de disposición final de equipos.

16. PROCEDIMIENTO PARA LA CANCELACIÓN DE UN SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

1. Titular de la sede deberá solicitar la cancelación por escrito al encargado del sistema explicando los motivos y tiempo que deberá permanecer disponible para consulta.
2. El responsable del sistema deberá realizar la suspensión de las credenciales de acceso al sistema o en su caso, bloquear el apartado inicio de sesión del mismo.
3. El responsable del sistema deberá notificar al Titilar de la sede de las acciones realizadas para lograr la cancelación temporal del sistema.
4. Una vez transcurrida la temporalidad en que el sistema quedó bloqueado, el encargado del sistema iniciará la eliminación segura del mismo siguiendo el procedimiento establecido de Borrado seguro.
5. El responsable del sistema notificará al Titular de la sede de que el sistema ha sido cancelado.

Así mismo en el momento de la cancelación del sistema se deberán definir los siguientes puntos:

K) DATOS DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES QUE SERÁ CANCELADO:

- **a)** Denominación
- **b)** Motivo de la cancelación

L) PLAZOS Y CONDICIONES PARA EL BLOQUEO DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES:

(Señalar el periodo de bloqueo, considerando los plazos de prescripción para el ejercicio de algún derecho por parte de los titulares de conformidad con la normatividad de cada área universitaria. Asimismo, se debe señalar las condiciones y el procedimiento que se seguirá para realizar el bloqueo)

M) MEDIDAS DE SEGURIDAD PARA EL BLOQUEO Y POSTERIOR SUPRESIÓN DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES:

(Describir las medidas de seguridad aplicables al periodo de bloqueo y la supresión del sistema, considerando el nivel de protección requerido en virtud del tipo de datos personales contenidos en el sistema)

N) PROCEDIMIENTO PARA LA SUPRESIÓN DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

(Describir el procedimiento para suprimir el sistema, una vez cumplido el plazo de bloqueo)

O) MECANISMOS PARA LA SUPRESIÓN DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

SISTEMA REGISTRO SUSCRIPCIÓN A BOLETÍN INFORMATIVO

1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

UNAM - Los Ángeles (Centro de Estudios Mexicanos)	
Identificador único*	**Suscripción boletín informativo**
(Nombre del sistema A4) *	**Registro suscripción al boletín informativo**
Datos personales (sensibles o no) contenidos en el sistema*:	Nombre, teléfono, correo electrónico.
Responsable: *	
Nombre*:	Alfredo Fernández Carmona
Cargo*:	Coordinador de relaciones y gestión
Funciones*:	Administrar acceso a responsables y usuarios. Actualizar campos de datos personales, cuando se requiera.
Obligaciones*:	No difundir información de los datos personales. Resguardar el sistema.
	Encargados:
(Nombre del Encargado 1*)	Ricardo de Rosenzweig Díaz
Cargo*:	Encargado área comunicación
Funciones*:	Dar seguimiento a los registros de nuevos suscriptores
Obligaciones*:	Mantener actualizado el estatus de los registros
	Usuarios:
(Nombre del Usuario 1*)	Ricardo de Rosenzweig Díaz
Cargo*:	Encargado área comunicación
Funciones*:	Envíar boletines informativos de actividades y/o eventos de la sede a los suscriptores.
Obligaciones*:	No modificar información de los registros de alumnos inscritos.

2. ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

UNAM - Los Ángeles (Centro de Estudios Mexicanos)	
Identificador único¨*	**Suscripción boletín informativo**
(Nombre del sistema A4*)	**Registro suscripción al boletín informativo**
Tipo de soporte: *	Soporte Electrónico
Descripción: *	Base de Datos
Características del lugar donde se resguardan los soportes: *	Alojamiento en la plataforma Wix.

3. ANÁLISIS DE RIESGOS

UNAM - Los Ángeles (Centro de Estudios Mexicanos)		
Identificador único*	**Suscripción boletín informativo**	
(Nombre del sistema A4) *	**Registro suscripción al boletín informativo**	
Riesgo*	**Impacto***	**Mitigación***
No se cuenta soporte físico	Pérdida de la información en caso de no poder acceder a la plataforma que aloja la información.	Realizar respaldo en soporte físico.

4. ANÁLISIS DE BRECHA

UNAM - Los Ángeles (Centro de Estudios Mexicanos)		
Identificador único*	**Suscripción boletín informativo**	
(Nombre del sistema A4) *	**Registro suscripción al boletín informativo**	
Medida de seguridad actual*	**Medida de seguridad necesaria***	**Acciones para remediación***
El acceso al sistema solo para responsable, encargado y usuario mediante correo electrónico y contraseña asignados el administrador en Wix	Establecer periodos para cambio de contraseñas.	Definir periodicidad para el cambio de contraseñas.

5. PLAN DE TRABAJO

UNAM - Los Ángeles (Centro de Estudios Mexicanos)			
Identificador único*	**Suscripción boletín informativo**		
(Nombre del sistema A4)*	**Registro suscripción al boletín informativo**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Respaldo en soporte físico	Realizar respaldo en un medio de almacenamiento físico del soporte electrónico.	Realizar respaldo mensual.	Respaldo del total de sistema de Registro de suscriptores del boletín.

6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

XXVIII. TRANSFERENCIAS DE DATOS PERSONALES

UNAM - Los Ángeles (Centro de Estudios Mexicanos)	
Identificador único*	**Suscripción boletín informativo**
(Nombre del sistema A4)*	**Registro suscripción al boletín informativo**
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	No se realiza transferencia de datos personales mediante el traslado de soportes físicos.
Transferencias mediante el traslado de soportes electrónicos:	No se realiza transferencia de datos personales mediante el traslado de soportes electrónicos.
Transferencias mediante el traslado sobre redes electrónicas:	No se realiza transferencia de datos personales mediante el traslado sobre redes electrónicas.

XXIX. RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS

NO SE REALIZAN RESGURADOS CON SOPORTES FÍSICOS

i. Señalar las medidas de seguridad que ha implementado el área universitaria para el resguardo de los soportes físicos del sistema de manera que evite la alteración, pérdida o acceso no autorizado a los mismos.
ii. Señalar en un listado las personas (nombre, cargo, funciones y obligaciones) que tienen acceso a los soportes físicos del sistema.

XXX. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

LA INFORMACIÓN DE ACCESO Y OPERACIÓN SE EN CUENTRA EN EL PROPIO SISTEMA COMO PANEL DE ACTIVIDAD

15. Los datos que se registran en las bitácoras:

- **a)** Quién accede a los datos personales, fecha y hora en la que se realiza el acceso o se intenta el mismo, propósito del acceso, así como fecha y hora de salida;
- **b)** Para soportes físicos: Número o clave del expediente utilizado, y
- **c)** Para soportes electrónicos: Operaciones o acciones llevadas a cabo y registros utilizados de la base de datos.

16. Si las bitácoras están en soporte físico o en soporte electrónico;
17. Lugar dónde almacena las bitácoras y por cuánto tiempo;
18. La manera en que asegura la integridad de las bitácoras, y
19. Respecto del análisis de las bitácoras:

- **a)** Quién es el responsable de analizarlas (si es el área universitaria o si es un tercero) y cada cuándo las analiza, y
- **b)** Para el caso de que las bitácoras estén en soporte electrónico: las herramientas de análisis utilizadas.

XXXI. REGISTRO DE INCIDENTES:

NO SE CUENTA CON UN PROCEDIMIENTO DE ATENCIÓN A INCIDENTES

Describir el procedimiento de atención de incidentes que tiene implementado el área universitaria y especificar si lleva registro de los incidentes relativos a soportes físicos, como lo son la pérdida o alteración no autorizada de expedientes, y para el caso de soportes electrónicos, ofrecer detalles sobre el registro de incidentes en el cual consigne los procedimientos realizados para la recuperación de los datos o para permitir la disponibilidad del proceso.
i. Los datos que registra:

1. La persona que resolvió el incidente;
2. La metodología aplicada;
3. Para soportes físicos: Los oficios, documentos, expedientes, estantes o archiveros, tanto los dañados como los recuperados, y
4. Para soportes electrónicos: Los campos, registros, tablas, bases de datos o archivos electrónicos, tanto dañados como recuperados, el nombre de los sistemas y la infraestructura afectada, indicar si el incidente afectó el servidor principal y los servidores de respaldo, etc.

ii. Si el registro está en soporte físico o en soporte electrónico;
iii. Cómo asegura la integridad de dicho registro, y
iv. Para el caso de soportes electrónicos, quién autoriza la recuperación de datos.
v.

XXXII.
ACCESO A LAS INSTALACIONES

9. Seguridad perimetral exterior (las instalaciones del área universitaria):

¿Qué medidas ha implementado para controlar el acceso de personas a sus instalaciones? Por ejemplo, se espera que describa si cuenta con uno o más puntos de control de acceso y quienes los operan, si tiene vigilancia las 24 horas, si ha levantado bardas o cercas, si existe un sistema de tratamiento de datos personales de videovigilancia, entre otras posibles medidas.

Para las personas que acceden a sus instalaciones:

a) ¿Cómo las identifica? No se cuenta con mecanismos de identificación.
b) ¿Cómo las autentifica? No se cuenta con mecanismos de autentificación.
c) ¿Cómo les autoriza el acceso? No se cuenta con mecanismos de control de acceso.

10. Seguridad perimetral interior (oficina, almacén o bodega para soportes físicos, centro de datos para soportes electrónicos):

¿Qué medidas de seguridad ha implementado para controlar el acceso a los espacios donde almacena los soportes físicos o electrónicos del sistema? Por ejemplo, se espera que precise el tipo de puertas y cerraduras instaladas, si tiene instalados controles biométricos, si administra la asignación de llaves y/o claves de acceso para abrir puertas y/o estantería, si cuenta con vigilancia las 24 horas, si hay un sistema de tratamiento de datos personales de videovigilancia, entre otras medidas.

Para las personas que acceden a dichos espacios interiores:

1. ¿Cómo las identifica? Solo el personal tiene acceso.
2. ¿Cómo las autentifica? Con identificación oficial.
3. ¿Cómo les autoriza el acceso? Se les asigna llave para ingreso a la oficina.

XXXIII. ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

En este apartado se deberá establecer un mecanismo o procedimiento institucional para la actualización de la información personal contenida en el sistema, en donde se establezca la frecuencia con la que se efectúa y la forma en que se está solicitando al titular acreditar de manera idónea sus requerimientos de rectificación de datos inexactos).

No se cuenta con un apartado de actualización de información en el sistema, en caso necesario los datos se ingresan nuevamente.

Las medidas de seguridad previstas a continuación en los incisos VII al IX, sólo aplican para soportes electrónicos

XXXIV. PERFILES DE USUARIO Y CONTRASEÑAS

En este rubro el área universitaria deberá describir el esquema de perfiles de usuario y contraseñas que tiene implementado para control de acceso mediante una red electrónica.

1. Modelo de control de acceso (alguno de los siguientes):

a) ¿Es obligatorio (etiquetas para objetos y acreditación para sujetos)? No
b) ¿Es discrecional (matriz de control de acceso)? No
c) ¿Está basado en roles (perfiles) o grupos? Si
d) ¿Está basado en reglas? No

2. Perfiles de usuario y contraseñas en el sistema operativo de red:

a) ¿Cuenta con un sistema operativo de red instalado en sus equipos? Si
b) ¿Proporciona dicho sistema operativo un manejo riguroso de perfiles de usuario y contraseñas? Si
c) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena? Si

3. Perfiles de usuario y contraseñas manejados por el software aplicativo del sistema de tratamiento de datos personales:

a) ¿Ofrece dicho software un manejo riguroso de perfiles de usuario y contraseñas? Si
b) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena? Solo las contraseñas.

4. Administración de perfiles de usuario y contraseñas:

a) ¿Quién da de alta nuevos perfiles? Delegado Administrativo.
b) ¿Quién autoriza la creación de nuevos perfiles? Delegado Administrativo
c) ¿Se lleva registro de la creación de nuevos perfiles? Si, en el mismo sistema.

5. Acceso remoto al sistema de tratamiento de datos personales:

a) ¿Requieren los usuarios acceso remoto al equipo de cómputo que por lo general utilizan para trabajar con el sistema? No, cada usuario puede acceder al sistema desde cualquier equipo con conexión a internet.
b) ¿Requiere el administrador acceso remoto al equipo donde reside el sistema para realizar tareas de mantenimiento? No
c) ¿Cómo se evita el acceso remoto no autorizado? El sistema no se aloja en un equipo, por lo que no habría acceso remoto a dicho equipo.

XXXV. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

13. Señalar si realiza respaldos

1. Completos_X, diferenciales ___ o incrementales___;
2. De forma automática ____ o Manual __X___,
3. Periodicidad con que los realiza: _Anual_____

14. El tipo de medios (por ejemplo: cintas magnéticas, discos duros, CD-ROM, entre otros) que utiliza para almacenar las copias de seguridad: Disco duro

15. Cómo y dónde archiva esos medios, Se archiva en archivero bajo llave.

16. Quién es el responsable de realizar estas operaciones (el área universitaria o un tercero). El área universitaria.

XXXVI. PLAN DE CONTINGENCIA

NO SE CUENTA CON UN PLAN DE CONTIGENCIA NI EN DESARROLLO.

10. Presentar el plan de contingencia con el cual garantiza la continuidad de la operación del sistema o informar si no lo tiene, pero se encuentra desarrollándolo.

11. Si cuenta con plan de contingencia y lo ha implementado, deberá indicar si realiza pruebas de eficiencia de este.

12. Informar si cuenta con un sitio redundante (alterno) y señalar lo siguiente:

a) El tipo de sitio (caliente, tibio o frío);
b) Si el sitio es propio o subcontratado con un tercero;
c) Los procedimientos, el equipo y el personal que designa para poner en marcha tal sitio y
d) Tiempo que le lleva poner en marcha el sitio, según las pruebas de eficiencia.

7. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

16.1. Herramientas y recursos para monitoreo de la protección de datos personales

UNAM - Los Ángeles (Centro de Estudios Mexicanos)		
Identificador único*	**Suscripción boletín informativo**	
(Nombre del sistema A4)*	**Registro suscripción al boletín informativo**	
Recurso*	**Descripción***	**Control***
Panel de actividad	Revisión aleatoria	Revisión de manera regular para supervisar el uso del sistema e identificar un posible uso inusual. Responsable: Alfredo Fernández Carmona

16.2. Procedimiento para la revisión de las medidas de seguridad

UNAM - Los Ángeles (Centro de Estudios Mexicanos)		
Identificador único*	**Suscripción boletín informativo**	
(Nombre del sistema A4)*	**Registro suscripción al boletín informativo**	
Medida de seguridad*	**Procedimiento***	**Responsable***
Principio del menor privilegio	Revisión de configuración de las cuentas de usuarios del sistema	Responsable de la revisión Alfredo Fernández Carmona. Duración de la revisión un día hábil.
Revisión de respaldos de la información	Revisar realización y ubicación de los respaldos realizados	Responsable de la revisión Alfredo Fernández Carmona Duración de la revisión un día hábil.

16.3. Resultados de la evaluación y pruebas a las medidas de seguridad

UNAM - Los Ángeles (Centro de Estudios Mexicanos)		
Identificador único*	**Suscripción boletín informativo**	
(Nombre del sistema A4)*	**Registro suscripción al boletín informativo**	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***
Principio del menor privilegio	Se encontró que todas las cuentas de usuarios del sistema cuentan con los privilegios correspondientes.	Responsable de realizar la revisión Alfredo Fernández Carmona Revisión realizada el 2 de noviembre de 2022.
Revisión de respaldos de la información	Se cuentan con respaldo realizados y en la ubicación correspondiente.	Responsable de realizar la revisión Alfredo Fernández Carmona Revisión realizada el 2 de noviembre de 2022.

16.4. Acciones para la corrección y actualización de las medidas de seguridad

UNAM - Los Ángeles (Centro de Estudios Mexicanos)		
Identificador único*	**Suscripción boletín informativo**	
(Nombre del sistema A4)*	**Registro suscripción al boletín informativo**	
Medida de seguridad*	**Acciones***	**Responsable***
Programa anual para evaluar medidas de seguridad.	Se revisaron las medidas implantadas. No se requirieron medidas correctivas.	Responsable de las acciones Alfredo Fernández Carmona. Fecha de conclusión de 02 de noviembre de 2022.

17. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

17.1. Programa de capacitación a los responsables de tratamiento de datos personales

UNAM - Los Ángeles (Centro de Estudios Mexicanos)			
Identificador único*	**Suscripción boletín informativo**		
(Nombre del sistema A4)*	**Registro suscripción al boletín informativo**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Programa de capacitación que se relaciona con las medidas de seguridad técnica para la protección de datos personales en posesión de la UNAM, elaborado por DGETIC	Cursos en video que contribuyen a la formación y capacitación del personal a cargo de la protección de los datos personales en la UNAM en las entidades y dependencias	fecha de inicio 01 de diciembre de 2022 fecha de término 31 de enero de 2023	Responsable del sistema. Sin Vigencia. Sin frecuencia de actualización.

17.2. Programa de difusión de la protección a los datos personales

UNAM - Los Ángeles (Centro de Estudios Mexicanos)			
Identificador único*	**Suscripción boletín informativo**		
(Nombre del sistema A4)*	**Registro suscripción al boletín informativo**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
No se cuenta con un programa de difusión de la protección de datos personales.			

18. MEJORA CONTINUA

18.1. Actualización y mantenimiento de sistemas de información

UNAM - Los Ángeles (Centro de Estudios Mexicanos)			
Identificador único*	**Suscripción boletín informativo**		
(Nombre del sistema A4)*	**Registro suscripción al boletín informativo**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
N/A	N/A	N/A	N/A

18.2. Actualización y mantenimiento de equipo de cómputo

UNAM - Los Ángeles (Centro de Estudios Mexicanos)			
Identificador único*	**Suscripción boletín informativo**		
(Nombre del sistema A4)*	**Registro suscripción al boletín informativo**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Mantenimiento preventivo	Realizar el mantenimiento preventivo del equipo de cómputo tanto a nivel hardware como software para su funcionamiento óptimo.	1 vez por año	Equipos de cómputo de los usuarios del sistema.

18.3. Procesos para la conservación, preservación y respaldos de información

UNAM - Los Ángeles (Centro de Estudios Mexicanos)		
Identificador único*	**Suscripción boletín informativo**	
(Nombre del sistema A4)*	**Registro suscripción al boletín informativo**	
Proceso*	**Descripción***	**Responsable***
Respaldos periódicos de información	De manera anual se genera una copia de todos los archivos del sistema en un disco duro externo	Responsable de realizar respaldo Alfredo Fernández Carmona. Se lleva a cabo en 1 día hábil.

Por el momento no se cuenta con procesos de conservación y preservación de la información distintos a la generación de respaldos informáticos.

18.4. Procesos de borrado seguro y disposición final de equipos y componentes informáticos

UNAM - Los Ángeles (Centro de Estudios Mexicanos)		
Identificador único*	**Suscripción boletín informativo**	
(Nombre del sistema A4)*	**Registro suscripción al boletín informativo**	
Proceso*	**Descripción***	**Responsable***
Borrado seguro de información	Borrado seguro de información Con base en la circular DGTIC/003/2017, utilizando la herramienta de borrado seguro SDelete.	Responsable del proceso de borrado seguro Alfredo Fernández Carmona Tiempo máximo de ejecución 1 día hábil.

El sistema no se aloja en equipos informáticos, por lo que no aplica el proceso de disposición final de equipos.

19. PROCEDIMIENTO PARA LA CANCELACIÓN DE UN SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

1. Titular de la sede deberá solicitar la cancelación por escrito al encargado del sistema explicando los motivos y tiempo que deberá permanecer disponible para consulta.
2. El responsable del sistema deberá realizar la suspensión de las credenciales de acceso al sistema o en su caso, bloquear el apartado inicio de sesión del mismo.
3. El responsable del sistema deberá notificar al Titilar de la sede de las acciones realizadas para lograr la cancelación temporal del sistema.
4. Una vez transcurrida la temporalidad en que el sistema quedó bloqueado, el encargado del sistema iniciará la eliminación segura del mismo siguiendo el procedimiento establecido de Borrado seguro.
5. El responsable del sistema notificará al Titular de la sede de que el sistema ha sido cancelado.

Así mismo en el momento de la cancelación del sistema se deberán definir los siguientes puntos:

P) DATOS DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES QUE SERÁ CANCELADO:

a) Denominación
b) Motivo de la cancelación

Q) PLAZOS Y CONDICIONES PARA EL BLOQUEO DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES:

(Señalar el periodo de bloqueo, considerando los plazos de prescripción para el ejercicio de algún derecho por parte de los titulares de conformidad con la normatividad de cada área universitaria. Asimismo, se debe señalar las condiciones y el procedimiento que se seguirá para realizar el bloqueo)

R) MEDIDAS DE SEGURIDAD PARA EL BLOQUEO Y POSTERIOR SUPRESIÓN DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES:
(Describir las medidas de seguridad aplicables al periodo de bloqueo y la supresión del sistema, considerando el nivel de protección requerido en virtud del tipo de datos personales contenidos en el sistema)

S) PROCEDIMIENTO PARA LA SUPRESIÓN DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

(Describir el procedimiento para suprimir el sistema, una vez cumplido el plazo de bloqueo)

T) MECANISMOS PARA LA SUPRESIÓN DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

SISTEMA REGISTRO EXPENDIENTES DEL PERSONAL

1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

UNAM - Los Ángeles (Centro de Estudios Mexicanos)	
Identificador único*	**Expedientes del personal UNAM LA**
(Nombre del sistema A5) *	**Expedientes del personal**
Datos personales (sensibles o no) contenidos en el sistema*:	Nombre, dirección, número de seguridad social, identificación, teléfono, correo electrónico, contacto de emergencia, teléfono de contacto de emergencia, condición médica existente.
Responsable/ Encargado/ Usuario: *	
Nombre*:	Alfredo Fernández Carmona
Cargo*:	Coordinador de relaciones y gestión
Funciones*:	Mantener actualizado el expediente por altas/bajas/cambios del personal de la sede.
Obligaciones*:	No difundir información de los datos personales. Resguardar el sistema.

2. ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

UNAM - Los Ángeles (Centro de Estudios Mexicanos)	
Identificador único¨*	**Expedientes del personal UNAM LA**
(Nombre del sistema A5*)	**Expedientes del personal**
Tipo de soporte: *	Soporte Electrónico y Soporte Físico
Descripción: *	Expedientes en papel y electrónico con documentación de identificación, formularios fiscales, formularios de empleo y formularios de seguros.
Características del lugar donde se resguardan los soportes: *	Archivero en oficina de administración de la sede y en la nube de Google Drive.

3. ANÁLISIS DE RIESGOS

UNAM - Los Ángeles (Centro de Estudios Mexicanos)		
Identificador único*	**Expedientes del personal UNAM LA**	
(Nombre del sistema A5) *	**Expedientes del personal**	
Riesgo*	**Impacto***	**Mitigación***
Una sola persona es responsable, encargado y usuario del sistema de expedientes del personal.	Pérdida de la información en caso de que la persona encargada no pueda acceder al soporte tanto físico como electrónico.	Designar a una persona diferente como usuario y sea soporte para tener acceso a la información de expediente de personal.

4. ANÁLISIS DE BRECHA

UNAM - Los Ángeles (Centro de Estudios Mexicanos)		
Identificador único*	**Expedientes del personal UNAM LA**	
(Nombre del sistema A5) *	**Expedientes del personal**	
Medida de seguridad actual*	**Medida de seguridad necesaria***	**Acciones para remediación***
El acceso al sistema solo para responsable, encargado y usuario mediante correo electrónico y contraseña generados con G Suite for Education.	Establecer periodos para cambio de contraseñas.	Definir periodicidad para el cambio de contraseñas.

5. PLAN DE TRABAJO

UNAM - Los Ángeles (Centro de Estudios Mexicanos)			
Identificador único*	**Expedientes del personal UNAM LA**		
(Nombre del sistema A5)*	**Expedientes del personal**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Respaldo en soporte electrónico	Realizar respaldo en un medio de almacenamiento electrónico del soporte físico.	Realizar respaldo anual.	Respaldo del total de sistema de expedientes del personal.

6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

XXXVII. TRANSFERENCIAS DE DATOS PERSONALES

UNAM - Los Ángeles (Centro de Estudios Mexicanos)	
Identificador único*	**Expedientes del personal UNAM LA**
(Nombre del sistema A5)*	**Expedientes del personal**
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	No se realiza transferencia de datos personales mediante el traslado de soportes físicos.
Transferencias mediante el traslado de soportes electrónicos:	No se realiza transferencia de datos personales mediante el traslado de soportes electrónicos.
Transferencias mediante el traslado sobre redes electrónicas:	No se realiza transferencia de datos personales mediante el traslado sobre redes electrónicas.

XXXVIII. RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS

NO SE REALIZAN RESGURADOS CON SOPORTES FÍSICOS

i. Señalar las medidas de seguridad que ha implementado el área universitaria para el resguardo de los soportes físicos del sistema de manera que evite la alteración, pérdida o acceso no autorizado a los mismos.

ii. Señalar en un listado las personas (nombre, cargo, funciones y obligaciones) que tienen acceso a los soportes físicos del sistema.

XXXIX. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

NO SE CUENTA CON UNA BITÁCORA DE ACCESO Y OPERACIÓN

20. Los datos que se registran en las bitácoras:

- **a)** Quién accede a los datos personales, fecha y hora en la que se realiza el acceso o se intenta el mismo, propósito del acceso, así como fecha y hora de salida;
- **b)** Para soportes físicos: Número o clave del expediente utilizado, y
- **c)** Para soportes electrónicos: Operaciones o acciones llevadas a cabo y registros utilizados de la base de datos.

21. Si las bitácoras están en soporte físico o en soporte electrónico;
22. Lugar dónde almacena las bitácoras y por cuánto tiempo;
23. La manera en que asegura la integridad de las bitácoras, y
24. Respecto del análisis de las bitácoras:

- **a)** Quién es el responsable de analizarlas (si es el área universitaria o si es un tercero) y cada cuándo las analiza, y
- **b)** Para el caso de que las bitácoras estén en soporte electrónico: las herramientas de análisis utilizadas.

XL. REGISTRO DE INCIDENTES:

NO SE CUENTA CON UN PROCEDIMIENTO DE ATENCIÓN A INCIDENTES

Describir el procedimiento de atención de incidentes que tiene implementado el área universitaria y especificar si lleva registro de los incidentes relativos a soportes físicos, como lo son la pérdida o alteración no autorizada de expedientes, y para el caso de soportes electrónicos, ofrecer detalles sobre el registro de incidentes en el cual consigne los procedimientos realizados para la recuperación de los datos o para permitir la disponibilidad del proceso.

i. Los datos que registra:

1. La persona que resolvió el incidente;
2. La metodología aplicada;
3. Para soportes físicos: Los oficios, documentos, expedientes, estantes o archiveros, tanto los dañados como los recuperados, y
4. Para soportes electrónicos: Los campos, registros, tablas, bases de datos o archivos electrónicos, tanto dañados como recuperados, el nombre de los sistemas y la infraestructura afectada, indicar si el incidente afectó el servidor principal y los servidores de respaldo, etc.

ii. Si el registro está en soporte físico o en soporte electrónico;
iii. Cómo asegura la integridad de dicho registro, y
iv. Para el caso de soportes electrónicos, quién autoriza la recuperación de datos.

XLI. ACCESO A LAS INSTALACIONES

11. Seguridad perimetral exterior (las instalaciones del área universitaria):

¿Qué medidas ha implementado para controlar el acceso de personas a sus instalaciones? Por ejemplo, se espera que describa si cuenta con uno o más puntos de control de acceso y quienes los operan, si tiene vigilancia las 24 horas, si ha levantado bardas o cercas, si existe un sistema de tratamiento de datos personales de videovigilancia, entre otras posibles medidas.

Para las personas que acceden a sus instalaciones:

a) ¿Cómo las identifica? No se cuenta con mecanismos de identificación.
b) ¿Cómo las autentifica? No se cuenta con mecanismos de autentificación.
c) ¿Cómo les autoriza el acceso? No se cuenta con mecanismos de control de acceso.

12. Seguridad perimetral interior (oficina, almacén o bodega para soportes físicos, centro de datos para soportes electrónicos):

¿Qué medidas de seguridad ha implementado para controlar el acceso a los espacios donde almacena los soportes físicos o electrónicos del sistema? Por ejemplo, se espera que precise el tipo de puertas y cerraduras instaladas, si tiene instalados controles biométricos, si administra la asignación de llaves y/o claves de acceso para abrir puertas y/o estantería, si cuenta con vigilancia las 24 horas, si hay un sistema de tratamiento de datos personales de videovigilancia, entre otras medidas.

Para las personas que acceden a dichos espacios interiores:

1. ¿Cómo las identifica? Solo el personal tiene acceso.
2. ¿Cómo las autentifica? Con identificación oficial.
3. ¿Cómo les autoriza el acceso? Se les asigna llave para ingreso a la oficina.

XLII. ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

En este apartado se deberá establecer un mecanismo o procedimiento institucional para la actualización de la información personal contenida en el sistema, en donde se establezca la frecuencia con la que se efectúa y la forma en que se está solicitando al titular acreditar de manera idónea sus requerimientos de rectificación de datos inexactos).

No se cuenta con un apartado de actualización de información en el sistema, en caso necesario los datos se ingresan nuevamente.

Las medidas de seguridad previstas a continuación en los incisos VII al IX, sólo aplican para soportes electrónicos

XLIII. PERFILES DE USUARIO Y CONTRASEÑAS

En este rubro el área universitaria deberá describir el esquema de perfiles de usuario y contraseñas que tiene implementado para control de acceso mediante una red electrónica.

1. Modelo de control de acceso (alguno de los siguientes):

a) ¿Es obligatorio (etiquetas para objetos y acreditación para sujetos)? No
b) ¿Es discrecional (matriz de control de acceso)? No
c) ¿Está basado en roles (perfiles) o grupos? Si
d) ¿Está basado en reglas? No

2. Perfiles de usuario y contraseñas en el sistema operativo de red:

a) ¿Cuenta con un sistema operativo de red instalado en sus equipos? Si
b) ¿Proporciona dicho sistema operativo un manejo riguroso de perfiles de usuario y contraseñas? Si
c) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena? Si

3. Perfiles de usuario y contraseñas manejados por el software aplicativo del sistema de tratamiento de datos personales:

a) ¿Ofrece dicho software un manejo riguroso de perfiles de usuario y contraseñas? Si
b) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena? Solo las contraseñas.

4. Administración de perfiles de usuario y contraseñas:

a) ¿Quién da de alta nuevos perfiles? Delegado Administrativo.
b) ¿Quién autoriza la creación de nuevos perfiles? Delegado Administrativo
c) ¿Se lleva registro de la creación de nuevos perfiles? Si, en el mismo sistema.

5. Acceso remoto al sistema de tratamiento de datos personales:

a) ¿Requieren los usuarios acceso remoto al equipo de cómputo que por lo general utilizan para trabajar con el sistema? No, cada usuario puede acceder al sistema desde cualquier equipo con conexión a internet.
b) ¿Requiere el administrador acceso remoto al equipo donde reside el sistema para realizar tareas de mantenimiento? No
c) ¿Cómo se evita el acceso remoto no autorizado? El sistema no se aloja en un equipo, por lo que no habría acceso remoto a dicho equipo.

XLIV. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

Señalar si realiza respaldos

1. Completos_X, diferenciales ___ o incrementales___;
2. De forma automática ____ o Manual __X___,
3. Periodicidad con que los realiza: _Anual_____

17. El tipo de medios (por ejemplo: cintas magnéticas, discos duros, CD-ROM, entre otros) que utiliza para almacenar las copias de seguridad: Disco duro

18. Cómo y dónde archiva esos medios, Se archiva en archivero bajo llave.

a) Quién es el responsable de realizar estas operaciones (el área universitaria o un tercero). El área universitaria.

XLV. PLAN DE CONTINGENCIA

NO SE CUENTA CON UN PLAN DE CONTIGENCIA NI EN DESARROLLO.

13. Presentar el plan de contingencia con el cual garantiza la continuidad de la operación del sistema o informar si no lo tiene, pero se encuentra desarrollándolo.

14. Si cuenta con plan de contingencia y lo ha implementado, deberá indicar si realiza pruebas de eficiencia de este.

15. Informar si cuenta con un sitio redundante (alterno) y señalar lo siguiente:

a) El tipo de sitio (caliente, tibio o frío);
b) Si el sitio es propio o subcontratado con un tercero;
c) Los procedimientos, el equipo y el personal que designa para poner en marcha tal sitio y
d) Tiempo que le lleva poner en marcha el sitio, según las pruebas de eficiencia.

7. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

19.1. Herramientas y recursos para monitoreo de la protección de datos personales

UNAM - Los Ángeles (Centro de Estudios Mexicanos)		
Identificador único*	**Expedientes del personal UNAM LA**	
(Nombre del sistema A5)*	**Expedientes del personal**	
Recurso*	**Descripción***	**Control***
Panel de actividad	Revisión aleatoria	Revisión de manera regular para supervisar el uso del sistema e identificar un posible uso inusual. Responsable: Alfredo Fernández Carmona

19.2. Procedimiento para la revisión de las medidas de seguridad

UNAM - Los Ángeles (Centro de Estudios Mexicanos)		
Identificador único*	**Expedientes del personal UNAM LA**	
(Nombre del sistema A5)*	**Expedientes del personal**	
Medida de seguridad*	**Procedimiento***	**Responsable***
Principio del menor privilegio	Revisión de configuración de las cuentas de usuarios del sistema	Responsable de la revisión Alfredo Fernández Carmona. Duración de la revisión un día hábil.
Revisión de respaldos de la información	Revisar realización y ubicación de los respaldos realizados	Responsable de la revisión Alfredo Fernández Carmona Duración de la revisión un día hábil.

19.3. Resultados de la evaluación y pruebas a las medidas de seguridad

UNAM - Los Ángeles (Centro de Estudios Mexicanos)		
Identificador único*	**Expedientes del personal UNAM LA**	
(Nombre del sistema A5)*	**Expedientes del personal**	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***
Principio del menor privilegio	Se encontró que todas las cuentas de usuarios del sistema cuentan con los privilegios correspondientes.	Responsable de realizar la revisión Alfredo Fernández Carmona Revisión realizada el 2 de noviembre de 2022.
Revisión de respaldos de la información	Se cuentan con respaldo realizados y en la ubicación correspondiente.	Responsable de realizar la revisión Alfredo Fernández Carmona Revisión realizada el 2 de noviembre de 2022.

19.4. Acciones para la corrección y actualización de las medidas de seguridad

UNAM - Los Ángeles (Centro de Estudios Mexicanos)		
Identificador único*	**Expedientes del personal UNAM LA**	
(Nombre del sistema A5)*	**Expedientes del personal**	
Medida de seguridad*	**Acciones***	**Responsable***
Programa anual para evaluar medidas de seguridad.	Se revisaron las medidas implantadas. No se requirieron medidas correctivas.	Responsable de las acciones Alfredo Fernández Carmona. Fecha de conclusión de 02 de noviembre de 2022.

20. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

20.1. Programa de capacitación a los responsables de tratamiento de datos personales

UNAM - Los Ángeles (Centro de Estudios Mexicanos)			
Identificador único*	**Expedientes del personal UNAM LA**		
(Nombre del sistema A5)*	**Expedientes del personal**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Programa de capacitación que se relaciona con las medidas de seguridad técnica para la protección de datos personales en posesión de la UNAM, elaborado por DGETIC	Cursos en video que contribuyen a la formación y capacitación del personal a cargo de la protección de los datos personales en la UNAM en las entidades y dependencias	Fec ha de inicio 01 de diciembre de 2022 fecha de término 31 de enero de 2023	Responsable del sistema. Sin Vigencia. Sin frecuencia de actualización.

20.2. Programa de difusión de la protección a los datos personales

UNAM - Los Ángeles (Centro de Estudios Mexicanos)			
Identificador único*	**Expedientes del personal UNAM LA**		
(Nombre del sistema A5)*	**Expedientes del personal**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
No se cuenta con un programa de difusión de la protección de datos personales.			

21. MEJORA CONTINUA

21.1. Actualización y mantenimiento de sistemas de información

UNAM - Los Ángeles (Centro de Estudios Mexicanos)			
Identificador único*	**Expedientes del personal UNAM LA**		
(Nombre del sistema A5)*	**Expedientes del personal**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
N/A	N/A	N/A	N/A

21.2. Actualización y mantenimiento de equipo de cómputo

UNAM - Los Ángeles (Centro de Estudios Mexicanos)			
Identificador único*	**Expedientes del personal UNAM LA**		
(Nombre del sistema A5)*	**Expedientes del personal**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Mantenimiento preventivo	Realizar el mantenimiento preventivo del equipo de cómputo tanto a nivel hardware como software para su funcionamiento óptimo.	1 vez por año	Equipos de cómputo de los usuarios del sistema.

21.3. Procesos para la conservación, preservación y respaldos de información

UNAM - Los Ángeles (Centro de Estudios Mexicanos)		
Identificador único*	**Expedientes del personal UNAM LA**	
(Nombre del sistema A5)*	**Expedientes del personal**	
Proceso*	**Descripción***	**Responsable***
Respaldos periódicos de información	De manera anual se genera una copia de todos los archivos del sistema en un disco duro externo	Responsable de realizar respaldo Alfredo Fernández Carmona. Se lleva a cabo en 1 día hábil.

Por el momento no se cuenta con procesos de conservación y preservación de la información distintos a la generación de respaldos informáticos.

21.4. Procesos de borrado seguro y disposición final de equipos y componentes informáticos

UNAM - Los Ángeles (Centro de Estudios Mexicanos)		
Identificador único*	**Expedientes del personal UNAM LA**	
(Nombre del sistema A5)*	**Expedientes del personal**	
Proceso*	**Descripción***	**Responsable***
Borrado seguro de información	Borrado seguro de información Con base en la circular DGTIC/003/2017, utilizando la herramienta de borrado seguro SDelete.	Responsable del proceso de borrado seguro Alfredo Fernández Carmona Tiempo máximo de ejecución 1 día hábil.

El sistema no se aloja en equipos informáticos, por lo que no aplica el proceso de disposición final de equipos.

22. PROCEDIMIENTO PARA LA CANCELACIÓN DE UN SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

1. Titular de la sede deberá solicitar la cancelación por escrito al encargado del sistema explicando los motivos y tiempo que deberá permanecer disponible para consulta.
2. El responsable del sistema deberá realizar la suspensión de las credenciales de acceso al sistema o en su caso, bloquear el apartado inicio de sesión del mismo.
3. El responsable del sistema deberá notificar al Titilar de la sede de las acciones realizadas para lograr la cancelación temporal del sistema.
4. Una vez transcurrida la temporalidad en que el sistema quedó bloqueado, el encargado del sistema iniciará la eliminación segura del mismo siguiendo el procedimiento establecido de Borrado seguro.
5. El responsable del sistema notificará al Titular de la sede de que el sistema ha sido cancelado.

Así mismo en el momento de la cancelación del sistema se deberán definir los siguientes puntos:

U) DATOS DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES QUE SERÁ CANCELADO:

a) Denominación
b) Motivo de la cancelación

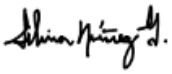
V) PLAZOS Y CONDICIONES PARA EL BLOQUEO DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES:
(Señalar el periodo de bloqueo, considerando los plazos de prescripción para el ejercicio de algún derecho por parte de los titulares de conformidad con la normatividad de cada área universitaria. Asimismo, se debe señalar las condiciones y el procedimiento que se seguirá para realizar el bloqueo)

W) MEDIDAS DE SEGURIDAD PARA EL BLOQUEO Y POSTERIOR SUPRESIÓN DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES:
(Describir las medidas de seguridad aplicables al periodo de bloqueo y la supresión del sistema, considerando el nivel de protección requerido en virtud del tipo de datos personales contenidos en el sistema)

X) PROCEDIMIENTO PARA LA SUPRESIÓN DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES
(Describir el procedimiento para suprimir el sistema, una vez cumplido el plazo de bloqueo)

Y) MECANISMOS PARA LA SUPRESIÓN DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES
(Describir las técnicas para la eliminación física del sistema)

23. APROBACIÓN DEL DOCUMENTO DE SEGURIDAD

		Nombre y firma de quienes revisaron el presente documento:
Responsable del desarrollo:	Alfredo Fernández Carmona Coordinador de Relaciones y Gestión Tel. 001-213-627-3930 afernandez@unamla.org	
Revisó:	Alfredo Fernández Carmona Coordinador de Relaciones y Gestión Tel. 001-213-627-3930 afernandez@unamla.org	
Autorizó:	Silvia Núñez García Directora Tel. 001-213-627-3930 silnugs@gmail.com	
Fecha de aprobación:	(Incluir la fecha de liberación del documento)	04 de noviembre de 2022
Fecha de actualización:	(Incluir la primera versión e ir agregando las subsiguientes del documento)	

UNAM-COSTA RICA

CENTRO DE ESTUDIOS MEXICANOS

2. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

(Denominación del área específica del Área Universitaria A)	
Identificador único*	SV_CR
(Nombre del sistema A1) *	Asistencia Seminario Virtual UNAM-Costa Rica y Charlando de…
Datos personales (sensibles o no) contenidos en el sistema*:	(Nombre, apellido paterno, apellido materno, correo electrónico, sexo, país, autorización para recibir información de eventos, institución de educación superior.
Responsable*:	
Nombre*:	Carlos Miguel Valdés González
Cargo*:	Director
Funciones*:	Supervisión del tratamiento de los datos personales de los asistentes a eventos de UNAM-Costa Rica Brindar los datos personales cuando sean solicitados por un encargado autorizado.
Obligaciones*:	Acatar las disposiciones para cumplir con el tratamiento de los datos personales de asistentes a eventos de UNAM-Costa Rica.
	Encargados:
(Nombre del Encargado 1*)	César Antonio Ríos Muñoz
Cargo*:	Coordinador de Relaciones y Gestión
Funciones*:	Elaboración de formularios de registro de actividades, salvaguarda de información y elaboración de estadísticas relacionadas con el registro de asistentes.
Obligaciones*:	Mantener a resguardo la información proporcionada por los asistentes a los eventos de UNAM-Costa Rica. No difundir información de los datos personales No modificar la información almacenada en el servidor No hacer respaldos en equipo personal de la información de datos personales
	Usuarios:
(Nombre del Usuario 1*)	Paola Suyette Mendieta Verdejo
Cargo*:	Jefa del Departamento de Apoyo Académico a las sedes en el extranjero
Funciones*:	Comprobar y la información vertida en el formato de Actividades Académicas y Culturales.
Obligaciones*:	No difundir información de los datos personales No modificar la información almacenada en el servidor No hacer respaldos en equipo personal de la información de datos personales

(Nombre del Usuario 2*)	No aplica
Sistema (Nombre del A2)*:	CC_CR
Datos personales contenidos en el sistema*:	Asistencia Cineclub “Pura Vida” UNAM-Costa Rica …
	Responsable:
Nombre*:	Carlos Miguel Valdés González
Cargo*:	Director
Funciones*:	Supervisión del tratamiento de los datos personales de los asistentes a eventos de UNAM-Costa Rica Brindar los datos personales cuando sean solicitados por un encargado autorizado.
Obligaciones*:	Acatar las disposiciones para cumplir con el tratamiento de los datos personales de asistentes a eventos de UNAM-Costa Rica.
	Encargados:
(Nombre del Encargado 1*)	César Antonio Ríos Muñoz
Cargo*:	Coordinador de Relaciones y Gestión
Funciones*:	Elaboración de formularios de registro de actividades, salvaguarda de información y elaboración de estadísticas relacionadas con el registro de asistentes.
Obligaciones*:	Mantener a resguardo la información proporcionada por los asistentes a los eventos de UNAM-Costa Rica. No difundir información de los datos personales No modificar la información almacenada en el servidor No hacer respaldos en equipo personal de la información de datos personales
	Usuarios:
(Nombre del Usuario 1*)	Paola Suyette Mendieta Verdejo
Cargo*:	Jefa del Departamento de Apoyo Académico a las sedes en el extranjero
Funciones*:	Comprobar y la información vertida en el formato de Actividades Académicas y Culturales.
Obligaciones*:	No difundir información de los datos personales No modificar la información almacenada en el servidor No hacer respaldos en equipo personal de la información de datos personales

2. ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

(Denominación del área específica del Área Universitaria A) *	
Identificador único¨*	SV_CR
(Nombre del sistema A1*)	Asistencia Seminario Virtual UNAM-Costa Rica y Charlando de…
Tipo de soporte:	Electrónico
Descripción:	Base de datos
Características del lugar donde se resguardan los soportes:	Alojamiento en nube privada de UNAM-Costa Rica Discos duros externos (respaldos)
(Nombre del sistema A2*)	Asistencia Cineclub “Pura Vida” UNAM-Costa Rica
Tipo de soporte*:	Electrónico
Descripción*:	Base de datos
Características del lugar donde se resguardan los soportes*:	Alojamiento en nube privada de UNAM-Costa Rica Discos duros externos (respaldos)

3. ANÁLISIS DE RIESGOS

(Denominación del área específica del Área Universitaria A)*		
Identificador único*	SV_CR	
(Nombre del sistema A1) *	Asistencia Seminario Virtual UNAM-Costa Rica y Charlando de…	
Riesgo*	**Impacto***	**Mitigación***
Acceso a la cuenta de Google drive de UNAM-Costa Rica a causa de una contraseña débil.	Acceso al sistema y modificación no autorizada de la información y datos	Cambiar la contraseña de acceso a la computadora y al sistema aplicando las “Políticas de contraseñas”.
Robo de soporte electrónico de almacenamiento (USB, CD, DVD, etc.)	Acceso a la información contenida en el dispositivo de almacenamiento y posible difusión y revelación de la información.	Asignar contraseñas a los archivos electrónicos que contengan datos personales. Mantener los soportes electrónicos de almacenamiento en gavetas bajo llave a cargo del responsable y el encargado.
Identificador único*	SV_CR	
(Nombre del sistema A2) *	Asistencia Seminario Virtual UNAM-Costa Rica y Charlando de…	
Riesgo*	**Impacto***	**Mitigación***
Acceso a la cuenta de Google drive de UNAM-Costa Rica a causa de una contraseña débil.	Acceso al sistema y modificación no autorizada de la información y datos	Cambiar la contraseña de acceso a la computadora y al sistema aplicando las “Políticas de contraseñas”
Robo de soporte electrónico de almacenamiento (USB, CD, DVD, etc.)	Acceso a la información contenido en el dispositivo de almacenamiento y posible difusión y revelación de la información.	Asignar contraseñas a los archivos electrónicos que contengan datos personales. Mantener los soportes electrónicos de almacenamiento en gavetas bajo llave a cargo del responsable y el encargado.

7. ANÁLISIS DE BRECHA

(Denominación del área específica del Área Universitaria A)*		
Identificador único*	SV_CR	
(Nombre del sistema A1) *	Asistencia Seminario Virtual UNAM-Costa Rica y Charlando de…	
Medida de seguridad actual*	**Medida de seguridad necesaria***	**Acciones para remediación***
Usuarios autorizados para consulta de datos personales.	Contraseñas robustas para usuarios autorizados por el titular correspondiente.	Tener un protocolo de contraseñas seguras y actualizarlas al menos cada semestre.
Acceso a los soportes electrónicos de almacenamiento solo por el responsable y el encargado.	Correcto	No es necesario
Identificador único*	CC_CR	
(Nombre del sistema A2) *	Asistencia Cineclub “Pura Vida” UNAM-Costa Rica	
Medida de seguridad actual*	**Medida de seguridad necesaria***	**Acciones para remediación***
Usuarios autorizados para consulta de datos personales	Contraseñas robustas para usuarios autorizados por el titular correspondiente	Tener un protocolo de contraseñas seguras y actualizarlas al menos cada semestre
Acceso a los soportes electrónicos de almacenamiento solo por el responsable y el encargado	Correcto	No es necesario

8. PLAN DE TRABAJO

UNAM-Costa Rica (Centro de Estudios Mexicanos)			
Identificador único	SV_CR		
(Nombre del sistema A1)	Asistencia Seminario Virtual UNAM-Costa Rica y Charlando de…		
Actividad*	**Descripción***	**Duración***	**Cobertura***
No hay actividades para reportar	*No aplica*	*No aplica*	*No aplica*
Identificador único*	CC_CR		
(Nombre del sistema A2)	Asistencia Cineclub “Pura Vida” UNAM-Costa Rica		
No hay actividades para reportar	*No aplica*	*No aplica*	*No aplica*

9. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

XLVI. TRANSFERENCIAS DE DATOS PERSONALES

(Denominación del área específica del Área Universitaria A)*	
Identificador único*	SV_CR
(Nombre del sistema A1)*	Asistencia Seminario Virtual UNAM-Costa Rica y Charlando de…
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	No aplica
Transferencias mediante el traslado de soportes electrónicos:	No aplica
Transferencias mediante el traslado sobre redes electrónicas:	No aplica

II. RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS

1. Señalar las medidas de seguridad que ha implementado el área universitaria para el resguardo de los soportes físicos del sistema de manera que evite la alteración, pérdida o acceso no autorizado a los mismos.

No se cuenta con soportes físicos

2. Señalar en un listado las personas (nombre, cargo, funciones y obligaciones) que tienen acceso a los soportes físicos del sistema.

No se cuenta con soportes físicos

III. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

1. Los datos que se registran en las bitácoras:

UNAM-Costa Rica no cuenta con bitácoras de acceso y operación cotidiana. Las bitácoras de acceso son controladas por el personal de la Universidad de Costa Rica.

a) Quién accede a los datos personales, fecha y hora en la que se realiza el acceso o se intenta el mismo, propósito del acceso, así como fecha y hora de salida;
b) Para soportes físicos: Número o clave del expediente utilizado, y
c) Para soportes electrónicos: Operaciones o acciones llevadas a cabo y registros utilizados de la base de datos.

25. Si las bitácoras están en soporte físico o en soporte electrónico;
26. Lugar dónde almacena las bitácoras y por cuánto tiempo;
27. La manera en que asegura la integridad de las bitácoras, y
28. Respecto del análisis de las bitácoras:

a) Quién es el responsable de analizarlas (si es el área universitaria o si es un tercero) y cada cuándo las analiza, y
b) Para el caso de que las bitácoras estén en soporte electrónico: las herramientas de análisis utilizadas.

IV. REGISTRO DE INCIDENTES:

Describir el procedimiento de atención de incidentes que tiene implementado el área universitaria y especificar si lleva registro de los incidentes relativos a soportes físicos, como lo son la pérdida o alteración no autorizada de expedientes, y para el caso de soportes electrónicos, ofrecer detalles sobre el registro de incidentes en el cual consigne los procedimientos realizados para la recuperación de los datos o para permitir la disponibilidad del proceso.

UNAM-Costa Rica no cuenta con registro de incidentes.

1. Los datos que registra:

a) La persona que resolvió el incidente;
b) La metodología aplicada;
c) Para soportes físicos: Los oficios, documentos, expedientes, estantes o archiveros, tanto los dañados como los recuperados, y
d) Para soportes electrónicos: Los campos, registros, tablas, bases de datos o archivos electrónicos, tanto dañados como recuperados, el nombre de los sistemas y la infraestructura afectada, indicar si el incidente afectó el servidor principal y los servidores de respaldo, etc.

2. Si el registro está en soporte físico o en soporte electrónico;
3. Cómo asegura la integridad de dicho registro, y
4. Para el caso de soportes electrónicos, quién autoriza la recuperación de datos.

V. ACCESO A LAS INSTALACIONES

13. Seguridad perimetral exterior (las instalaciones del área universitaria):

La seguridad perimetral exterior depende completamente de la Universidad de Costa Rica.

¿Qué medidas ha implementado para controlar el acceso de personas a sus instalaciones? Por ejemplo, se espera que describa si cuenta con uno o más puntos de control de acceso y quienes los operan, si tiene vigilancia las 24 horas, si ha levantado bardas o cercas, si existe un sistema de tratamiento de datos personales de videovigilancia, entre otras posibles medidas.

Para las personas que acceden a sus instalaciones:

a) ¿Cómo las identifica?
b) ¿Cómo las autentifica?
c) ¿Cómo les autoriza el acceso?

14. Seguridad perimetral interior (oficina, almacén o bodega para soportes físicos, centro de datos para soportes electrónicos):

La seguridad perimetral interior depende completamente de la Universidad de Costa Rica.

¿Qué medidas de seguridad ha implementado para controlar el acceso a los espacios donde almacena los soportes físicos o electrónicos del sistema? Por ejemplo, se espera que precise el tipo de puertas y cerraduras instaladas, si tiene instalados controles biométricos, si administra la asignación de llaves y/o claves de acceso para abrir puertas y/o estantería, si cuenta con vigilancia las 24 horas, si hay un sistema de tratamiento de datos personales de videovigilancia, entre otras medidas.

Para las personas que acceden a dichos espacios interiores:

1. ¿Cómo las identifica?
2. ¿Cómo las autentifica?
3. ¿Cómo les autoriza el acceso?

VI.ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

Los datos personales que son solicitados por UNAM-Costa Rica son únicamente para eventos académico-culturales, no requieren actualización.

En este apartado se deberá establecer un mecanismo o procedimiento institucional para la actualización de la información personal contenida en el sistema, en donde se establezca la frecuencia con la que se efectúa y la forma en que se está solicitando al titular acreditar de manera idónea sus requerimientos de rectificación de datos inexactos).

Las medidas de seguridad previstas a continuación en los incisos VII al IX, sólo aplican para soportes electrónicos

VII. PERFILES DE USUARIO Y CONTRASEÑAS

UNAM-Costa Rica no cuenta con sistemas que requieran perfil de usuario y contraseñas.

En este rubro el área universitaria deberá describir el esquema de perfiles de usuario y contraseñas que tiene implementado para control de acceso mediante una red electrónica.

1. Modelo de control de acceso (alguno de los siguientes):

a) ¿Es obligatorio (etiquetas para objetos y acreditación para sujetos)?
b) ¿Es discrecional (matriz de control de acceso)?
c) ¿Está basado en roles (perfiles) o grupos?
d) ¿Está basado en reglas?

3. Perfiles de usuario y contraseñas en el sistema operativo de red:

a) ¿Cuenta con un sistema operativo de red instalado en sus equipos?
b) ¿Proporciona dicho sistema operativo un manejo riguroso de perfiles de usuario y contraseñas?
c) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?

4. Perfiles de usuario y contraseñas manejados por el software aplicativo del sistema de tratamiento de datos personales:

a) ¿Ofrece dicho software un manejo riguroso de perfiles de usuario y contraseñas?
b) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?

5. Administración de perfiles de usuario y contraseñas:

a) ¿Quién da de alta nuevos perfiles?
b) ¿Quién autoriza la creación de nuevos perfiles?
c) ¿Se lleva registro de la creación de nuevos perfiles?

6. Acceso remoto al sistema de tratamiento de datos personales:

a) ¿Requieren los usuarios acceso remoto al equipo de cómputo que por lo general utilizan para trabajar con el sistema?
b) ¿Requiere el administrador acceso remoto al equipo donde reside el sistema para realizar tareas de mantenimiento?
c) ¿Cómo se evita el acceso remoto no autorizado?

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

UNAM-Costa Rica no cuenta con procedimientos de respaldo y recuperación de datos.

19. Señalar si realiza respaldos

a) Completos__, diferenciales ___ o incrementales___;
b) De forma automática ____ o Manual _____,
c) Periodicidad con que los realiza: _____

20. El tipo de medios (por ejemplo: cintas magnéticas, discos duros, CD-ROM, entre otros) que utiliza para almacenar las copias de seguridad;

21. Cómo y dónde archiva esos medios, y

22. Quién es el responsable de realizar estas operaciones (el área universitaria o un tercero).

IX. PLAN DE CONTINGENCIA

UNAM-Costa Rica no cuenta con plan de contingencia.

16. Presentar el plan de contingencia con el cual garantiza la continuidad de la operación del sistema o informar si no lo tiene, pero se encuentra desarrollándolo.

17. Si cuenta con plan de contingencia y lo ha implementado, deberá indicar si realiza pruebas de eficiencia de este.

18. Informar si cuenta con un sitio redundante (alterno) y señalar lo siguiente:

a) El tipo de sitio (caliente, tibio o frío);
b) Si el sitio es propio o subcontratado con un tercero;
c) Los procedimientos, el equipo y el personal que designa para poner en marcha tal sitio y
d) Tiempo que le lleva poner en marcha el sitio, según las pruebas de eficiencia.

Continuar los mismos pasos con el siguiente SISTEMA A2. (Nombre del sistema A2), B1. (Nombre del sistema B1), etc.

I. Transferencias de datos personales
II. Resguardo de sistemas de tratamiento de datos personales con soportes físicos
III. Bitácoras para accesos y operación cotidiana
IV. Registro de incidentes
V. Acceso a las instalaciones
VI. Actualización del sistema de tratamiento de datos personales
VII. Perfiles de usuario y contraseñas
VIII. Procedimientos de respaldo y recuperación de datos
IX. Plan de contingencia

7. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

UNAM-Costa Rica no cuenta con mecanismos de monitoreo y revisión de medidas de seguridad

Herramientas y recursos para monitoreo de la protección de datos personales

(Denominación del área específica del Área Universitaria A)*		
Identificador único*	*Usar el identificador único declarado en el inciso 1. que corresponda*	
(Nombre del sistema A1)*		
Recurso*	**Descripción***	**Control***
Describa la herramienta o el recurso para monitorear la protección de datos personales. Agregue un renglón para cada uno	*Indique el tipo de herramienta o recurso, tales como auditorías internas, revisiones aleatorias, pruebas de penetración, etc.*	*Indique la forma de controlar y verificar el uso o aplicación de la herramienta de protección y el responsable de ello.* (ingresar el tipo de licencia, duración y la cantidad de licencias con las que se cuentan)

23.1. Procedimiento para la revisión de las medidas de seguridad

(Denominación del área específica del Área Universitaria A)*		
Identificador único*		
(Nombre del sistema A1)*	**(Nombre del sistema A1)***	
Medida de seguridad*	**Procedimiento***	**Responsable***
Indique la medida de seguridad correspondiente al procedimiento de revisión. Agregue un renglón por cada medida.	*Indique el procedimiento para la revisión de la medida de seguridad, tales como comprobación de actualización, pruebas de penetración, revisión de estabilidad, etc.*	*Indicar:* *a) nombre del responsable del procedimiento* *b) tiempo máximo de ejecución en días.*

23.2. Resultados de la evaluación y pruebas a las medidas de seguridad

(Denominación del área específica del Área Universitaria A)*		
Identificador único*		
(Nombre del sistema A1)*	**(Nombre del sistema A1)***	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***
Indique la medida de seguridad Agregue un renglón por cada medida.	*Indique el resultado de la evaluación de la medida de seguridad*	*Indicar:* *a) nombre del responsable de la evaluación* *b) fecha de conclusión.*

23.3. Acciones para la corrección y actualización de las medidas de seguridad

(Denominación del área específica del Área Universitaria A)*		
Identificador único*		
(Nombre del sistema A1)*	**(Nombre del sistema A1)***	
Medida de seguridad*	**Acciones***	**Responsable***
Indique la medida de seguridad (Agregue un renglón por cada medida).	*Indique las acciones aplicables para corregir o actualizar la medida de seguridad.* a) Precisar las acciones correctivas. b) Precisar las acciones preventivas.	*Indicar:* *a) nombre del responsable de las acciones* *b) fecha límite de conclusión.*

24. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

UNAM-Costa Rica no cuenta con programa específico de capacitación

24.1. Programa de capacitación a los responsables de tratamiento de datos personales

(Denominación del área específica del Área Universitaria A)*			
Identificador único*			
(Nombre del sistema A1)*	**(Nombre del sistema A1)***		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Indique actividad, tema, curso, material didáctico o recurso educativo para la capacitación. Agregar un renglón por cada elemento	*Describa el tipo de elemento, sus objetivos y forma de impartición, publicación o distribución*	*Indique duración del elemento en horas, días, meses, su fecha de inicio y de término*	*Mencione público objetivo, vigencia del elemento y frecuencia de actualización*

24.2. Programa de difusión de la protección a los datos personales

(Denominación del área específica del Área Universitaria A)*			
Identificador único*			
(Nombre del sistema A1)*	**(Nombre del sistema A1)***		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Indique actividad, tema, recursos para la difusión. Agregar un renglón por cada elemento	*Describa el tipo de elemento, sus objetivos y forma de impartición, publicación o distribución*	*Indique duración del elemento en horas, días, meses, su fecha de inicio y de término*	*Mencione público objetivo, vigencia del elemento y frecuencia de actualización*

25. MEJORA CONTINUA

UNAM-Costa Rica no cuenta con un sistema de actualización

25.1. Actualización y mantenimiento de sistemas de información

(Denominación del área específica del Área Universitaria A)*			
Identificador único*			
(Nombre del sistema A1)*	**(Nombre del sistema A1)***		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Indique actividad. Agregar un renglón por cada elemento	*Describa el tipo de actividad, sus objetivos e impacto la actualización o mantenimiento del sistema de información*	*Indique duración en la ejecución de la actividad en horas, días, meses, su fecha de inicio y de término*	*Mencione los aspectos del sistema de información que son resueltos, total o parcialmente, por la actividad.*

Actualización y mantenimiento de equipo de cómputo

(Denominación del área específica del Área Universitaria A)*			
Identificador único*			
(Nombre del sistema A1)*	**(Nombre del sistema A1)***		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Indique actividad. Agregar un renglón por cada elemento	*Describa el tipo de actividad, sus objetivos e impacto la actualización o mantenimiento del equipo de cómputo*	*Indique duración en la ejecución de la actividad en horas, días, meses, su fecha de inicio y de término*	*Mencione los aspectos de equipo de cómputo que son resueltos, total o parcialmente, por la actividad.*

25.2. Procesos para la conservación, preservación y respaldos de información

(Denominación del área específica del Área Universitaria A)*		
Identificador único*		
(Nombre del sistema A1)*	**(Nombre del sistema A1)***	
Proceso*	**Descripción***	**Responsable***
Indique el proceso en materia de conservación, preservación y respaldo de información. Agregue un renglón por proceso	*Describa el proceso en todas sus acciones.*	*Indicar:* *a) Nombre del responsable del proceso* *b) Tiempo máximo de ejecución en días.*

25.3. Procesos de borrado seguro y disposición final de equipos y componentes informáticos

(Denominación del área específica del Área Universitaria A)*		
Identificador único*		
(Nombre del sistema A1)*	**(Nombre del sistema A1)***	
Proceso*	**Descripción***	**Responsable***
Indique el proceso en materia de borrado seguro, disposición final de equipos o componentes de cómputo. Agregue un renglón por proceso	*Describa el proceso en todas sus acciones.*	*Indicar:* *a) Nombre del responsable del proceso* *b) Tiempo máximo de ejecución en días.*

26. PROCEDIMIENTO PARA LA CANCELACIÓN DE UN SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

Al recopilar únicamente información para eventos académico-culturales, UNAM-Costa Rica no requiere un procedimiento de cancelación de tratamiento de datos personales.

(Informar y describir el procedimiento para la cancelación de un sistema de tratamiento de datos personales.)

Z) DATOS DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES QUE SERÁ CANCELADO:

a) Denominación
b) Motivo de la cancelación

AA) PLAZOS Y CONDICIONES PARA EL BLOQUEO DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES:

(Señalar el periodo de bloqueo, considerando los plazos de prescripción para el ejercicio de algún derecho por parte de los titulares de conformidad con la normatividad de cada área universitaria. Asimismo, se debe señalar las condiciones y el procedimiento que se seguirá para realizar el bloqueo)

BB) MEDIDAS DE SEGURIDAD PARA EL BLOQUEO Y POSTERIOR SUPRESIÓN DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES:
(Describir las medidas de seguridad aplicables al periodo de bloqueo y la supresión del sistema, considerando el nivel de protección requerido en virtud del tipo de datos personales contenidos en el sistema)

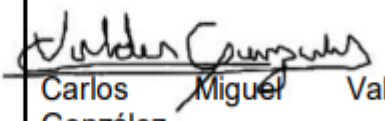
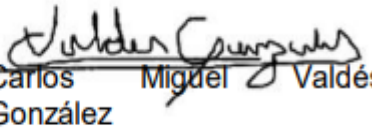
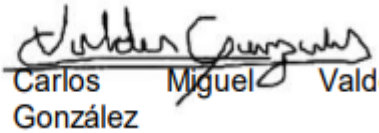
CC) PROCEDIMIENTO PARA LA SUPRESIÓN DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

(Describir el procedimiento para suprimir el sistema, una vez cumplido el plazo de bloqueo)

DD) MECANISMOS PARA LA SUPRESIÓN DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

(Describir las técnicas para la eliminación física del sistema)

11. APROBACIÓN DEL DOCUMENTO DE SEGURIDAD

		Nombre y firma de quienes revisaron el presente documento:
Responsable del desarrollo:	No aplica	 Carlos Miguel Valdés González
Revisó:	No aplica	 Carlos Miguel Valdés González
Autorizó:	No aplica	 Carlos Miguel Valdés González
Fecha de aprobación:	No aplica	
Fecha de actualización:	No aplica	

ANEXOS COSTA RICA

ANEXO II. FORMATO UNIVERSITARIO DE "SOLICITUD DE EJERCICIO DE DERECHOS ARCO"

Formato de solicitud de ejercicio de derechos Acceso, Rectificación, Cancelación y Oposición (ARCO)

Con fundamento en el artículo 54 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, esta área universitaria le solicita llenar el presente formato para ejercer sus derechos de Acceso, Rectificación, Cancelación y Oposición.

1. Datos del Área Universitaria de la UNAM responsable de tratar los datos personales*:

2. Datos del Titular de los Datos Personales*:

Primer apellido:	Segundo apellido:	Nombre(s):
CURP (para evitar homónimos):		

3. Datos del solicitante:

Primer apellido:	Segundo apellido:	Nombre(s):
Indicar si los datos corresponden a:		
☐Titular		
☐Menor de edad		
☐Persona que se encuentren en estado de interdicción o incapacidad establecida por ley.		
☐Fallecida		
Datos de identidad y representación legal (opcional, solo si usted no es el titular de los datos personales)		
☐Persona física:		
☐Nombre completo del representante:		
☐Representación de un menor de edad:		
☐Representación de una persona que se encuentren en estado de interdicción o incapacidad establecida por ley.		
☐Persona moral:		
☐Nombre o razón social del representante:		
Registro Federal de Contribuyentes (RFC):		
Documento con el que acredita la representación:		
☐Poder notarial ☐Carta poder simple signada ante dos testigos (con copia de los documentos que acrediten la identidad de los testigos y titular) ☐Declaración en comparecencia del Titular (en las instalaciones del área universitaria).		

4. Documento oficial de identificación del titular o solicitante (sólo originales) *:

☐Credencial para votar (INE)	☐Pasaporte	☐Licencia de conducir
☐Cédula profesional	☐Cartilla del Servicio militar nacional	☐Documento migratorio
☐Acta de nacimiento	☐Acta de defunción	☐Otra identificación con fotografía (especifique):

5. Medio por el cual prefiere que le sea notificada la puesta a disposición de la respuesta*:

☐Acudir al área universitaria donde presentó este formato	☐Correo electrónico (especificar):

6. Modalidad en la cual prefiere le sean entregados los datos, en caso de ser procedente. *

☐C opia simple	☐Correo electrónico
☐Copia certificada	☐ Otro medio electrónico como USB/CD ROOM/ DVD *(previo depósito de ficha de pago):*
☐Consultas directas	☐Yo proporciono el medio magnético o electrónico para reproducir los datos personales.

7. Tipo de solicitud de ejercicio de Derechos Acceso, Rectificación, Cancelación y Oposición (ARCO) a datos personales*:

☐ACCESO
Describir la información datos personales que obran en posesión del área universitaria y a los que requiere tener acceso*: _____ _____ _____ _____ _____
Señalar el nombre y ubicación del archivo o registro de datos personales*: _____ _____ _____ _____ _____
☐RECTIFICACIÓN
☐Son inexactos.
☐Son incompletos.
☐Requieren ser actualizados
Justificación y documentación original que acompaña para motivar su petición*: _____ _____ _____ _____
CANCELACIÓN (supresión o eliminación)
Causas que motivan la cancelación*:
OPOSICIÓN (cese del tratamiento)
Causas que motivan la oposición (daño o perjuicio que le causa la persistencia del tratamiento de sus datos)*:_____ _____ _____ _____
Señalar si es para una finalidad específica o para todos los sistemas de información que obren en el área universitaria*._____ _____
Documentación original que acompaña para motivar su petición*: _____ _____
Señalar la referencia o documento que facilite la localización de sus datos personales*
_____ _____

Leí el Aviso de privacidad del área universitaria a la que acudo y en este acto otorgo el consentimiento para que mis datos personales sean tratados conforme al mismo.

_____

Firma o huella dactilar*

Plazos y procedimiento para la atención de las solicitudes de ejercicio de derechos ARCO:
Una vez que se presentó la solicitud, esta área universitaria cuenta con:

• Un plazo de 20 días hábiles, contados a partir del día siguiente a la recepción de la solicitud, para informarle si procede o no el ejercicio del derecho solicitado.
• Un plazo de 15 días hábiles, contados a partir del día siguiente en el que le haya notificado la respuesta anterior, en caso de que haya procedido el ejercicio del derecho, deberá llevar a cabo las acciones necesarias para hacerlo efectivo.

El ejercicio de los derechos ARCO será sencillo y gratuito, siempre que no rebase las 20 hojas simples, por lo que las áreas universitarias realizarán el cobro del costo de reproducción de acuerdo con los Lineamientos para la determinación de los costos de reproducción y envío en el marco de solicitudes de acceso a Información y entrega de datos personales en la Universidad Nacional Autónoma de México.

Carta compromiso de confidencialidad, no divulgación, reserva y resguardo de información y datos personales

CIUDAD DE _____, A (DD-MM-AAAA)

(Nombre completo), *(cargo)*, adscrita(o) *(dependencia/entidad de adscripción)* de la Universidad Nacional Autónoma de México (en adelante la UNAM) acepto los términos y condiciones, que se describen más adelante, de resguardo, reserva, custodia y protección de la seguridad y confidencialidad de la información, datos personales y de todo tipo de documentos propiedad de la UNAM de los que tenga conocimiento, con motivo de las funciones que desempeño en la Universidad.

El presente compromiso me responsabiliza respecto de la información que me sea proporcionada por la UNAM, ya sea de forma oral, escrita, impresa, sonora, visual, electrónica, informática u holográfica, contenida en cualquier tipo de documento, que puede consistir en: expedientes, reportes, estudios, actas, resoluciones, oficios, correspondencia, acuerdos, directivas, directrices, circulares, contratos, convenios, instructivos, notas, memorandos, estadísticas, o bien, cualquier otro registro en medio conocido o por conocer que documente el ejercicio de las facultades, funciones y competencias del área universitaria y de los servidores universitarios, sin importar su fuente o fecha de elaboración.

La información que me sea proporcionada podría ser considerada, según el caso, como reservada, privilegiada y confidencial, en los términos de las leyes aplicables, por lo que me obligo a protegerla, reservarla, resguardarla y no divulgarla, utilizándola única y exclusivamente para llevar a cabo y cumplir con las actividades y obligaciones que expresamente me sean conferidas por la Universidad.

Es mi responsabilidad no reproducir, hacer pública o divulgar a terceros la información objeto de la presente Carta, y de cumplir con las medidas de seguridad adecuadas al tipo de documento con el que se trabaje.

Mi obligación de confidencialidad no es aplicable en los siguientes casos:

a) Cuando la información se encuentre en el dominio público en el momento en que me sea suministrada o, una vez suministrada, ésta se haga pública.
b) Cuando la legislación vigente o un mandato judicial exija su divulgación.
c) Cuando la información se desarrolle o reciba legítimamente de terceros, de forma totalmente independiente a mi relación con la Universidad.

A t e n t a m e n t e

_

Firma o huella dactilar

ANEXO IV. RUTA CRÍTICA PARA CUMPLIMIENTO DE LAS MEDIDAS DE SEGURIDAD TÉCNICAS (MST)

A continuación, se presentan los requisitos técnicos para sistemas de información, descritos en las MST del capítulo II de las Normas Complementarias, por orden de prioridad, esto es: de los mínimos indispensables para asegurar los datos personales hasta los necesarios para incrementar la protección de dichos datos.

Dada la complejidad de diversos sistemas en la UNAM, se ha dispuesto la ruta crítica para el cumplimiento de las MST en tres etapas para los sistemas de información que a la fecha de publicación de esta guía estén en producción o funcionamiento. Todo sistema de información deberá satisfacer a cabalidad el 100% de las MST en un tiempo máximo de un año contado a partir de la publicación de las MST para conservar su registro y publicación dentro del dominio institucional .***unam.mx***.

a) Etapa 1. Corto plazo. Requisitos de misión crítica y mínimos indispensables para la protección de datos personales y datos personales sensibles. Cumplimiento obligatorio en menos de treinta días hábiles.
b) Etapa 2. Mediano plazo. Requisitos importantes para garantizar la protección de datos personales y datos personales sensibles. Ejecución estimada entre un mes y seis meses.
c) Etapa 3. Largo plazo. Requisitos necesarios para reforzar la seguridad en la protección de datos personales y datos personales sensibles. Ejecución estimada entre seis y doce meses.

Instrucciones

- Para cada MST se ha diseñado un formato, el cual está numerado en correspondencia con la ruta crítica de cumplimiento.
- Se deberán completar todos los formatos aplicables por cada uno de los sistemas de información a cargo del Área Universitaria.
- Todos los formatos deberán integrar el anexo del documento de seguridad de datos personales.
- En el caso de los sistemas que estén en desarrollo al momento de la publicación de las Normas complementarias, deberán cumplir con el 100% de las MST, previo a su publicación como sistema en producción.
- Es requisito indispensable el cumplimiento de las MST para conservar el registro dominio institucional ***.unam.mx*** en el caso de servicios Web.

Núm. formato	Etapa	Duración estimada	Medidas de seguridad técnicas y proceso recomendado para su cumplimiento
ETAPA 1			
Anexo I, numerales 1 y 2	1	Un día hábil	**Generar el inventario de sistemas de tratamiento de datos personales y la Estructura de descripción de los sistemas de tratamiento de datos personales.** **A)** Integrar la información correspondiente a todos los sistemas que dan tratamiento de datos personales en el área universitaria. **B)** Llenar formatos y colocar nombre y firma de quien realizó la acción.
1	1	Un día hábil	**Artículo 18. I. c) Utilizar datos no personales durante el desarrollo y pruebas de los sistemas.** **A)** Realizar respaldo completo de la base de datos. **B)** Ejecutar consulta en el sistema de información, por medio de formato o comandos. **C)** Verificar que los datos usados en el desarrollo no correspondan a personas identificables. **D)** Si se usan datos de personas identificables, cambiar por datos genéricos o datos ficticios y regresar al punto B. **E)** Si no se usan datos de personas

Núm. formato	Etapa	Duración estimada	Medidas de seguridad técnicas y proceso recomendado para su cumplimiento
			identificables, llenar formato 1 con nombre y firma de quien realizó la acción, fecha de inicio y de conclusión.
2	1	Un día hábil	**Artículo 18. I. e) Asignar o revocar los privilegios de acceso para los usuarios teniendo como base el principio del menor privilegio.**
			A) Realizar respaldo completo de la base de datos. **B)** Ejecutar consulta en el sistema de información de la lista de usuarios y sus niveles o privilegios de acceso. **C)** Validar que los niveles de acceso son acordes a la relación del usuario con el tratamiento de datos personales. **D)** Si hay usuarios con privilegios mayores a los que les son necesarios, cambiar al mínimo indispensable e informarlo al usuario. Regresar al punto B. **E)** Si los privilegios de acceso son correctos para los usuarios, llenar formato 2 con nombre y firma de quien realizó la acción, fecha de inicio y de conclusión.
3	1	Tres días hábiles	**Artículo 18. I. g) Instalar y mantener vigentes certificados**

Núm. formato	Etapa	Duración estimada	Medidas de seguridad técnicas y proceso recomendado para su cumplimiento
			de comunicación segura SSL en el caso de servicios basados en Web.
			A) En caso de no tener un certificado SSL vigente, enviar correo electrónico al Departamento de Firma Electrónica de DGTIC a firma.tic@unam.mx solicitando la asignación. **B)** El Departamento de Firma Electrónica Avanzada envía procedimiento para obtención de CSR del servidor, formato de la solicitud y costos de recuperación en función del tipo de certificado requerido (organizacional, comodín o corporativo). **C)** Completar documentación, proceso y pago de costo de recuperación. Enviar comprobantes a firma.tic@unam.mx. **D)** Al recibir el certificado SSL, instalarlo en el servidor de acuerdo con las instrucciones recibidas junto con el certificado. **E)** Llenar formato 3 y colocar nombre y firma de quien realizó la acción.
4	1	Dos días hábiles	**Artículo 18. I. h) Definir el plan de respaldos de la información,**

Núm. formato	Etapa	Duración estimada	Medidas de seguridad técnicas y proceso recomendado para su cumplimiento
			incluyendo periodicidad y alcance.
			A) Elaborar documento con la secuencia de respaldos al menos con el siguiente orden: - Diario – incremental. - Semanal – incremental. - Mensual – total. **B)** Establecer en el plan los medios para resguardo del respaldo y su forma de identificación: - En línea: mismo equipo donde se ejecuta el sistema. - Respaldo como servicio: otro equipo de almacenamiento. - Fuera de línea: medios magnéticos (cintas, discos) y/u ópticos. **C)** Incluir en el plan: - Responsables de cada tipo y medio de respaldo. - Rotación de respaldos y medios. - Áreas de resguardo. - Métodos de cifrado. - RTO: *Recovery Time Objective*. Tiempo objetivo de recuperación. - RPO: *Recovery Point Objective*: Punto objetivo de recuperación. **D)** Concluir este documento, adjuntarlo a SGPDP, llenar formato 4 y colocar nombre y firma de quien realizó la acción.

Núm. formato	Etapa	Duración estimada	Medidas de seguridad técnicas y proceso recomendado para su cumplimiento
5	1	Un día hábil	**Artículo 18. I. i) Definir el procedimiento para el borrado seguro.**
			A) Elaborar documento con el procedimiento y la herramienta para borrado seguro en función del tipo de base de datos para registros, tablas y base de datos. **B)** Incluir en el documento de borrado seguro el proceso de verificación de la no existencia del dato, generalmente por medio de consultas y de copias de respaldo. **C)** El borrado seguro debe incluirse en los respaldos incrementales y totales y en cualquiera de los medios de respaldo, así como máquinas virtuales o contenedores. **D)** Concluir este documento, adjuntarlo a SGPDP llenar formato 5 y colocar nombre y firma de quien realizó la acción.
6	1	Un día hábil	**Artículo 18. II. a) Sincronizar la fecha y hora con el servidor NTP (Network Time Protocol) oficial de la UNAM**
			A) Realizar la verificación y configuración con privilegio de administrador del sistema operativo.

Núm. formato	Etapa	Duración estimada	Medidas de seguridad técnicas y proceso recomendado para su cumplimiento
			B) En función del sistema operativo, acceder a la configuración de servidor de tiempo (NTP) en interfaz gráfica o por medio de línea de comandos. *Por ejemplo*, en el caso del sistema operativo Linux: - Verificar la existencia del archivo */etc/ntp.conf* - Editar el archivo *ntp.conf* incluyendo en la primera línea: *server ntpdgtic.redunam.unam.mx* ***ó*** *server 132.247.169.17* - Reiniciar el demonio del cliente NTP con el comando *sudo service ntp reload.* **C)** En caso de no tener el cliente NTP instalado, descargarlo del repositorio de aplicaciones del sistema operativo, instalarlo y regresar al punto B. **D)** Llenar formato 6 y colocar nombre y firma de quien realizó la acción.
7	1	Dos días hábiles	**Artículo 18. II. b) Instalar y mantener actualizado el software antimalware.**
			A) En función del sistema operativo, instalar uno o varios programas para la contención de malware. *Por ejemplo*, para el

Núm. formato	Etapa	Duración estimada	Medidas de seguridad técnicas y proceso recomendado para su cumplimiento
			caso del sistema operativo Linux existen herramientas de código abierto y uso libre como *chkrootkit, rootkit hunter, bothunter, clamAV, avast*, entre otros, que se pueden instalar desde el repositorio correspondiente a la distribución de Linux en uso. **B)** Disponer de comandos para la localización de amenazas. *Por ejemplo*, para el caso de Linux, se recomienda usar el comando *grep* para la detección de cadenas regulares de texto en las invocaciones al *shell*. **C)** Una vez instalada la solución, verificar periódicamente su actualización. **D)** Llenar formato 7 y colocar nombre y firma de quien realizó la acción.
8	1	Cuatro días hábiles	**Artículo 18. II. c) Instalar las actualizaciones de seguridad más recientes disponibles.**
			A) En función del sistema operativo, se debe revisar la vigencia y actualización de las herramientas de seguridad de la información. *Por ejemplo*, en el sistema operativo Linux ejecutar

Núm. formato	Etapa	Duración estimada	Medidas de seguridad técnicas y proceso recomendado para su cumplimiento
			apt-get update para obtener la lista de actualizaciones, especialmente en el repositorio *security* de la respectiva distribución. **B)** Realizar un respaldo del sistema para garantizar retorno a versión anterior en caso de incompatibilidad con alguna aplicación de las actualizaciones de seguridad. **C)** Instalar las actualizaciones en el sistema operativo. **D)** Llenar formato 8 y colocar nombre y firma de quien realizó la acción.
9	1	Cuatro días hábiles	**Artículo 19. I. a) Aplicar un mecanismo de autenticación para las personas autorizadas con base en el principio del menor privilegio.**
			A) Verificar el tipo de control de acceso al sistema, esto es: a través de contraseñas, claves, identificadores, nombres de usuario, nombres de dominio, entre otros. Según sea aplicable al sistema de información en lo particular. En caso de no tener un control de acceso establecer al menos uno como: usuarios de sistema

Núm. formato	Etapa	Duración estimada	Medidas de seguridad técnicas y proceso recomendado para su cumplimiento
			operativo, cuenta y contraseña de sistema. **B)** Revisar que los privilegios de acceso sean los adecuados en función del rol del usuario. *Por ejemplo:* el usuario de conexión a la base de datos no debe estar asignado a alguna cuenta del personal que tiene acceso al sistema. **D)** Llenar formato 9 y colocar nombre y firma de quien realizó la acción.
10	1	Dos días hábiles	**Artículo 19. II. b) Evitar la instalación de cualquier elemento de software que implique algún riesgo para el tratamiento de datos personales.**
			A) Dependiendo del sistema operativo, configurar las actualizaciones solamente para versiones maduras o revisiones certificadas de las aplicaciones. *Por ejemplo*: en sistemas Linux desactivar la instalación de versiones *beta, test, debug, non-official.* **B)** De la lista de software instalado, verificar el consumo de recursos de aplicaciones *TSR (Terminal and Stay Resident)*. Identificar demonios que ocupen excesiva RAM o tiempo

Núm. formato	Etapa	Duración estimada	Medidas de seguridad técnicas y proceso recomendado para su cumplimiento
			de ejecución en el procesador. *Por ejemplo*: En sistemas Windows usar el Administrador de Tareas para identificar programas de alto consumo. **C)** Desinstalar toda aquella aplicación, librería, programa, paquetería o servicio que no sea estrictamente necesario para la operación del sistema. *Por ejemplo*, si el servidor Linux no proporcionará direcciones IP, el demonio o servicio *dchpd* no debe estar instalado. **D)** Llenar formato 10 y colocar nombre y firma de quien realizó la acción.
11	1	Dos días hábiles	**Artículo 19. III. a) Establecer las medidas físicas de seguridad que controlen el acceso a los equipos.**
			A) Identificar las medidas físicas que restrinjan el acceso físico a equipos, tales como chapas, puertas, biométricos. **B)** En función de la ubicación del equipo de cómputo, hacer una relación de las condiciones más adecuadas para su protección que aún sean necesarias implementar.

Núm. formato	Etapa	Duración estimada	Medidas de seguridad técnicas y proceso recomendado para su cumplimiento
			C) Establecer y seguir un plan de mejoramiento de la protección física de equipos. *Por ejemplo*; cámaras de videovigilancia, bitácoras, vigilantes, cuartos cerrados, racks con puerta y chapa, candados en equipos, bloqueo o desconexión física de puertos USB, alarmas y sensores, según sea lo más conveniente como mínimo para la protección de los datos. **D)** Llenar formato 11 y colocar nombre y firma de quien realizó la acción.
12	1	Un día hábil	**Artículo 19. III. b) Restringir la salida de equipos de las instalaciones de cada área universitaria.**
			A) Diseñar una bitácora o formato para el registro de entrada y salida de equipos de cómputo y periféricos asociados como discos duros, cintas, unidades flash, discos ópticos, monitores, teclados, ratones y en lo general todo componente de un equipo. **B)** La bitácora de entrada y salida debe incluir el registro de número de serie e inventario UNAM. responsable de ingreso o

Núm. formato	Etapa	Duración estimada	Medidas de seguridad técnicas y proceso recomendado para su cumplimiento
			egreso del componente y firma autorizada del responsable del área. **C)** Incluir en el procedimiento la revisión periódica (al menos una vez al mes) de la consistencia del inventario registrado contra la bitácora de entrada y salida. **D)** Llenar 12 y colocar nombre y firma de quien realizó la acción.
13	1	Tres días hábiles	**Artículo 19. IV. a) Realizar la transmisión de datos personales a través de un canal cifrado.** **A)** Identificar, mediante el administrador de aplicaciones que corresponda al sistema operativo, los protocolos y aplicaciones instalados para comunicación cifrada. *Por ejemplo*: *SFTP (Secure File Transfer Protocol), SSH (Secure Shell), SCP (Secure Copy*). **B)** Instalar con el administrador de aplicaciones o comando similar los protocolos de comunicación cifrada que sean necesarios para el tipo de transacciones y accesos del sistema. *Por ejemplo*, en el caso de requerir ejecutar comandos de forma remota en un servidor Linux, instalarlo

Núm. formato	Etapa	Duración estimada	Medidas de seguridad técnicas y proceso recomendado para su cumplimiento
			con el comando *apt-get install openssh-server.* **C)** Activar los protocolos de comunicación encriptada en el servidor. *Por ejemplo*: en Linux con el comando *sudo systemctl enable ssh*. **D)** Llenar formato 13 y colocar nombre y firma de quien realizó la acción.
14	1	Tres días hábiles	**Artículo 20. Aplicar el procedimiento de borrado seguro que impida la recuperación en las bases de datos y todos sus respaldos.**
			A) Realizar una copia integral del sistema de información y colocarla en un servicio temporal. *Por ejemplo:* máquina virtual o directorio temporal en el servidor. **B)** Ingresar a la copia del sistema de información y realizar el borrado de un registro. Verificar que el dato no persiste en la base de datos por medio de forma de consulta o comando. **C)** Realizar el mismo proceso del punto B para una tabla y finalmente para la base de datos completa. D) En caso de persistencia del dato, instalar y ejecutar herramientas para borrado seguro. *Por ejemplo*: en Linux se

Núm. formato	Etapa	Duración estimada	Medidas de seguridad técnicas y proceso recomendado para su cumplimiento
			dispone *de shred, wipe, secure-delete, srm, sfill, sswap, sdmem,* que se pueden instalar desde el administrador de aplicaciones. **D)** Llenar formato 14 y colocar nombre y firma de quien realizó la acción.
ETAPA 2			
15	2	Hito	**Artículo 18. I. a) Utilizar los datos personales preexistentes que estén disponibles, de acuerdo con sus respectivas políticas de uso y acceso, en bases de datos a cargo de otras áreas universitarias.**
			A) Disponer del inventario de datos del sistema de información, esto es: documento con la descripción de tablas, campos, tipo de datos, relaciones y consultas. **B)** Con el Área Universitaria que esté identificada como la instancia autoritativa en materia de datos personales, comparar el inventario de datos. *Por ejemplo*: La Dirección General de Administración Escolar es la dependencia autoritativa en materia de datos personales de estudiantes. **C)** Establecer el acuerdo por escrito para el uso de

Núm. formato	Etapa	Duración estimada	Medidas de seguridad técnicas y proceso recomendado para su cumplimiento
			campos específicos de datos personales de la instancia autoritativa. **D)** Establecer el mecanismo de comunicación entre el sistema de información y el de la instancia autoritativa. *Por ejemplo*: *Webservices*, transferencia *SFTP.* **E)** Llenar 15 y colocar nombre y firma de quien realizó la acción.
16	2	Ocho días hábiles	**Artículo 18. I. d) Permitir el acceso al código fuente de los sistemas exclusivamente a la administración del sistema y personal para el desarrollo.** **A)** Recopilar el código fuente y documentación del sistema de información en todas sus versiones disponibles. **B)** Depositar en un equipo central de desarrollo todas las versiones de código fuente y su documentación (inventario de datos, manual de administración, manual de programador). **C)** Establecer control de acceso por usuario y contraseña hacia el equipo central de desarrollo. **D)** Activar bitácoras de acceso (*log*) hacia el

Núm. formato	Etapa	Duración estimada	Medidas de seguridad técnicas y proceso recomendado para su cumplimiento
			equipo central de desarrollo. **E)** Proporcionar las credenciales de acceso al equipo central de desarrollo exclusivamente al personal a cargo de programación y mantenimiento de código y manuales. **F)** Llenar formato 16 y colocar nombre y firma de quien realizó la acción.
17	2	Cuatro días hábiles	**Artículo 19. I. b) Establecer las medidas de seguridad en los periodos de inactividad o mantenimiento.**
			A) Elaborar documento con las medidas necesarias de seguridad para períodos vacacionales, contingencias y ventanas de mantenimiento, incluyendo: control de acceso físico y lógico a los equipos, ejecución de respaldos, sistemas de alta disponibilidad (redundancia). **B)** Incluir en el documento la descripción de los procedimientos en caso de contingencia por falla de servicio de red, falla de equipo de cómputo, falla lógica en sistema operativo. **C)** Incluir en el documento el directorio

Núm. formato	Etapa	Duración estimada	Medidas de seguridad técnicas y proceso recomendado para su cumplimiento
			de responsables de cada uno de los puntos a atender: apagado seguro, apagado fortuito, apagado programado, verificación de integridad de información, activación de servicios locales o de respaldo. **D)** Llenar formato 17 y colocar nombre y firma de quien realizó la acción.
18	2	Ocho días hábiles	**Artículo 19. I. c) Generar respaldos y aplicar los mecanismos de control y protección para su resguardo.**
			A) De acuerdo con el plan de respaldos establecido, ejecutar la secuencia de respaldos. **B)** Designar responsables de respaldos y responsables de verificación de respaldos. **C)** Completar bitácora de control de los respaldos, indicando fecha, hora, tipo de respaldo (integral, total, parcial de registros), ejecutor y revisor del respaldo, ubicación del respaldo, medio y etiqueta. **D)** Llenar formato 18 y colocar nombre y firma de quien realizó la acción.
19	2	Veinte días hábiles	**Artículo 19. I. d) Impedir el uso de cuentas y servicios**

Núm. formato	Etapa	Duración estimada	Medidas de seguridad técnicas y proceso recomendado para su cumplimiento
			gestionados por personas físicas para el tratamiento de los datos personales.
			A) Realizar revisión integral del sistema de información en materia de accesos, cuentas y servicios. *Por ejemplo*: En caso de consultar vía un *Webservice* a un sistema autoritativo de datos personales en la DGAE, identificar la cuenta de acceso a ese sistema. **B)** Determinar si las cuentas de acceso a servicios locales o remotos están bajo el control de la administración del sistema. *Por ejemplo*: Si la cuenta de acceso a un *Webservice* – su usuario y contraseña – está bajo el control del administrador del sistema, o si un respaldo que se realiza en un equipo remoto es con una cuenta y contraseña controlada por el administrador del sistema. **C)** Si las cuentas de acceso a servicios locales o remotos pertenecen a personas del Área Universitaria, cambiarlas por cuentas institucionales dentro del control de la instancia universitaria. *Por ejemplo*: si la

Núm. formato	Etapa	Duración estimada	Medidas de seguridad técnicas y proceso recomendado para su cumplimiento
			identificación para acceder a un respaldo remoto es del tipo xxx@google.com, deberá cambiarse por una cuenta del tipo xxxx@unam.mx. **D)** Llenar formato 19 y colocar nombre y firma de quien realizó la acción.
20	2	Cuatro días hábiles	**Artículo 19. II. a) Proteger ante manipulaciones indebidas y accesos no autorizados las bitácoras y los dispositivos donde se almacenan.**
			A) Elaborar una lista de las bitácoras relacionadas con el sistema de información, tanto en medio digital como físico. *Por ejemplo*: En el equipo de cómputo las bitácoras de acceso de usuarios al sistema operativo y al sistema de información (*logs*), de forma física las bitácoras de acceso al área donde está el equipo de cómputo. **B)** Junto a la lista elaborar el cronograma de revisión de integridad y respaldo de las bitácoras. *Por ejemplo*: diario, semanal, mensual. **C)** Establecer en el documento el procedimiento de

Núm. formato	Etapa	Duración estimada	Medidas de seguridad técnicas y proceso recomendado para su cumplimiento
			resguardo de las bitácoras. *Por ejemplo*: respaldo y protección de *logs* en el caso de equipo de cómputo o zonas seguras de almacenamiento de bitácoras en papel, digitalización de registros. **D)** Llenar formato 20 y colocar nombre y firma de quien realizó la acción.
21	2	Cuatro días hábiles	**Artículo 19. IV. b) Supervisar los controles de seguridad en la red de datos donde opere el sistema para tratamiento de datos personales.**
			A) Identificar los equipos activos de red que permiten la conexión del equipo de cómputo con el sistema de información, incluyendo marca, modelo, versión de software, vigencia de mantenimiento y capacidades de protección de las comunicaciones. **B)** Determinar las reglas de seguridad físicas (acceso restringido, cuartos de telecomunicaciones) y lógicas (cuentas de acceso, puertos activos, protocolos activos) para el equipo de red. **C)** Incluir en las acciones para aseguramiento de

Núm. formato	Etapa	Duración estimada	Medidas de seguridad técnicas y proceso recomendado para su cumplimiento
			la red de datos aquellas que sean necesarias en función de los controles actuales. Definir un plan de regularización de la seguridad en caso de ser aplicable. **D)** Mantener actualizados los equipos activos de red y con un programa de mantenimiento. **E)** Identificar y en su caso programar la instalación de equipo para seguridad perimetral de la red de datos. **D)** Llenar formato 21 y colocar nombre y firma de quien realizó la acción.
22	2	Cuatro días hábiles	**Artículo 19. IV. c) Proporcionar el acceso exclusivamente desde redes y servicios autorizados.**
			A) Revisar los puertos de comunicación (*TCP y UDP*) que requiera el sistema de información para su operación. *Por ejemplo*: para servicios *Web* los puertos 80 y 8080 son los convencionales. **B)** Activar en el sistema operativo la herramienta correspondiente para el control de puertos de comunicación. *Por ejemplo*, en Linux puede tratarse de un *firewall* a nivel de software o las

Núm. formato	Etapa	Duración estimada	Medidas de seguridad técnicas y proceso recomendado para su cumplimiento
			herramientas que para tal efecto contenga la distribución correspondiente del sistema operativo. **C)** Dejar activos solamente los puertos necesarios para la operación del sistema. **D)** Activar el filtrado de la comunicación por direccionamiento IP en caso de ser posible para la operación del sistema. *Por ejemplo*: Permitir el acceso al puerto de *SSH* solamente a direcciones IP en una subred de la UNAM (132.248.x.y) o a un grupo de direcciones IP específicas. **E)** Llenar formato 22 y colocar nombre y firma de quien realizó la acción.
ETAPA 3			
23	3	Veinte días hábiles	**Artículo 18. I. b) Contar con entornos para desarrollo, pruebas y operación.**
			A) Instalar y configurar equipos similares en características, preferentemente virtuales, a los equipos donde se instalará el sistema de información en su nueva o actualizada versión. **B)** Crear un repositorio en un equipo central de desarrollo para el resguardo de códigos, documentación,

Núm. formato	Etapa	Duración estimada	Medidas de seguridad técnicas y proceso recomendado para su cumplimiento
			inventarios de datos y manuales de usuario, administrador y programador. **C)** Ejecutar las pruebas de nuevas versiones o actualizaciones del sistema de información en el equipo dispuesto para tal efecto. Nunca usar -equipos físicos o virtuales con el sistema actualmente en producción como las plataformas para evaluación de versiones en desarrollo. **D)** Llenar formato 23 y colocar nombre y firma de quien realizó la acción.
24	3	Veinte días hábiles	**Artículo 18. I. f) Cumplir con las especificaciones de seguridad informática previo a la puesta en operación.**
			A) Una vez concluido el desarrollo o actualización de un sistema de información, solicitar al área de seguridad del Área Universitaria la revisión de seguridad informática del sistema, lo que incluye: pruebas de penetración, pruebas de estabilidad, pruebas de carga y endurecimiento de la seguridad. En caso de no contar con esa área, requerirlo a UNAM CERT al correo

Núm. formato	Etapa	Duración estimada	Medidas de seguridad técnicas y proceso recomendado para su cumplimiento
			seguridad.tic@unam.mx . **B)** Una vez recibido el reporte del área de seguridad, aplicar las medidas de corrección que incluya el reporte. Regresar al punto A. **C)** Habiendo resuelto los hallazgos y sugerencias de mejora de la seguridad señalados por el área especializada, realizar la instalación del sistema en la plataforma definitiva de cómputo, extrayéndolo del entorno de desarrollo. **D)** Llenar formato 24 y colocar nombre y firma de quien realizó la acción.
25	3	Hito	**Artículo 18. III. a) Utilizar equipos con componentes actualizados, protegidos con garantías y soporte, y con la capacidad suficiente para atender la demanda del servicio y de los usuarios.**
			A) Elaborar una lista del inventario de los equipos de cómputo, periféricos y de almacenamiento necesarios para la ejecución del sistema de información. **B)** Determinar la razón por la que el sistema de información requerirá estar localizado en un equipo físico y no en un

Núm. formato	Etapa	Duración estimada	Medidas de seguridad técnicas y proceso recomendado para su cumplimiento
			servidor virtual. Con ello justificar una adquisición o actualización. Por ejemplo: por incompatibilidad con hipervisores, necesidades de comunicación exclusivamente locales en la entidad y dependencia o el no necesitar de un entorno de alta disponibilidad automática. **C)** Identificar en el inventario versiones, introducción en el mercado, vida útil, contratos de mantenimiento y soporte para todos y cada uno de los componentes, en el caso de emplear equipo físico. **D)** Adquirir los componentes y elementos necesarios para la actualización, vigencia de soporte y capacidad para atención a los usuarios en el equipo de cómputo físico. **E)** Llenar formato 25 y colocar nombre y firma de quien realizó la acción.
26	3	Hito	**Artículo 18. III. b) Definir el programa de mantenimiento preventivo.** **A)** De la lista de equipo de cómputo físico necesario para la

Núm. formato	Etapa	Duración estimada	Medidas de seguridad técnicas y proceso recomendado para su cumplimiento
			operación del sistema de información, extraer las vigencias de mantenimiento. **B)** En caso de no estar en posibilidad de aplicar el mantenimiento preventivo por el personal del Área Universitaria, cotizar pólizas de mantenimiento de acuerdo con el tipo de componente, preferentemente una sola póliza para el conjunto del equipo físico. **C)** Adquirir las pólizas de mantenimiento preventivo y observar su vigencia. La vigencia no podrá ser menor de un año. **D)** Llenar formato 26 y colocar nombre y firma de quien realizó la acción.
27	3	Seis días hábiles	**Artículo 19. III. c) Aplicar el programa de mantenimiento preventivo a los equipos.**
			A) En caso de que el personal del Área Universitaria pueda realizar el mantenimiento preventivo, definir el calendario de inactividad del sistema de información, notificar a los usuarios y aplicar el plan en caso de

Núm. formato	Etapa	Duración estimada	Medidas de seguridad técnicas y proceso recomendado para su cumplimiento
			mantenimiento o inactividad. **B)** En caso de que sea a través de un proveedor que se proporcione el mantenimiento al equipo de cómputo, ejecutar el calendario de acciones preventivas en un período no superior a cada 3 meses hasta la conclusión del contrato o póliza respectivo. **C)** Llenar formato 27 y colocar nombre y firma de quien realizó la acción.
28	3	Hito	**Artículo 21. Solo se permitirá el uso de servicios de nube pública para el resguardo de archivos cifrados que contengan respaldos de la información.**
			A) Identificar los respaldos que se tengan resguardados en servicios de nube pública. **B)** Verificar el cifrado en cada uno de los respaldos que se almacenen en nube pública. El cifrado no deberá ser de menor capacidad al equivalente a AES de 128 bits. **C)** Llenar formato 28 y colocar nombre y firma de quien realizó la acción.

Núm. formato	Etapa	Duración estimada	Medidas de seguridad técnicas y proceso recomendado para su cumplimiento

ANEXO V. FORMATOS PARA CUMPLIMIENTO DE LAS MST

(Nombre del sistema A1)		Identificador único A1	
Formato	**Verificación anual**	**Acción concluida**	( )
Medida de seguridad técnica:	**Artículo 18. I. c) Utilizar datos no personales durante el desarrollo y pruebas de los sistemas.**		
Aplicable en:	I. Bases de datos y sistemas de tratamiento.		
Tiempo estimado:	Un día hábil.		
Importancia de la acción:	Evitar usar datos personales mientras se está desarrollando, actualizando o modificando el código fuente de un sistema de información.		
Proceso recomendado:	**A)** Realizar respaldo completo de la base de datos. **B)** Ejecutar consulta en el sistema de información, por medio de formato o comandos. **C)** Verificar que los datos usados en el desarrollo no correspondan a personas identificables. **D)** Si se usan datos de personas identificables, cambiar por datos genéricos o datos ficticios y regresar al punto B. **E)** Si no se usan datos de personas identificables, llenar formato con nombre y firma de quien realizó la acción, fecha de inicio y de conclusión.		
Mejores prácticas, referencias:	**1.-** Se recomienda al desarrollar un sistema de información no usar datos personales sino ficticios. **2.-** Se sugiere incluir en la documentación del desarrollo de un sistema de información el inventario de datos y el tipo de información de prueba.		
Conocimientos requeridos:	Administración de bases de datos. Consulta y actualización de tablas.		
Ejecución		**Fecha inicio**	
Nombre y firma Programador, desarrollador o diseñador del sistema de información		**Fecha término**	
Observaciones			

(Nombre del sistema A1)			Identificador único A1	
Formato:	**2**	**Verificación anual**	**Acción concluida**	( )
Medidas de seguridad técnicas:		**Artículo 18. I. e) Asignar o revocar los privilegios de acceso para los usuarios teniendo como base el principio del menor privilegio.**		
Aplicable en:		I. Bases de datos y sistemas de tratamiento.		
Tiempo estimado:		Un día hábil.		
Importancia de la acción:		No se deben asignar privilegios de acceso a los usuarios en niveles que no estén relacionados con su responsabilidad en el tratamiento de datos.		
Proceso recomendado:		**A)** Realizar respaldo completo de la base de datos. **B)** Ejecutar consulta en el sistema de información de la lista de usuarios y sus niveles o privilegios de acceso. **C)** Validar que los niveles de acceso son acordes a la relación del usuario con el tratamiento de datos personales. **D)** Si hay usuarios con privilegios mayores a los que les son necesarios, cambiar al mínimo indispensable e informarlo al usuario. Regresar al punto B. **E)** Si los privilegios de acceso son correctos para los usuarios, llenar formato con nombre y firma de quien realizó la acción, fecha de inicio y de conclusión.		
Mejores prácticas, referencias:		**1.-** Definir niveles de acceso adecuados para cada perfil o tipo de usuario. **2.-** Tener un mínimo de administradores o usuarios con altos privilegios en el sistema.		
Conocimientos requeridos:		Administración de bases de datos. Consulta y actualización de usuarios.{		
Ejecución			**Fecha inicio**	
Nombre y firma Administrador del sistema de información			**Fecha término**	
Observaciones / anotaciones				

(Nombre del sistema A1)			Identificador único A1	
Formato:		**Verificación anual**	**Acción concluida**	( )
Medidas de seguridad técnicas:	**Artículo 18. I. g) Instalar y mantener vigentes certificados de comunicación segura SSL en el caso de servicios basados en Web.**			
Aplicable en:	I. Bases de datos y sistemas de tratamiento.			
Tiempo estimado:	Tres días hábiles.			
Importancia de la acción:	El instalar un certificado SSL en servidores web incrementa la seguridad al encriptar la transferencia de datos y la unicidad del sitio para los usuarios.			
Proceso recomendado:	**A)** En caso de no tener un certificado SSL vigente, enviar correo electrónico al Departamento de Firma Electrónica de DGTIC a firma.tic@unam.mx solicitando la asignación. **B)** El Departamento de Firma Electrónica Avanzada envía procedimiento para obtención de CSR del servidor, formato de la solicitud y costos de recuperación en función del tipo de certificado requerido (organizacional, comodín o corporativo). **C)** Completar documentación, proceso y pago de costo de recuperación. Enviar comprobantes a firma.tic@unam.mx. **D)** Al recibir el certificado SSL, instalarlo en el servidor de acuerdo con las instrucciones recibidas junto con el certificado.			
Mejores prácticas, referencias:	**1.-** Los certificados SSL deben tener una vigencia de al menos un año. **2.-** En caso de tener varios sistemas de información bajo un mismo dominio, se recomienda obtener un certificado SSL del tipo comodín (*wildcard*). **3.-** Se debe realizar el proceso de renovación del certificado al menos 10 días hábiles antes de su vencimiento.			
Conocimientos requeridos:	Administración de sistema operativo. Administración de servicios Web.			
Ejecución			**Fecha inicio**	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término**	
Observaciones				

<table>
<tr><td colspan="3">(Nombre del sistema A1)</td><td colspan="2">Identificador único A1</td></tr>
<tr><td>Formato:</td><td>6</td><td>Verificación anual</td><td>Acción concluida</td><td>( )</td></tr>
<tr><td colspan="2">Medidas de seguridad técnicas:</td><td colspan="3">Artículo 18. II. a) Sincronizar la fecha y hora con el servidor NTP (Network Time Protocol) oficial de la UNAM</td></tr>
<tr><td colspan="2">Aplicable en:</td><td colspan="3">II. Sistemas operativos y servicios.</td></tr>
<tr><td colspan="2">Tiempo estimado:</td><td colspan="3">Un día hábil.</td></tr>
<tr><td colspan="2">Importancia de la acción:</td><td colspan="3">A fin de poseer información consistente, los sistemas de información deben estar sincronizados con una instancia central de tiempo, en este caso el servidor NTP de la UNAM.</td></tr>
<tr><td colspan="2">Proceso recomendado:</td><td colspan="3">A) Realizar la verificación y configuración con privilegio de administrador del sistema operativo.
B) En función del sistema operativo, acceder a la configuración de servidor de tiempo (NTP) en interfaz gráfica o por medio de línea de comandos.
<u>Por ejemplo</u>, en el caso del sistema operativo Linux:
- Verificar la existencia del archivo /etc/ntp.conf
- Editar el archivo ntp.conf incluyendo en la primera línea:
server ntpdgtic.redunam.unam.mx ó
server 132.247.169.17
- Reiniciar el demonio del cliente NTP con el comando sudo service ntp reload.
C) En caso de no tener el cliente NTP instalado, descargarlo del repositorio de aplicaciones del sistema operativo, instalarlo y regresar al punto B.
D) Llenar y firmar formato.</td></tr>
<tr><td colspan="2">Mejores prácticas, referencias:</td><td colspan="3">1.- Los servidores virtuales y contenedores hospedados en el Centro de Datos en DGTIC son configurados de origen con sincronización al servidor NTP de la UNAM.
2.- No se deben usar otros servidores de NTP distintos al de UNAM.</td></tr>
<tr><td colspan="2">Conocimientos requeridos:</td><td colspan="3">Administración de sistema operativo.</td></tr>
<tr><td colspan="4">Ejecución</td><td>Fecha inicio</td></tr>
<tr><td colspan="4"></td><td></td></tr>
<tr><td colspan="4">Nombre y firma
Administrador del sistema de información o servidor</td><td>Fecha término</td></tr>
<tr><td colspan="4"></td><td></td></tr>
<tr><td colspan="4">Observaciones / anotaciones</td><td></td></tr>
</table>

(Nombre del sistema A1)			Identificador único A1	
Formato:	**7**	**Verificación anual**	**Acción concluida**	( )
Medidas de seguridad técnicas:		**Artículo 18. II. b) Instalar y mantener actualizado el software antimalware.**		
Aplicable en:		II. Sistemas operativos y servicios.		
Tiempo estimado:		Dos días hábiles.		
Importancia de la acción:		El servidor que hospede el sistema de información debe tener protecciones instaladas para mitigar la inserción de *malware* (*rootkits, backdoors o* códigos maliciosos) que pueda alterar su operación o la integridad y seguridad de los datos.		
Proceso recomendado:		**A)** En función del sistema operativo, instalar uno o varios programas para la contención de malware. *Por ejemplo*, para el caso del sistema operativo Linux existen herramientas de código abierto y uso libre como *chkrootkit, rootkit hunter, bothunter, clamAV, avast*, entre otros, que se pueden instalar desde el repositorio correspondiente a la distribución de Linux en uso. **B)** Disponer de comandos para la localización de amenazas. *Por ejemplo*, para el caso de Linux, se recomienda usar el comando *grep* para la detección de cadenas regulares de texto en las invocaciones al *shell*. **C)** Una vez instalada la solución, verificar periódicamente su actualización **D)** Llenar y firmar formato.		
Mejores prácticas, referencias:		**1.-** UNAM-CERT puede asesorar en la selección de las herramientas *anti malware* más adecuadas para el servidor donde se aloje el sistema de información. Contactar al correo seguridad.tic@unam.mx.		
Conocimientos requeridos:		Administración de sistema operativo. Instalación de aplicaciones.		
Ejecución			**Fecha inicio**	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término**	
Observaciones / anotaciones				

<table>
<tr><td colspan="3">(Nombre del sistema A1)</td><td colspan="2">Identificador único A1</td></tr>
<tr><td>Formato:</td><td>8</td><td>Verificación anual</td><td>Acción concluida</td><td>( )</td></tr>
<tr><td colspan="2">Medidas de seguridad técnicas:</td><td colspan="3">Artículo 18. II. c) Instalar las actualizaciones de seguridad más recientes disponibles.</td></tr>
<tr><td colspan="2">Aplicable en:</td><td colspan="3">II. Sistemas operativos y servicios.</td></tr>
<tr><td colspan="2">Tiempo estimado:</td><td colspan="3">Cuatro días hábiles.</td></tr>
<tr><td colspan="2">Importancia de la acción:</td><td colspan="3">El servidor que hospede el sistema de información debe tener vigentes todas las actualizaciones de seguridad proporcionadas por el fabricante o desarrollador del sistema operativo.</td></tr>
<tr><td colspan="2">Proceso recomendado:</td><td colspan="3">A) En función del sistema operativo, se debe revisar la vigencia y actualización de las herramientas de seguridad de la información. Por ejemplo, en el sistema operativo Linux ejecutar apt-get update para obtener la lista de actualizaciones, especialmente en el repositorio security de la respectiva distribución.
B) Realizar un respaldo del sistema para garantizar retorno a versión anterior en caso de incompatibilidad con alguna aplicación de las actualizaciones de seguridad.
C) Instalar las actualizaciones en el sistema operativo.
D) Llenar y firmar formato.</td></tr>
<tr><td colspan="2">Mejores prácticas, referencias:</td><td colspan="3">1.- Debe verificarse la actualización de seguridad del sistema operativo al menos una vez a la semana y configurar la actualización o notificación inmediata en caso de complementos de seguridad urgentes.</td></tr>
<tr><td colspan="2">Conocimientos requeridos:</td><td colspan="3">Administración de sistema operativo. Instalación de aplicaciones.</td></tr>
<tr><td colspan="3">Ejecución</td><td colspan="2">Fecha inicio</td></tr>
<tr><td colspan="3"></td><td colspan="2"></td></tr>
<tr><td colspan="3">Nombre y firma
Administrador del sistema de información o servidor</td><td colspan="2">Fecha término</td></tr>
<tr><td colspan="3"></td><td colspan="2"></td></tr>
<tr><td colspan="3">Observaciones / anotaciones</td><td colspan="2"></td></tr>
</table>

Nombre del sistema A1)			Identificador único A1	
Formato:	**9**	**Verificación anual**	**Acción concluida**	( )
Medidas de seguridad técnicas:		**Artículo 19. I. a) Aplicar un mecanismo de autenticación para las personas autorizadas con base en el principio del menor privilegio.**		
Aplicable en:		I. Bases de datos y sistemas de tratamiento.		
Tiempo estimado:		Cuatro días hábiles.		
Importancia de la acción:		Partiendo de la asignación o niveles de acceso a la información con el principio del menor privilegio, debe haber en operación en el sistema al menos un mecanismo para la validación de los usuarios autorizados.		
Proceso recomendado:		**A)** Verificar el tipo de control de acceso al sistema, esto es: a través de contraseñas, claves, identificadores, nombres de usuario, nombres de dominio, entre otros. Según sea aplicable al sistema de información en lo particular. En caso de no tener un control de acceso establecer al menos uno como: usuarios de sistema operativo, cuenta y contraseña de sistema. **B)** Revisar que los privilegios de acceso sean los adecuados en función del rol del usuario. *Por ejemplo:* el usuario de conexión a la base de datos no debe estar asignado a alguna cuenta del personal que tiene acceso al sistema. **D)** Llenar y firmar formato.		
Mejores prácticas, referencias:		**1.-** Se recomienda usar un esquema estándar de acceso a sistemas que están vinculados, por ejemplo: por medio de Directorio Activo (*Active Directory*), *LDAP* u *OpenAIM.* **2.-** Las contraseñas deben ser de 12 caracteres o más con uso de signos, letras mayúsculas y minúsculas y números.		
Conocimientos requeridos:		Administración de bases de datos. Consulta y actualización de usuarios.		
Ejecución			**Fecha inicio**	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término**	
Observaciones / anotaciones				

(Nombre del sistema A1)			Identificador único A1	
Formato:	**10**	**Verificación anual**	**Acción concluida**	( )

Medida de seguridad técnica:	**Artículo 19. II. b) Evitar la instalación de cualquier elemento de software que implique algún riesgo para el tratamiento de datos personales.**
Aplicable en:	II. Sistemas operativos.
Tiempo estimado:	Dos días hábiles.
Importancia de la acción:	Por la relevancia de los sistemas de información con datos personales se debe minimizar o erradicar el riesgo de seguridad que implica instalar aplicaciones no verificadas.
Proceso recomendado:	**A)** Dependiendo del sistema operativo, configurar las actualizaciones solamente para versiones maduras o revisiones certificadas de las aplicaciones. *Por ejemplo*: en sistemas Linux desactivar la instalación de versiones *beta, test, debug, non-official.* **B)** De la lista de software instalado, verificar el consumo de recursos de aplicaciones *TSR (Terminal and Stay Resident)*. Identificar demonios que ocupen excesiva RAM o tiempo de ejecución en el procesador. *Por ejemplo*: En sistemas Windows usar el Administrador de Tareas para identificar programas de alto consumo. **C)** Desinstalar toda aquella aplicación, librería, programa, paquetería o servicio que no sea estrictamente necesario para la operación del sistema. *Por ejemplo*, si el servidor Linux no proporcionará direcciones IP, el demonio o servicio *dchpd* no debe estar instalado. **D)** Llenar y firmar formato.
Mejores prácticas, referencias:	**1.-** En ningún caso puede instalarse software de procedencia desconocida. Se debe impedir a los usuarios en sus privilegios de acceso instalar software o inyectar código a la aplicación del sistema de información. y se debe realizar un control estricto de los puertos de comunicación (USB, Red, etc) para evitar la extracción no autorizada de datos.
Conocimientos requeridos:	Administración de sistema operativo. Instalación de aplicaciones.

Ejecución	**Fecha inicio**
Nombre y firma Administrador del sistema de información o servidor	**Fecha término**
Observaciones / anotaciones	

(Nombre del sistema A1)			Identificador único A1	
Formato:	**11**	**Verificación anual**	**Acción concluida**	( )
Medidas de seguridad técnicas:	**Artículo 19. III. a) Establecer las medidas físicas de seguridad que controlen el acceso a los equipos.**			
Aplicable en:	III. Equipo de cómputo.			
Tiempo estimado:	Dos días hábiles.			
Importancia de la acción:	Además de las protecciones de tipo lógico, deben implementarse medidas de seguridad para reducir el riesgo al sistema de información por accesos físicos no autorizados.			
Proceso recomendado:	**A)** Identificar las medidas físicas que restrinjan el acceso físico a equipos, tales como chapas, puertas, biométricos. **B)** En función de la ubicación del equipo de cómputo, hacer una relación de las condiciones más adecuadas para su protección que aún sean necesarias implementar. **C)** Establecer y seguir un plan de mejoramiento de la protección física de equipos. *Por ejemplo*; cámaras de videovigilancia, bitácoras, vigilantes, cuartos cerrados, racks con puerta y chapa, candados en equipos, bloqueo o desconexión física de puertos USB, alarmas y sensores, según sea lo más conveniente como mínimo para la protección de los datos. **D)** Llenar y firmar formato.			
Mejores prácticas, referencias:	**1.-** Las medidas físicas de seguridad deben revisarse regularmente y formar parte de plan de continuidad de operaciones, así como ser del conocimiento de la Comisión local de seguridad.			
Conocimientos requeridos:	Administración de bases de datos. Consulta y actualización de usuarios.			
Ejecución			**Fecha inicio**	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término**	
Observaciones / anotaciones				

(Nombre del sistema A1)			Identificador único A1	
Formato:	**12**	**Verificación anual**	**Acción concluida**	( )
Medidas de seguridad técnicas:	**Artículo 19. III. b) Restringir la salida de equipos de las instalaciones de cada área universitaria.**			
Aplicable en:	III. Equipo de cómputo.			
Tiempo estimado:	Un día hábil.			
Importancia de la acción:	Se debe tener un mecanismo de control para la entrada y salida de equipos de cómputo y eliminar extracciones no autorizadas.			
Proceso recomendado:	**A)** Diseñar una bitácora o formato para el registro de entrada y salida de equipos de cómputo y periféricos asociados como discos duros, cintas, unidades *flash*, discos ópticos, monitores, teclados, ratones y en lo general todo componente de un equipo. **B)** La bitácora de entrada y salida debe incluir el registro de número de serie e inventario UNAM. responsable de ingreso o egreso del componente y firma autorizada del responsable del área. **C)** Incluir en el procedimiento la revisión periódica (al menos una vez al mes) de la consistencia del inventario registrado contra la bitácora de entrada y salida. **D)** Llenar y firmar formato.			
Mejores prácticas, referencias:	**1.-** Se recomienda usar un formato estándar de control de entrada y salida de bienes proporcionado por las áreas administrativas de las entidades y dependencias y conservar una copia en el área responsable del equipo de cómputo. **2.-** En la bitácora se debe incluir la razón de la entrada o salida del equipo. En el caso de baja, se deberá firmar la declaración de borrado seguro de Patrimonio Universitario.			
Conocimientos requeridos:	Gestión de Tecnología de información, control de entrada y salida de equipo y materiales.			
Ejecución			**Fecha inicio**	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término**	
Observaciones				

(Nombre del sistema A1)			Identificador único A1	
Formato :	**13**	**Verificación anual**	**Acción concluida**	( )

Medidas de seguridad técnicas:	**Artículo 19. IV. a) Realizar la transmisión de datos personales a través de un canal cifrado.**
Aplicable en:	IV. Red de datos.
Tiempo estimado:	Tres días hábiles.
Importancia de la acción:	La comunicación del sistema de información con otros sistemas o servicios, así como el acceso de administración para ejecución de procesos por comandos, debe estar encriptada para evitar el envío o recepción de datos susceptibles de ser interceptados en tránsito.
Proceso recomendado:	**A)** Identificar, mediante el administrador de aplicaciones que corresponda al sistema operativo, los protocolos y aplicaciones instalados para comunicación cifrada. *Por ejemplo*: *SFTP (Secure File Transfer Protocol), SSH (Secure Shell), SCP (Secure Copy*). **B)** Instalar con el administrador de aplicaciones o comando similar los protocolos de comunicación cifrada que sean necesarios para el tipo de transacciones y accesos del sistema. *Por ejemplo*, en el caso de requerir ejecutar comandos de forma remota en un servidor Linux, instalarlo con el comando *apt-get install openssh-server.* **C)** Activar los protocolos de comunicación encriptada en el servidor. *Por ejemplo*: en Linux con el comando *sudo systemctl enable ssh*. **D)** Llenar y firmar formato.
Mejores prácticas, referencias:	**1.-** Se deben mantener actualizados los protocolos de comunicación por canal cifrado al igual que las utilerías de seguridad. 2.- El protocolo de comunicación cifrada requiere puertos específicos TCP, los cuales deberán estar permitidos en la configuración del equipo activo de red.
Conocimientos requeridos:	Administración de sistema operativo. Instalación de aplicaciones. Administración de red.

Ejecución	Fecha inicio
Nombre y firma Administrador del sistema de información o servidor	**Fecha término**
Observaciones / anotaciones	

(Nombre del sistema A1)			Identificador único A1	
Formato:	**14**	**Verificación anual**	**Acción concluida**	( )
Medidas de seguridad técnicas:	**Artículo 20. Aplicar el procedimiento de borrado seguro que impida la recuperación en las bases de datos y todos sus respaldos.**			
Aplicable en:	Bases de datos y sistemas de tratamiento.			
Tiempo estimado:	Tres días hábiles.			
Importancia de la acción:	Se debe verificar que el procedimiento de borrado seguro es funcional y que el dato no persiste en función del tipo de borrado (registro, tabla, base, sistema).			
Proceso recomendado:	**A)** Realizar una copia integral del sistema de información y colocarla en un servicio temporal. *Por ejemplo:* máquina virtual directorio temporal en el servidor. **B)** Ingresar a la copia del sistema de información y realizar el borrado de un registro. Verificar que el dato no persiste en la base de datos por medio de forma de consulta o comando. **C)** Realizar el mismo proceso del punto B para una tabla y finalmente para la base de datos completa. D) En caso de persistencia del dato, instalar y ejecutar herramientas para borrado seguro. *Por ejemplo*: en Linux se dispone *de shred, wipe, secure-delete, srm, sfill, sswap, sdmem,* que se pueden instalar desde el administrador de aplicaciones. **D)** Llenar y firmar este formato.			
Mejores prácticas, referencias:	**1.-** Se recomienda usar al menos un comando a nivel de sistema operativo para el borrado seguro de conformidad con el procedimiento establecido.			
Conocimientos requeridos:	Administración de sistema operativo. Instalación de aplicaciones. Gestión de archivos.			
Ejecución			**Fecha inicio**	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término**	
Observaciones / anotaciones				

(Nombre del sistema A1)			Identificador único A1	
Formato:	**15**	**Verificación anual**	**Acción concluida**	( )
Medidas de seguridad técnicas	**Artículo 18. I. a) Utilizar los datos personales preexistentes que estén disponibles, de acuerdo con sus respectivas políticas de uso y acceso en bases de datos a cargo de otras áreas universitarias.**			
Aplicable en:	I. Bases de datos y sistemas de tratamiento.			
Tiempo estimado:	Hito.			
Importancia de la acción:	Optimizar y consolidar el uso y la protección de datos personales al hacer referencia a instancias universitarias que sean las principales responsables de su obtención, resguardo y protección.			
Proceso recomendado:	**A)** Disponer del inventario de datos del sistema de información, esto es: documento con la descripción de tablas, campos, tipo de datos, relaciones y consultas. **B)** Con la Área Universitaria que esté identificada como la instancia autoritativa en materia de datos personales, comparar el inventario de datos. *Por ejemplo*: La Dirección General de Administración Escolar es la dependencia autoritativa en materia de datos personales de estudiantes. **C)** Establecer el acuerdo por escrito para el uso de campos específicos de datos personales de la instancia autoritativa. **D)** Establecer el mecanismo de comunicación entre el sistema de información y el de la instancia autoritativa. *Por ejemplo*: *Webservices*, transferencia *SFTP.* **E)** Llenar y firmar formato.			
Mejores prácticas, referencias:	**1.-** El hacer referencia a instancias a cargo de la obtención de los datos personales y su protección se garantiza la homogeneidad de la información.			
Conocimientos requeridos:	Administración de sistema de información. Gestión de bases de datos.			
Ejecución			**Fecha inicio**	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término**	
Observaciones / anotaciones				

(Nombre del sistema A1)			Identificador único A1	
Formato:	**16**	**Verificación anual**	**Acción concluida**	( )
Medidas de seguridad técnicas:	**Artículo 18. I. d) Permitir el acceso al código fuente de los sistemas exclusivamente a la administración del sistema y personal para el desarrollo.**			
Aplicable en:	I. Bases de datos y sistemas de tratamiento.			
Tiempo estimado:	Ocho días hábiles.			
Importancia de la acción:	Evitar el uso de códigos originales de los sistemas de información que posteriormente implique un riesgo a la seguridad de estos.			
Proceso recomendado:	**A)** Recopilar el código fuente y documentación del sistema de información en todas sus versiones disponibles. **B)** Depositar en un equipo central de desarrollo todas las versiones de código fuente y su documentación (inventario de datos, manual de administración, manual de programador). **C)** Establecer control de acceso por usuario y contraseña hacia el equipo central de desarrollo **D)** Activar bitácoras de acceso (*log*) hacia el equipo central de desarrollo. **E)** Proporcionar las credenciales de acceso al equipo central de desarrollo exclusivamente al personal a cargo de programación y mantenimiento de código y manuales. **F)** Llenar y firmar formato.			
Mejores prácticas, referencias:	**1.-** Se debe documentar todo el proceso de desarrollo y actualización de un sistema de información.			
Conocimientos requeridos:	Administración de sistema de información. Gestión de bases de datos.			
Ejecución			**Fecha inicio**	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término**	
Observaciones / anotaciones				

(Nombre del sistema A1)			Identificador único A1	
Formato:	**17**	**Verificación anual**	**Acción concluida**	( )
Medidas de seguridad técnicas:	**Artículo 19. I. b) Establecer las medidas de seguridad en los periodos de inactividad o mantenimiento.**			
Aplicable en:	I. Bases de datos y sistemas de tratamiento.			
Tiempo estimado:	Cuatro días hábiles.			
Importancia de la acción:	Garantizar la continuidad de la operación y disponibilidad de los sistemas de información especialmente durante períodos vacacionales, contingencias o ciclos de mantenimiento.			
Proceso recomendado:	**A)** Elaborar documento con las medidas necesarias de seguridad para períodos vacacionales, contingencias y ventanas de mantenimiento, incluyendo: control de acceso físico y lógico a los equipos, ejecución de respaldos, sistemas de alta disponibilidad (redundancia). **B)** Incluir en el documento la descripción de los procedimientos en caso de contingencia por falla de servicio de red, falla de equipo de cómputo, falla lógica en sistema operativo. **C)** Incluir en el documento el directorio de responsables de cada uno de los puntos a atender: apagado seguro, apagado fortuito, apagado programado, verificación de integridad de información, activación de servicios locales o de respaldo. **D)** Llenar y firmar formato.			
Mejores prácticas, referencias:	**1.-** Las medidas de seguridad durante períodos de mantenimiento deben formar parte de un plan de continuidad de operaciones y de recuperación ante desastres (**DRP**).			
Conocimientos requeridos:	Administración de sistema de información. Administración de sistema operativo.			
Ejecución			**Fecha inicio**	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término**	
Observaciones / anotaciones				

(Nombre del sistema A1)			Identificador único A1	
Formato:	**18**	**Verificación anual**	**Acción concluida**	( )
Medidas de seguridad técnica:	**Artículo 19. I. c) Generar respaldos y aplicar los mecanismos de control y protección para su resguardo.**			
Aplicable en:	I. Bases de datos y sistemas de tratamiento.			
Tiempo estimado:	Ocho días hábiles.			
Importancia de la acción:	Verificar que el plan de respaldos opera adecuadamente para su utilización en caso de contingencia.			
Proceso recomendado:	**A)** De acuerdo con el plan de respaldos establecido, ejecutar la secuencia de respaldos. **B)** Designar responsables de respaldos y responsables de verificación de respaldos. **C)** Completar bitácora de control de los respaldos, indicando fecha, hora, tipo de respaldo (integral, total, parcial de registros), ejecutor y revisor del respaldo, ubicación del respaldo, medio y etiqueta. **D)** Llenar y firmar formato.			
Mejores prácticas, referencias:	**1.-** La generación de respaldos, su control y protección deben formar parte de un plan de continuidad de operaciones y de recuperación ante desastres (**DRP**).			
Conocimientos requeridos:	Administración de sistema de información. Administración de sistema operativo.			
Ejecución			**Fecha inicio**	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término**	
Observaciones / anotaciones				

(Nombre del sistema A1)			Identificador único A1	
Formato:	**19**	**Verificación anual**	**Acción concluida**	( )
Medidas de seguridad técnicas:	**Artículo 19. I. d) Impedir el uso de cuentas y servicios gestionados por personas físicas para el tratamiento de los datos personales.**			
Aplicable en:	I. Bases de datos y sistemas de tratamiento.			
Tiempo estimado:	Veinte días hábiles.			
Importancia de la acción:	Debe evitarse el riesgo que implica el depender de cuentas de control personal para acceder a servicios, fuentes de información o cualquier elemento del sistema de información que ponga en riesgo su estabilidad y confiabilidad.			
Proceso recomendado:	**A)** Realizar revisión integral del sistema de información en materia de accesos, cuentas y servicios. *Por ejemplo*: En caso de consultar vía un *Webservice* a un sistema autoritativo de datos personales en la DGAE, identificar la cuenta de acceso a ese sistema. **B)** Determinar si las cuentas de acceso a servicios locales o remotos están bajo el control de la administración del sistema. *Por ejemplo*: Si la cuenta de acceso a un *Webservice* – su usuario y contraseña – está bajo el control del administrador del sistema, o si un respaldo que se realiza en un equipo remoto es con una cuenta y contraseña controlada por el administrador del sistema. **C)** Si las cuentas de acceso a servicios locales o remotos pertenecen a personas del Área Universitaria, cambiarlas por cuentas institucionales dentro del control de la instancia universitaria. *Por ejemplo*: si la identificación para acceder a un respaldo remoto es del tipo xxx@google.com, deberá cambiarse por una cuenta del tipo xxxx@unam.mx **D)** Llenar y firmar formato.			
Mejores prácticas, referencias:	**1.-** Nunca deben usarse cuentas, servicios, suscripciones, licencias o cualquier otro elemento informático cuyo control dependa de una sola persona.			
Conocimientos requeridos:	Administración de sistema de información. Gestión de bases de datos.			

Ejecución	**Fecha inicio**
Nombre y firma Administrador del sistema de información o servidor	**Fecha término**
Observaciones / anotaciones	

(Nombre del sistema A1)			Identificador único A1	
Formato:	**20**	**Verificación anual**	**Acción concluida**	( )
Medidas de seguridad técnicas:	**Artículo 19. II. a) Proteger ante manipulaciones indebidas y accesos no autorizados las bitácoras y los dispositivos donde se almacenan.**			
Aplicable en:	II. Sistemas operativos.			
Tiempo estimado:	Cuatro días hábiles.			
Importancia de la acción:	Las bitácoras son un elemento esencial para determinar acciones que atentan contra la estabilidad del sistema de información y la protección de los datos personales.			
Proceso recomendado:	**A)** Elaborar una lista de las bitácoras relacionadas con el sistema de información, tanto en medio digital como físico. *Por ejemplo*: En el equipo de cómputo las bitácoras de acceso de usuarios al sistema operativo y al sistema de información (*logs*), de forma física las bitácoras de acceso al área donde está el equipo de cómputo. **B)** Junto a la lista elaborar el cronograma de revisión de integridad y respaldo de las bitácoras. *Por ejemplo*: diario, semanal, mensual. **C)** Establecer en el documento el procedimiento de resguardo de las bitácoras. *Por ejemplo*: respaldo y protección de *logs* en el caso de equipo de cómputo o zonas seguras de almacenamiento de bitácoras en papel, digitalización de registros. **D)** Llenar y firmar formato.			
Mejores prácticas, referencias:	**1.-** Las bitácoras digitales y en papel deben resguardarse preferentemente en una zona independiente de la ubicación del sistema de información.			
Conocimientos requeridos:	Administración de sistema de información. Administración de sistema operativo.			
Ejecución			**Fecha inicio**	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término**	
Observaciones / anotaciones				

(Nombre del sistema A1)			Identificador único A1	
Formato:	**21**	**Verificación anual**	**Acción concluida**	( )
Norma Complementaria Técnica	**Artículo 19. IV. b) Supervisar los controles de seguridad en la red de datos donde opere el sistema para tratamiento de datos personales.**			
Aplicable en:	IV. Red de datos.			
Tiempo estimado:	Cuatro días hábiles.			
Importancia de la acción:	El control de seguridad de los equipos activos de red que suministran la conectividad al sistema de información es un elemento básico para la protección de los datos.			
Proceso recomendado:	**A)** Identificar los equipos activos de red que permiten la conexión del equipo de cómputo con el sistema de información, incluyendo marca, modelo, versión de software, vigencia de mantenimiento y capacidades de protección de las comunicaciones. **B)** Determinar las reglas de seguridad físicas (acceso restringido, cuartos de telecomunicaciones) y lógicas (cuentas de acceso, puertos activos, protocolos activos) para el equipo de red. **C)** Incluir en las acciones para aseguramiento de la red de datos aquellas que sean necesarias en función de los controles actuales. Definir un plan de regularización de la seguridad en caso de ser aplicable. **D)** Mantener actualizados los equipos activos de red y con un programa de mantenimiento. **E)** Identificar y en su caso programar la instalación de equipo para seguridad perimetral de la red de datos. **D)** Llenar y firmar formato.			
Mejores prácticas, referencias:	**1.-** Las ubicaciones físicas de los equipos activos de red deben estar protegidas con cerraduras y controles de acceso, cumplir las normas de operación y no emplearse para ningún otro equipo o uso.			
Conocimientos requeridos:	Administración de redes de datos.			
Ejecución			**Fecha inicio**	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término**	
Observaciones / anotaciones				

(Nombre del sistema A1)			Identificador único A1	
Formato:	**22**	**Verificación anual**	**Acción concluida**	( )
Medidas de seguridad técnicas:	**Artículo 19. IV. c) Proporcionar exclusivamente el acceso desde redes y servicios autorizados.**			
Aplicable en:	IV. Red de datos.			
Tiempo estimado:	Cuatro días hábiles.			
Importancia de la acción:	Es necesario reducir el mínimo necesario los puertos de comunicación para el funcionamiento del sistema de información.			
Proceso recomendado:	**A)** Revisar los puertos de comunicación (*TCP y UDP*) que requiera el sistema de información para su operación. *Por ejemplo*: para servicios *Web* los puertos 80 y 8080 son los convencionales. **B)** Activar en el sistema operativo la herramienta correspondiente para el control de puertos de comunicación. *Por ejemplo*, en Linux puede tratarse de un *firewall* a nivel de software o las herramientas que para tal efecto contenga la distribución correspondiente del sistema operativo. **C)** Dejar activos solamente los puertos necesarios para la operación del sistema. **D)** Activar el filtrado de la comunicación por direccionamiento IP en caso de ser posible para la operación del sistema. *Por ejemplo*: Permitir el acceso al puerto de *SSH* solamente a direcciones IP en una subred de la UNAM (132.248.x.y) o a un grupo de direcciones IP específicas. **E)** Llenar y firmar formato.			
Mejores prácticas, referencias:	**1.-** No se deben tener activos accesos que no son necesarios vía la red de datos.			
Conocimientos requeridos:	Administración de sistema de información. Administración de sistema operativo.			
Ejecución			**Fecha inicio**	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término**	
Observaciones / anotaciones				

(Nombre del sistema A1)			Identificador único A1	
Formato:	**23**	**Verificación anual**	**Acción concluida**	( )
Medidas de seguridad técnicas:	**Artículo 18. I. b) Contar con entornos para desarrollo, pruebas y operación.**			
Aplicable en:	I. Bases de datos y sistemas de tratamiento.			
Tiempo estimado:	Veinte días hábiles.			
Importancia de la acción:	Para evitar riesgos innecesarios a la información, el desarrollo y actualización de los mismos deberá ser realizado siempre en una plataforma y ambientes por separado.			
Proceso recomendado:	**A)** Instalar y configurar equipos similares en características, preferentemente virtuales, a los equipos donde se instalará el sistema de información en su nueva o actualizada versión. **B)** Crear un repositorio en un equipo central de desarrollo para el resguardo de códigos, documentación, inventarios de datos y manuales de usuario, administrador y programador. **C)** Ejecutar las pruebas de nuevas versiones o actualizaciones del sistema de información en el equipo dispuesto para tal efecto. Nunca usar -equipos físicos o virtuales con el sistema actualmente en producción como las plataformas para evaluación de versiones en desarrollo. **D)** Llenar y firmar formato.			
Mejores prácticas, referencias:	**1.-** Se deben realizar respaldos de la información en los sistemas en desarrollo del mismo modo que como se realicen con el sistema en producción.			
Conocimientos requeridos:	Administración de sistema de información. Desarrollo de aplicaciones.			
Ejecución			**Fecha inicio**	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término**	
Observaciones / anotaciones				

(Nombre del sistema A1)			Identificador único A1	
Formato:	**24**	**Verificación anual**	**Acción concluida**	( )
Medidas de seguridad técnicas:	**Artículo 18. I. f) Cumplir con las especificaciones de seguridad informática previo a la puesta en operación.**			
Aplicable en:	I. Bases de datos y sistemas de tratamiento.			
Tiempo estimado:	Veinte días hábiles.			
Importancia de la acción:	Solo los sistemas de información revisados integralmente en su seguridad y estabilidad pueden ser publicados bajo el dominio .unam.mx .			
Proceso recomendado:	**A)** Una vez concluido el desarrollo o actualización de un sistema de información, solicitar al área de seguridad del Área Universitaria la revisión de seguridad informática del sistema, lo que incluye: pruebas de penetración, pruebas de estabilidad, pruebas de carga y endurecimiento de la seguridad. En caso de no contar con esa área, requerirlo a UNAM CERT al correo seguridad.tic@unam.mx . **B)** Una vez recibido el reporte del área de seguridad, aplicar las medidas de corrección que incluya el reporte. Regresar al punto A. **C)** Habiendo resuelto los hallazgos y sugerencias de mejora de la seguridad señalados por el área especializada, realizar la instalación del sistema en la plataforma definitiva de cómputo, extrayéndolo del entorno de desarrollo. **D)** Llenar y firmar formato.			
Mejores prácticas, referencias:	**1.-** El equipo de UNAM CERT puede asesorar a las entidades y dependencias en la aplicación de las medidas de corrección y mitigación a partir de los resultados de la revisión de seguridad.			
Conocimientos requeridos:	Administración de aplicaciones. Administración de sistema operativo.			
Ejecución			**Fecha inicio**	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término**	
Observaciones / anotaciones				

(Nombre del sistema A1)			Identificador único A1	
Formato:	**25**	**Verificación anual**	**Acción concluida**	( )
Medidas de seguridad técnicas:	**Artículo 18. III. a) Utilizar equipos con componentes actualizados, protegidos con garantías y soporte, y con la capacidad suficiente para atender la demanda del servicio y de los usuarios.**			
Aplicable en:	III. Equipos de cómputo.			
Tiempo estimado:	Hito.			
Importancia de la acción:	Mantener en adecuada condición de operación el equipo de cómputo incrementa la estabilidad y seguridad del sistema de información.			
Proceso recomendado:	**A)** Elaborar una lista del inventario de los equipos de cómputo, periféricos y de almacenamiento necesarios para la ejecución del sistema de información. **B)** Determinar la razón por la que el sistema de información requerirá estar localizado en un equipo físico y no en un servidor virtual. Con ello justificar una adquisición o actualización. Por ejemplo: por incompatibilidad con hipervisores, necesidades de comunicación exclusivamente locales en la entidad y dependencia o el no necesitar de un entorno de alta disponibilidad automática. **C)** Identificar en el inventario versiones, introducción en el mercado, vida útil, contratos de mantenimiento y soporte para todos y cada uno de los componentes, en el caso de emplear equipo físico. **D)** Adquirir los componentes y elementos necesarios para la actualización, vigencia de soporte y capacidad para atención a los usuarios en el equipo de cómputo físico. **E)** Llenar y firmar formato.			
Mejores prácticas, referencias:	**1.-** El mantenimiento preventivo debe contar con medidas de verificación.			
Conocimientos requeridos:	Administración de infraestructura.			
Ejecución			**Fecha inicio**	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término**	
Observaciones / anotaciones				

(Nombre del sistema A1)			Identificador único A1	
Formato:	**26**	**Verificación anual**	**Acción concluida**	( )
Medidas de seguridad técnicas:	**Artículo 18. III. b) Definir el programa de mantenimiento preventivo.**			
Aplicable en:	III. Equipos de cómputo.			
Tiempo estimado:	Hito.			
Importancia de la acción:	Garantizar que el plan de mantenimiento de equipo se realiza en tiempo y forma.			
Proceso recomendado:	**A)** De la lista de equipo de cómputo físico necesario para la operación del sistema de información, extraer las vigencias de mantenimiento. **B)** En caso de no estar en posibilidad de aplicar el mantenimiento preventivo por el personal del Área Universitaria, cotizar pólizas de mantenimiento de acuerdo con el tipo de componente, preferentemente una sola póliza para el conjunto del equipo físico. **C)** Adquirir las pólizas de mantenimiento preventivo y observar su vigencia. La vigencia no podrá ser menor de un año. **D)** Llenar y firmar formato.			
Mejores prácticas, referencias:	**1.-** El programa de mantenimiento debe considerar los costos de contratos, refacciones, partes, actualizaciones y reemplazos.			
Conocimientos requeridos:	Administración de infraestructura.			
Ejecución			**Fecha inicio**	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término**	
Observaciones / anotaciones				

(Nombre del sistema A1)			Identificador único A1	
Formato:	**27**	**Verificación anual**	**Acción concluida**	( )
Medidas de seguridad técnicas:	**Artículo 19. III. c) Aplicar el programa de mantenimiento preventivo a los equipos.**			
Aplicable en:	III. Equipos de cómputo.			
Tiempo estimado:	Seis días hábiles.			
Importancia de la acción:	Garantizar que el plan de mantenimiento de equipo se realiza en tiempo y forma.			
Proceso recomendado:	**A)** En caso de que el personal del Área Universitaria pueda realizar el mantenimiento preventivo, definir el calendario de inactividad del sistema de información, notificar a los usuarios y aplicar el plan en caso de mantenimiento o inactividad. **B)** En caso de que sea a través de un proveedor que se proporcione el mantenimiento al equipo de cómputo, ejecutar el calendario de acciones preventivas en un período no superior a cada 3 meses hasta la conclusión del contrato o póliza respectivo. **C)** Llenar y firmar formato.			
Mejores prácticas, referencias:	**1.-** Debe actualizarse el equipo de cómputo de manera suficiente para continuar la operación del sistema y considerar en el mantenimiento preventivo sistemas paralelos de manera temporal hasta la conclusión de los trabajos.			
Conocimientos requeridos:	Administración de infraestructura.			
Ejecución			**Fecha inicio**	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término**	
Observaciones / anotaciones				

(Nombre del sistema A1)			Identificador único A1	
Formato:	**28**	**Verificación anual**	**Acción concluida**	( )
Medidas de seguridad técnicas:	**Artículo 21. Solo se permitirá el uso de servicios de nube pública para el resguardo de archivos cifrados que contengan respaldos de la información.**			
Aplicable en:	Servicios en la nube pública.			
Tiempo estimado:	Hito.			
Importancia de la acción:	No pueden conservarse o usarse datos personales que sean tratados por la UNAM en servicios de nube pública. Estos servicios sólo se permiten para el respaldo de archivos cifrados, no en producción.			
Proceso recomendado:	**A)** Identificar los respaldos que se tengan resguardados en servicios de nube pública. **B)** Verificar el cifrado en cada uno de los respaldos que se almacenen en nube pública. El cifrado no deberá ser de menor capacidad al equivalente a AES de 128 bits.			
Mejores prácticas, referencias:	**1.-** La DGTIC proporciona el servicio de respaldos en el Centro de Datos, por lo que se sugiere utilizarlo en lugar de respaldos en la nube pública.			
Conocimientos requeridos:	Administración de respaldos. Administración de sistema operativo.			
Ejecución			**Fecha inicio**	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término**	
Observaciones / anotaciones				

CENTRO DE ESTUDIOS MEXICANOS

UNAM-SUDÁFRICA

1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

CENTRO DE ESTUDIOS MEXICANOS UNAM-SUDÁFRICA	
Identificador único*	CEM-SUD
Formulario de registro gener	**FRSUD**
Datos personales (sensibles o no) contenidos en el sistema*:	Nombre completo, correo electrónico, RFC, nacionalidad, edad, nivel de inglés
Responsable*:	
Nombre*:	**Dr. Arturo Mendoza Ramos**
Cargo*:	**Director**
Funciones*:	Señalar qué datos son relevantes para recopilar e instruir dónde se alojarán.
Obligaciones*:	No divulgación de datos personales.
	Encargados:
(Nombre del Encargado 1*)	**Dr. David Ruiz Guzmán**
Cargo*:	**Coordinador de relaciones y gestión**
Funciones*:	Supervisar que el sistema funcione y monitorear que se active o desactive dependiendo de las convocatorias para el que fue creado.
Obligaciones*:	Advertir sobre algún cambio o actualización del sistema.
(Nombre del Encargado 2*)	María Fernanda López Díaz
Cargo*:	Responsable del área de sistemas e informática
Funciones*:	Ejecutar la activación o cancelación del sistema y crear la base de datos para facilitarla al director.
Obligaciones*:	No alteración de la información sin previa autorización.
	Usuarios:
(Nombre del Usuario 1*)	María Fernanda López Díaz
Cargo*:	Responsable del área de sistemas e informática
Funciones*:	Envío de fichas de pago, constancias, información del servicio que se contrató con el CEMSUD, enviar cartelera semanal de eventos.
Obligaciones*:	No divulgación de datos personales, y no almacenamiento de copias de la información en equipos personales.
(Nombre del Usuario 2*)	N/A
Cargo*:	
Funciones*:	
Obligaciones*:	
(Nombre del Usuario 3*)	N/A

Cargo*:	
Funciones*:	
Obligaciones*:	
Hoja de registro eventos	**HRSUD**
Datos personales contenidos en el sistema*:	Nombre completo, correo electrónico y afiliación (si es alumno, académico, visitante, diplomático, etc.)
	Responsable:
Nombre*:	**Dr. David Ruiz Guzmán**
Cargo*:	**Coordinador de relaciones y gestión**
Funciones*:	Supervisar que el sistema se resguarde tras el evento y pasarlo al encargado. Verificar que se vacié el sistema en una base de datos y se destruya después.
Obligaciones*:	No divulgar datos personales.
	Encargados:
(Nombre del Encargado 1*)	María Fernanda López Díaz
Cargo*:	Responsable del área de sistemas e informática
Funciones*:	Vaciar los datos en un concentrado para su resguardo. Captura y dar hoja original a responsable para su destrucción.
Obligaciones*:	No alterar la información sin un precedente de autorización. No almacenar copias de la información en equipos personales.
(Nombre del Encargado 2*)	N/A
Cargo*:	
Funciones*:	
Obligaciones*:	
	Usuarios:
(Nombre del Usuario 1*)	María Fernanda López Díaz
Cargo*:	Responsable del área de sistemas e informática
Funciones*:	Envío de cartelera semanal de eventos.
Obligaciones*:	No divulgación de datos personales.
(Nombre del Usuario 2*)	N/A
Cargo*:	
Funciones*:	
Obligaciones*:	
(Nombre del Usuario 3*)	N/A
Cargo*:	
Funciones*:	
Obligaciones*:	

2. ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

CENTRO DE ESTUDIOS MEXICANOS UNAM-SUDÁFRICA	
Identificador único¨*	CEM-SUD
Formulario de registro	**FRSUD**
Tipo de soporte: *	Soporte Electrónico
Descripción: *	Formulario de registro en hoja de cálculo
Características del lugar donde se resguardan los soportes: *	Alojamiento en Google drive institucional de amendoza@sudafrica.unam.mx, compartido con druiz@sudafrica.unam.mx y flopez@sudafrica.unam.mx
Hoja de registro eventos	**HRSUD**
Tipo de soporte*:	Soporte Físico y electrónico
Descripción*:	Hoja impresa cuya información se pasa a una base de datos en Google Drive en hoja de cálculo
Características del lugar donde se resguardan los soportes*:	Alojamiento en Google drive institucional de amendoza@sudafrica.unam.mx, compartido con druiz@sudafrica.unam.mx y flopez@sudafrica.unam.mx
(Nombre del sistema A3*)	N/A

3. ANÁLISIS DE RIESGOS

CENTRO DE ESTUDIOS MEXICANOS UNAM-SUDÁFRICA		
Identificador único*	CEM-SUD	
Formulario de registro	**FRSUD**	
Riesgo*	**Impacto***	**Mitigación***
Violación de cuenta (Hackeo)	*Vulnerabilidad de datos personales y otra información privilegiada.*	*Que la CRAI brinde un espacio virtual seguro y que la UNAM pueda gestionar y defender. Y cambio de contraseñas}*

CENTRO DE ESTUDIOS MEXICANOS UNAM-SUDÁFRICA		
Identificador único *	CEM-SUD	
Hoja de registro eventos	**HRSUD**	
Riesgo*	**Impacto***	**Mitigación***
Violación de cuenta (Hackeo)	*Vulnerabilidad de datos personales y otra información privilegiada.*	*Que la CRAI brinde un espacio virtual seguro y que la UNAM pueda gestionar y defender. Y cambio de contraseñas.*

10. ANÁLISIS DE BRECHA

CENTRO DE ESTUDIOS MEXICANOS UNAM-SUDÁFRICA		
Identificador único*	CEM-SUD	
Formulario de registro	**FRSUD**	
Medida de seguridad actual*	**Medida de seguridad necesaria***	**Acciones para remediación***
Se envía por correo electrónico institucional en archivo encriptado la base de datos para conciliación financiera de los cursos a la CRAI	*No hay*	*No hay*

11. PLAN DE TRABAJO

N/A

(Denominación del área específica del Área Universitaria A)*			
Identificador único*	*Usar el identificador único declarado en el inciso 1. que corresponda*		
(Nombre del sistema A1) *			
Actividad*	**Descripción***	**Duración***	**Cobertura***
Indique actividad. Agregar un renglón por cada elemento	*Describa el tipo de actividad, sus objetivos e impacto en la protección de datos personales*	*Indique duración en la ejecución de la actividad en horas, días, meses, su fecha de inicio y de término*	*Mencione los aspectos de la protección a datos personales que son resueltos, total o parcialmente, por la actividad.*

12. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

XLVII. TRANSFERENCIAS DE DATOS PERSONALES

CENTRO DE ESTUDIOS MEXICANOS UNAM-SUDÁFRICA	
Identificador único*	*CEM-SUD*
Formulario de registro	**FRSUD**
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	N/A
Transferencias mediante el traslado de soportes electrónicos:	N/A
Transferencias mediante el traslado sobre redes electrónicas:	Una vez que se manda la información vía correo electrónico el destinatario envía acuse de recibido.
Hoja de registro eventos	**HRSUD**
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	N/A
Transferencias mediante el traslado de soportes electrónicos:	N/A
Transferencias mediante el traslado sobre redes electrónicas:	Una vez que se manda la información vía correo electrónico el destinatario envía acuse de recibido.
(Nombre del sistema A3)	N/A

V. RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS

1. No hay registros físicos, solo las bases de datos de los sistemas descritos, los cuales todos se alojan en plataforma Google institucional.

2. Quien tiene acceso a los datos

i) Dr. Arturo Mendoza Ramos, Director – ver tabla 1
ii) Dr. David Ruiz Guzmán, Coordinador de relaciones y gestión, ver tabla 1
iii) María Fernanda López Díaz, ver tabla 1
iv) Lic. Paola Mendieta Verdejo, Jefa del Dpto. de Apoyo Académico a sedes en el Extranjero, acceso a información de los inscritos en los cursos de la sede a través de un reporte trimestral.
v) Lic. Montes de Oca Aranda, Jefa de Dpto. de Control contable y administrativo de sedes foráneas CRAI, y Lic. Héctor Apolinar, asistente de procesos, con acceso a datos de los inscritos y su información fiscal para efectos de conciliación bancaria y gestión de facturas fiscales.

VI. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

NO TENEMOS BITÁCORAS

1. Los datos que se registran en las bitácoras:

a) Quién accede a los datos personales, fecha y hora en la que se realiza el acceso o se intenta el mismo, propósito del acceso, así como fecha y hora de salida;
b) Para soportes físicos: Número o clave del expediente utilizado, y
c) Para soportes electrónicos: Operaciones o acciones llevadas a cabo y registros utilizados de la base de datos.

2. Si las bitácoras están en soporte físico o en soporte electrónico;

a) Lugar dónde almacena las bitácoras y por cuánto tiempo;

b) La manera en que asegura la integridad de las bitácoras, y

c) Respecto del análisis de las bitácoras:

d) Quién es el responsable de analizarlas (si es el área universitaria o si es un tercero) y cada cuándo las analiza, y

e) Para el caso de que las bitácoras estén en soporte electrónico: las herramientas de análisis utilizadas.

VII. REGISTRO DE INCIDENTES:

No se cuenta con un procedimiento de atención de incidentes.

Describir el procedimiento de atención de incidentes que tiene implementado el área

V. ACCESO A LAS INSTALACIONES

1. **Seguridad perimetral exterior** (las instalaciones del área universitaria):

La seguridad perimetral de ingreso a la institución le pertenece y la administra la Universidad de Witwatersrand

Para las personas que acceden a sus instalaciones:

a) ¿Cómo las identifica? Se cuenta con sistema de registro para visitantes mismo que solo controla la Universidad.
b) ¿Cómo las autentifica? La mayoría de la comunidad tiene acceso por vía credencial imantada o bioregistro.
c) ¿Cómo les autoriza el acceso? Bioregistro, credencial.

2. Seguridad perimetral interior (oficina, almacén o bodega para soportes físicos, centro de datos para soportes electrónicos):

¿Qué medidas de seguridad ha implementado para controlar el acceso a los espacios donde almacena los soportes físicos o electrónicos del sistema? Por ejemplo, se espera que precise el tipo de puertas y cerraduras instaladas, si tiene instalados controles biométricos, si administra la asignación de llaves y/o claves de acceso para abrir puertas y/o estantería, si cuenta con vigilancia las 24 horas, si hay un sistema de tratamiento de datos personales de videovigilancia, entre otras medidas.

Para las personas que acceden a dichos espacios interiores: De formal local, se tiene un código de acceso a las oficinas, así como llave simple de la puerta. También se cuenta con llave en los escritorios y gavetas.

1. ¿Cómo las identifica? Con nombre o por cita.
2. ¿Cómo las autentifica? Por nombre, generalmente se recibe a personas que ya conocemos o referidas de alguien. Rara vez acceden personas extrañas.
3. ¿Cómo les autoriza el acceso? A nuestras oficinas solo pueden ingresar si estamos presentes, si no nadie tiene acceso, excepto intendencia.

VI. ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

Las actualizaciones son continuas, dependiendo de los eventos y convocatorias y tomando en cuenta el correo del boletín en donde preguntamos a nuestros suscriptores si desean continuar o des inscribirse. Así con esos datos se eliminan definitivamente de la base de datos a quienes ya no desean estar.

Las medidas de seguridad previstas a continuación en los incisos VII al IX, sólo aplican para soportes electrónicos

VII. PERFILES DE USUARIO Y CONTRASEÑAS

En este rubro el área universitaria deberá describir el esquema de perfiles de usuario y contraseñas que tiene implementado para control de acceso mediante una red electrónica.

1. Modelo de control de acceso (alguno de los siguientes):

Está basado en roles (perfiles).

3. Perfiles de usuario y contraseñas en el sistema operativo de red:

a) ¿Cuenta con un sistema operativo de red instalado en sus equipos? Si

b) ¿Proporciona dicho sistema operativo un manejo riguroso de perfiles de usuario y contraseñas? No

c) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena? No

4. Perfiles de usuario y contraseñas manejados por el software aplicativo del sistema de tratamiento de datos personales:

a) ¿Ofrece dicho software un manejo riguroso de perfiles de usuario y contraseñas? No

b) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena? No

5. Administración de perfiles de usuario y contraseñas:

a) ¿Quién da de alta nuevos perfiles? No se han dado de alta nuevos usuarios, sin previa autorización.

b) ¿Quién autoriza la creación de nuevos perfiles? El secretario técnico es quién puede autorizar la creación de nuevos perfiles.

c) ¿Se lleva registro de la creación de nuevos perfiles? Se visualizan los nuevos perfiles desde el sistema.

5. Acceso remoto al sistema de tratamiento de datos personales:

a) ¿Requieren los usuarios acceso remoto al equipo de cómputo que por lo general utilizan para trabajar con el sistema? No, cada usuario puede acceder al sistema desde cualquier equipo con conexión a internet.

b) ¿Requiere el administrador acceso remoto al equipo donde reside el sistema para realizar tareas de mantenimiento? Si

c) ¿Cómo se evita el acceso remoto no autorizado? Sólo personal autorizado puedes acceder al sistema. Por ende, no hay riesgo de accesos remotos.

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

1. Señalar si realiza respaldos

a) Completos_X_, diferenciales ___ o incrementales___;

b) De forma automática __X__ o Manual _____,

c) Periodicidad con que los realiza: __cada que se crea un archivo __

d) El tipo de medios (por ejemplo: cintas magnéticas, discos duros, CD-ROM, entre otros) que utiliza para almacenar las copias de seguridad; Ningún medio físico, se guarda en el mismo Google drive

2. Cómo y dónde archiva esos medios, y Directorio principal Google drive de UNAM Sudáfrica
3. Quién es el responsable de realizar estas operaciones (el área universitaria o un tercero). Área universitaria (coordinación de sistemas e informática)

IX. PLAN DE CONTINGENCIA

Actualmente no se cuenta con un plan de contingencia.

19. Presentar el plan de contingencia con el cual garantiza la continuidad de la operación del sistema o informar si no lo tiene, pero se encuentra desarrollándolo.
20. Si cuenta con plan de contingencia y lo ha implementado, deberá indicar si realiza pruebas de eficiencia de este.
21. Informar si cuenta con un sitio redundante (alterno) y señalar lo siguiente:

- **a)** El tipo de sitio (caliente, tibio o frío);
- **b)** Si el sitio es propio o subcontratado con un tercero;
- **c)** Los procedimientos, el equipo y el personal que designa para poner en marcha tal sitio y
- **d)** Tiempo que le lleva poner en marcha el sitio, según las pruebas de eficiencia.

X. Transferencias de datos personales
XI. Resguardo de sistemas de tratamiento de datos personales con soportes físicos
XII. Bitácoras para accesos y operación cotidiana
XIII. Registro de incidentes
XIV. Acceso a las instalaciones
XV. Actualización del sistema de tratamiento de datos personales
XVI. Perfiles de usuario y contraseñas
XVII. Procedimientos de respaldo y recuperación de datos
XVIII. Plan de contingencia

7. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

26.1. Herramientas y recursos para monitoreo de la protección de datos personales

CENTRO DE ESTUDIOS MEXICANOS UNAM-SUDÁFRICA		
Identificador único*	CEM-SUD	
Formulario de registro	**FRSUD**	
Recurso*	**Descripción***	**Control***
N/A	*N/A*	*N/A*

CENTRO DE ESTUDIOS MEXICANOS UNAM-SUDÁFRICA		
Identificador único*	CEM-SUD	
Hoja de registro eventos	**HRSUD**	
Recurso*	**Descripción***	**Control***
N/A	*N/A*	*N/A*

26.2. Procedimiento para la revisión de las medidas de seguridad

CENTRO DE ESTUDIOS MEXICANOS UNAM-SUDÁFRICA		
Identificador único*	CEM-SUD	
Formulario de registro	**FRSUD**	
Medida de seguridad*	**Procedimiento***	**Responsable***
N/A	*N/A*	*N/A*

CENTRO DE ESTUDIOS MEXICANOS UNAM-SUDÁFRICA		
Identificador único*	CEM-SUD	
Hoja de registro eventos	**HRSUD**	
Medida de seguridad*	**Procedimiento***	**Responsable***
N/A	*N/A*	*N/A*

26.3. Resultados de la evaluación y pruebas a las medidas de seguridad

CENTRO DE ESTUDIOS MEXICANOS UNAM-SUDÁFRICA		
Identificador único*	CEM-SUD	
Formulario de registro	**FRSUD**	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***
N/A	*N/A*	*N/A*

CENTRO DE ESTUDIOS MEXICANOS UNAM-SUDÁFRICA		
Identificador único*	CEM-SUD	
Hoja de registro eventos	**HRSUD**	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***
N/A	*N/A*	*N/A*

26.4. Acciones para la corrección y actualización de las medidas de seguridad

CENTRO DE ESTUDIOS MEXICANOS UNAM-SUDÁFRICA		
Identificador único*	CEM-SUD	
Formulario de registro	**FRSUD**	
Medida de seguridad*	**Acciones***	**Responsable***
N/A	*N/A*	*N/A*

CENTRO DE ESTUDIOS MEXICANOS UNAM-SUDÁFRICA		
Identificador único*	CEM-SUD	
Hoja de registro eventos	**HRSUD**	
Medida de seguridad*	**Acciones***	**Responsable***
N/A	*N/A*	*N/A*

27. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

27.1. Programa de capacitación a los responsables de tratamiento de datos personales

CENTRO DE ESTUDIOS MEXICANOS UNAM-SUDÁFRICA			
Identificador único*	CEM-SUD		
Formulario de registro	**FRSUD**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
N/A	*N/A*	*N/A*	*N/A*

CENTRO DE ESTUDIOS MEXICANOS UNAM-SUDÁFRICA			
Identificador único*	CEM-SUD		
Hoja de registro eventos	**HRSUD**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
N/A	*N/A*	*N/A*	*N/A*

27.2. Programa de difusión de la protección a los datos personales

CENTRO DE ESTUDIOS MEXICANOS UNAM-SUDÁFRICA			
Identificador único*	CEM-SUD		
Formulario de registro	**FRSUD**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Curso-taller Derechos de autor	*Se mandará a que tomen un curso de Derechos de autor para que sepan cómo proteger los datos personales*	*Tiene una duración de 8 clases, impartidas dos veces a la semana de dos horas cada clase*	*Comunidad UNAM, público externo. El curso-taller está vigente y se imparte dos veces al año*

CENTRO DE ESTUDIOS MEXICANOS UNAM-SUDÁFRICA			
Identificador único*	CEM-SUD		
Hoja de registro eventos	**HRSUD**		
Actividad*	**Descripción***	**Duración***	**Cobertura***

27.3. Procesos para la conservación, preservación y respaldos de información

CENTRO DE ESTUDIOS MEXICANOS UNAM-SUDÁFRICA		
Identificador único*	CEM-SUD	
Formulario de registro	**FRSUD**	
Proceso*	**Descripción***	**Responsable***
Respaldo de información	*El respaldo de información sólo se hace semestralmente y consiste en descargar una copia de las respuestas del formulario*	*Indicar:* *c) María Fernanda López Díaz* *d) 1 día*

CENTRO DE ESTUDIOS MEXICANOS UNAM-SUDÁFRICA		
Identificador único*	CEM-SUD	
Hoja de registro eventos	**HRSUD**	
Proceso*	**Descripción***	**Responsable***
Respaldo de información	*El respaldo de información sólo se hace semestralmente y consiste en descargar una copia de las respuestas de la hoja de registros de los eventos*	*Indicar:* *e) María Fernanda López Díaz* *a) 1 día*

27.4. Procesos de borrado seguro y disposición final de equipos y componentes informáticos

CENTRO DE ESTUDIOS MEXICANOS UNAM-SUDÁFRICA		
Identificador único*	CEM-SUD	
Formulario de registro	**FRSUD**	
Proceso*	**Descripción***	**Responsable***
Cambio de contraseñas *Carta responsiva*	*Se realiza un cambio de contraseñas de todas las cuentas* *Los usuarios que tienen acceso a las cuentas firman una carta responsiva en donde se comprometen en no difundir nada sobre la sede*	*Indicar:* *c) María Fernanda López Díaz* *d) 1 día*

CENTRO DE ESTUDIOS MEXICANOS UNAM-SUDÁFRICA		
Identificador único*	CEM-SUD	
Hoja de registro eventos	**HRSUD**	
Proceso*	**Descripción***	**Responsable***
Cambio de contraseñas *Carta responsiva*	*Se realiza un cambio de contraseñas de todas las cuentas* *Los usuarios que tienen acceso a las cuentas firman una carta responsiva en donde se comprometen en no difundir nada sobre la sede*	*Indicar:* *a) María Fernanda López Díaz* *b) 1 día*

28. PROCEDIMIENTO PARA LA CANCELACIÓN DE UN SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

No existe un sistema de tratamiento de datos personales que se quiera eliminar por el momento.

(Informar y describir el procedimiento para la cancelación de un sistema de tratamiento de datos personales.)

EE) DATOS DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES QUE SERÁ CANCELADO:

a) Denominación
b) Motivo de la cancelación

FF) PLAZOS Y CONDICIONES PARA EL BLOQUEO DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES:

(Señalar el periodo de bloqueo, considerando los plazos de prescripción para el ejercicio de algún derecho por parte de los titulares de conformidad con la normatividad de cada área universitaria. Asimismo, se debe señalar las condiciones y el procedimiento que se seguirá para realizar el bloqueo)

GG) MEDIDAS DE SEGURIDAD PARA EL BLOQUEO Y POSTERIOR SUPRESIÓN DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES:
(Describir las medidas de seguridad aplicables al periodo de bloqueo y la supresión del sistema, considerando el nivel de protección requerido en virtud del tipo de datos personales contenidos en el sistema)

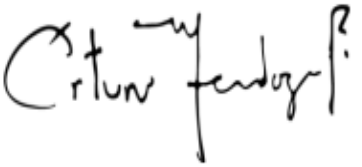
HH) PROCEDIMIENTO PARA LA SUPRESIÓN DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

(Describir el procedimiento para suprimir el sistema, una vez cumplido el plazo de bloqueo)

II) MECANISMOS PARA LA SUPRESIÓN DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

(Describir las técnicas para la eliminación física del sistema)

11. APROBACIÓN DEL DOCUMENTO DE SEGURIDAD

		Nombre y firma de quienes revisaron el presente documento:
Responsable del desarrollo:	María Fernanda López Díaz Coordinadora de Sistemas e informática de la sede flopez@sudafrica.unam.mx +27 17168124	
Revisó:	Dr. David Ruiz Guzmán Coordinador de Relaciones y Gestión flopez@sudafrica.unam.mx +27 17179141	
Autorizó:	Dr. Arturo Mendoza Ramos Director amendoza@sudafrica.unam.mx +27 17179143	
Fecha de aprobación:	12 octubre 2022	UNAM-SUDÁFRICA CENTRO DE ESTUDIOS MEXICANOS
Fecha de actualización:	24 de septiembre 2022	

ANEXO II. FORMATO UNIVERSITARIO DE "SOLICITUD DE EJERCICIO DE DERECHOS ARCO"

Formato de solicitud de ejercicio de derechos Acceso, Rectificación, Cancelación y Oposición (ARCO)

Con fundamento en el artículo 54 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, esta área universitaria le solicita llenar el presente formato para ejercer sus derechos de Acceso, Rectificación, Cancelación y Oposición.

1. Datos del Área Universitaria de la UNAM responsable de tratar los datos personales*:

2. Datos del Titular de los Datos Personales*:

Primer apellido:	Segundo apellido:	Nombre(s):
CURP (para evitar homónimos):		

3. Datos del solicitante:

Primer apellido:	Segundo apellido:	Nombre(s):
Indicar si los datos corresponden a:		
☐Titular		
☐Menor de edad		
☐Persona que se encuentren en estado de interdicción o incapacidad establecida por ley.		
☐Fallecida		
Datos de identidad y representación legal (opcional, solo si usted no es el titular de los datos personales)		
☐Persona física:		
☐Nombre completo del representante:		
☐Representación de un menor de edad:		
☐Representación de una persona que se encuentren en estado de interdicción o incapacidad establecida por ley.		
☐Persona moral:		
☐Nombre o razón social del representante:		
Registro Federal de Contribuyentes (RFC):		
Documento con el que acredita la representación:		
☐Poder notarial ☐Carta poder simple signada ante dos testigos (con copia de los documentos que acrediten la identidad de los testigos y titular) ☐Declaración en comparecencia del Titular (en las instalaciones del área universitaria).		

4. Documento oficial de identificación del titular o solicitante (sólo originales) *:

☐Credencial para votar (INE)	☐Pasaporte	☐Licencia de conducir
☐Cédula profesional	☐Cartilla del Servicio militar nacional	☐Documento migratorio
☐Acta de nacimiento	☐Acta de defunción	☐Otra identificación con fotografía (especifique):

5. Medio por el cual prefiere que le sea notificada la puesta a disposición de la respuesta*:

☐Acudir al área universitaria donde presentó este formato	☐Correo electrónico (especificar):

6. Modalidad en la cual prefiere le sean entregados los datos, en caso de ser procedente. *

☐Copia simple	☐Correo electrónico
☐Copia certificada	☐ Otro medio electrónico como USB/CD ROOM/ DVD *(previo depósito de ficha de pago):*
☐Consultas directas	☐Yo proporciono el medio magnético o electrónico para reproducir los datos personales.

7. Tipo de solicitud de ejercicio de Derechos Acceso, Rectificación, Cancelación y Oposición (ARCO) a datos personales*:

☐ACCESO
Describir la información datos personales que obran en posesión del área universitaria y a los que requiere tener acceso*: _____ ___ _____ _____ _____
Señalar el nombre y ubicación del archivo o registro de datos personales*: _____ ____ _____ _____ _____
☐RECTIFICACIÓN
☐Son inexactos.
☐Son incompletos.
☐Requieren ser actualizados
Justificación y documentación original que acompaña para motivar su petición*: _____ _____ _____ _____
CANCELACIÓN (supresión o eliminación)
Causas que motivan la cancelación*:
OPOSICIÓN (cese del tratamiento)
Causas que motivan la oposición (daño o perjuicio que le causa la persistencia del tratamiento de sus datos)*:_____ ___ _____ ____
Señalar si es para una finalidad específica o para todos los sistemas de información que obren en el área universitaria*._____ ____
Documentación original que acompaña para motivar su petición*: _____ ____
Señalar la referencia o documento que facilite la localización de sus datos personales*
_____ _____

Leí el Aviso de privacidad del área universitaria a la que acudo y en este acto otorgo el consentimiento para que mis datos personales sean tratados conforme al mismo.

_____

Firma o huella dactilar*

Plazos y procedimiento para la atención de las solicitudes de ejercicio de derechos ARCO:
Una vez que se presentó la solicitud, esta área universitaria cuenta con:

- Un plazo de 20 días hábiles, contados a partir del día siguiente a la recepción de la solicitud, para informarle si procede o no el ejercicio del derecho solicitado.
- Un plazo de 15 días hábiles, contados a partir del día siguiente en el que le haya notificado la respuesta anterior, en caso de que haya procedido el ejercicio del derecho, deberá llevar a cabo las acciones necesarias para hacerlo efectivo.

El ejercicio de los derechos ARCO será sencillo y gratuito, siempre que no rebase las 20 hojas simples, por lo que las áreas universitarias realizarán el cobro del costo de reproducción de acuerdo con los Lineamientos para la determinación de los costos de reproducción y envío en el marco de solicitudes de acceso a Información y entrega de datos personales en la Universidad Nacional Autónoma de México.

ANEXO III. CARTA DE CONFIDENCIALIDAD

Carta compromiso de confidencialidad, no divulgación, reserva y resguardo de información y datos personales

(Este documento debe firmarse por todas aquellas personas que por su empleo, cargo o comisión en la Universidad reciban y traten información confidencial de otras personas)

CIUDAD DE _____, A (DD-MM-AAAA)

(Nombre completo), *(cargo)*, adscrita(o) *(dependencia/entidad de adscripción)* de la Universidad Nacional Autónoma de México (en adelante la UNAM) acepto los términos y condiciones, que se describen más adelante, de resguardo, reserva, custodia y protección de la seguridad y confidencialidad de la información, datos personales y de todo tipo de documentos propiedad de la UNAM de los que tenga conocimiento, con motivo de las funciones que desempeño en la Universidad.

El presente compromiso me responsabiliza respecto de la información que me sea proporcionada por la UNAM, ya sea de forma oral, escrita, impresa, sonora, visual, electrónica, informática u holográfica, contenida en cualquier tipo de documento, que puede consistir en: expedientes, reportes, estudios, actas, resoluciones, oficios, correspondencia, acuerdos, directivas, directrices, circulares, contratos, convenios, instructivos, notas, memorandos, estadísticas, o bien, cualquier otro registro en medio conocido o por conocer que documente el ejercicio de las facultades, funciones y competencias del área universitaria y de los servidores universitarios, sin importar su fuente o fecha de elaboración.

La información que me sea proporcionada podría ser considerada, según el caso, como reservada, privilegiada y confidencial, en los términos de las leyes aplicables, por lo que me obligo a protegerla, reservarla, resguardarla y no divulgarla, utilizándola única y exclusivamente para llevar a cabo y cumplir con las actividades y obligaciones que expresamente me sean conferidas por la Universidad.

Es mi responsabilidad no reproducir, hacer pública o divulgar a terceros la información objeto de la presente Carta, y de cumplir con las medidas de seguridad adecuadas al tipo de documento con el que se trabaje.

Mi obligación de confidencialidad no es aplicable en los siguientes casos:

d) Cuando la información se encuentre en el dominio público en el momento en que me sea suministrada o, una vez suministrada, ésta se haga pública.
e) Cuando la legislación vigente o un mandato judicial exija su divulgación.
f) Cuando la información se desarrolle o reciba legítimamente de terceros, de forma totalmente independiente a mi relación con la Universidad.

A t e n t a m e n t e

_____
Firma o huella dactilar

ANEXO IV. RUTA CRÍTICA PARA CUMPLIMIENTO DE LAS MEDIDAS DE SEGURIDAD TÉCNICAS (MST)

A continuación, se presentan los requisitos técnicos para sistemas de información, descritos en las MST del capítulo II de las Normas Complementarias, por orden de prioridad, esto es: de los mínimos indispensables para asegurar los datos personales hasta los necesarios para incrementar la protección de dichos datos.

Dada la complejidad de diversos sistemas en la UNAM, se ha dispuesto la ruta crítica para el cumplimiento de las MST en tres etapas para los sistemas de información que a la fecha de publicación de esta guía estén en producción o funcionamiento. Todo sistema de información deberá satisfacer a cabalidad el 100% de las MST en un tiempo máximo de un año contado a partir de la publicación de las MST para conservar su registro y publicación dentro del dominio institucional .***unam.mx***.

A) **Etapa 1. Corto plazo**. Requisitos de misión crítica y mínimos indispensables para la protección de datos personales y datos personales sensibles. Cumplimiento obligatorio en menos de treinta días hábiles.
B) **Etapa 2. Mediano plazo**. Requisitos importantes para garantizar la protección de datos personales y datos personales sensibles. Ejecución estimada entre un mes y seis meses.
C) **Etapa 3. Largo plazo**. Requisitos necesarios para reforzar la seguridad en la protección de datos personales y datos personales sensibles. Ejecución estimada entre seis y doce meses.

Instrucciones

- Para cada MST se ha diseñado un formato, el cual está numerado en correspondencia con la ruta crítica de cumplimiento.
- Se deberán completar todos los formatos aplicables por cada uno de los sistemas de información a cargo del Área Universitaria.
- Todos los formatos deberán integrar el anexo del documento de seguridad de datos personales.
- En el caso de los sistemas que estén en desarrollo al momento de la publicación de las Normas complementarias, deberán cumplir con el 100% de las MST, previo a su publicación como sistema en producción.
- Es requisito indispensable el cumplimiento de las MST para conservar el registro dominio institucional ***.unam.mx*** en el caso de servicios Web.

Núm. formato	Etapa	Duración estimada	Medidas de seguridad técnicas y proceso recomendado para su cumplimiento
ETAPA 1			
Anexo I, numerales 1 y 2	1	Un día hábil	**Generar el inventario de sistemas de tratamiento de datos personales y la Estructura de descripción de los sistemas de tratamiento de datos personales.** **A)** Integrar la información correspondiente a todos los sistemas que dan tratamiento de datos personales en el área universitaria. **B)** Llenar formatos y colocar nombre y firma de quien realizó la acción.
1	1	Un día hábil	**Artículo 18. I. c) Utilizar datos no personales durante el desarrollo y pruebas de los sistemas.** **A)** Realizar respaldo completo de la base de datos. **B)** Ejecutar consulta en el sistema de información, por medio de formato o comandos. **C)** Verificar que los datos usados en el desarrollo no correspondan a personas identificables.

Núm. formato	Etapa	Duración estimada	Medidas de seguridad técnicas y proceso recomendado para su cumplimiento
			D) Si se usan datos de personas identificables, cambiar por datos genéricos o datos ficticios y regresar al punto B. **E)** Si no se usan datos de personas identificables, llenar formato 1 con nombre y firma de quien realizó la acción, fecha de inicio y de conclusión.
2	1	Un día hábil	**Artículo 18. I. e) Asignar o revocar los privilegios de acceso para los usuarios teniendo como base el principio del menor privilegio.**
			A) Realizar respaldo completo de la base de datos. **B)** Ejecutar consulta en el sistema de información de la lista de usuarios y sus niveles o privilegios de acceso. **C)** Validar que los niveles de acceso son acordes a la relación del usuario con el tratamiento de datos personales. **D)** Si hay usuarios con privilegios

Núm. formato	Etapa	Duración estimada	Medidas de seguridad técnicas y proceso recomendado para su cumplimiento
			mayores a los que les son necesarios, cambiar al mínimo indispensable e informarlo al usuario. Regresar al punto B. **E)** Si los privilegios de acceso son correctos para los usuarios, llenar formato 2 con nombre y firma de quien realizó la acción, fecha de inicio y de conclusión.
3	1	Tres días hábiles	**Artículo 18. I. g) Instalar y mantener vigentes certificados de comunicación segura SSL en el caso de servicios basados en Web.** **A)** En caso de no tener un certificado SSL vigente, enviar correo electrónico al Departamento de Firma Electrónica de DGTIC a firma.tic@unam.mx solicitando la asignación. **B)** El Departamento de Firma Electrónica Avanzada envía procedimiento para obtención de CSR del servidor, formato de la solicitud y costos de

Núm. formato	Etapa	Duración estimada	Medidas de seguridad técnicas y proceso recomendado para su cumplimiento
			recuperación en función del tipo de certificado requerido (organizacional, comodín o corporativo). **C)** Completar documentación, proceso y pago de costo de recuperación. Enviar comprobantes a firma.tic@unam.mx. **D)** Al recibir el certificado SSL, instalarlo en el servidor de acuerdo con las instrucciones recibidas junto con el certificado. **E)** Llenar formato 3 y colocar nombre y firma de quien realizó la acción.
4	1	Dos días hábiles	**Artículo 18. I. h) Definir el plan de respaldos de la información, incluyendo periodicidad y alcance.** **A)** Elaborar documento con la secuencia de respaldos al menos con el siguiente orden: - Diario – incremental. - Semanal – incremental. - Mensual – total.

Núm. formato	Etapa	Duración estimada	Medidas de seguridad técnicas y proceso recomendado para su cumplimiento
			B) Establecer en el plan los medios para resguardo del respaldo y su forma de identificación: - En línea: mismo equipo donde se ejecuta el sistema. - Respaldo como servicio: otro equipo de almacenamiento. - Fuera de línea: medios magnéticos (cintas, discos) y/u ópticos. **C)** Incluir en el plan: - Responsables de cada tipo y medio de respaldo. - Rotación de respaldos y medios. - Áreas de resguardo. - Métodos de cifrado. - RTO: *Recovery Time Objective*. Tiempo objetivo de recuperación. - RPO: *Recovery Point Objective*: Punto objetivo de recuperación. **D)** Concluir este documento, adjuntarlo a SGPDP, llenar formato 4 y colocar nombre y firma de quien realizó la acción.
5	1	Un día hábil	**Artículo 18. I. i) Definir el**

Núm. formato	Etapa	Duración estimada	Medidas de seguridad técnicas y proceso recomendado para su cumplimiento
			procedimiento para el borrado seguro.
			A) Elaborar documento con el procedimiento y la herramienta para borrado seguro en función del tipo de base de datos para registros, tablas y base de datos. **B)** Incluir en el documento de borrado seguro el proceso de verificación de la no existencia del dato, generalmente por medio de consultas y de copias de respaldo. **C)** El borrado seguro debe incluirse en los respaldos incrementales y totales y en cualquiera de los medios de respaldo, así como máquinas virtuales o contenedores. **D)** Concluir este documento, adjuntarlo a SGPDP llenar formato 5 y colocar nombre y firma de quien realizó la acción.
6	1	Un día hábil	**Artículo 18. II. a) Sincronizar la fecha y hora con el servidor NTP**

Núm. formato	Etapa	Duración estimada	Medidas de seguridad técnicas y proceso recomendado para su cumplimiento
			(Network Time Protocol) oficial de la UNAM

			A) Realizar la verificación y configuración con privilegio de administrador del sistema operativo. **B)** En función del sistema operativo, acceder a la configuración de servidor de tiempo (NTP) en interfaz gráfica o por medio de línea de comandos. *Por ejemplo*, en el caso del sistema operativo Linux: - Verificar la existencia del archivo */etc/ntp.conf* - Editar el archivo *ntp.conf* incluyendo en la primera línea: *server ntpdgtic.redunam.unam.mx* ***ó*** *server 132.247.169.17* - Reiniciar el demonio del cliente NTP con el comando *sudo service ntp reload.* **C)** En caso de no tener el cliente NTP instalado, descargarlo del repositorio de aplicaciones del sistema operativo, instalarlo y regresar al punto B. **D)** Llenar formato 6 y colocar nombre y firma de quien realizó la acción.

Núm. formato	Etapa	Duración estimada	Medidas de seguridad técnicas y proceso recomendado para su cumplimiento
7	1	Dos días hábiles	**Artículo 18. II. b) Instalar y mantener actualizado el software antimalware.** **A)** En función del sistema operativo, instalar uno o varios programas para la contención de malware. *Por ejemplo*, para el caso del sistema operativo Linux existen herramientas de código abierto y uso libre como *chkrootkit, rootkit hunter, bothunter, clamAV, avast*, entre otros, que se pueden instalar desde el repositorio correspondiente a la distribución de Linux en uso. **B)** Disponer de comandos para la localización de amenazas. *Por ejemplo*, para el caso de Linux, se recomienda usar el comando *grep* para la detección de cadenas regulares de texto en las invocaciones al *shell*. **C)** Una vez instalada la solución, verificar

Núm. formato	Etapa	Duración estimada	Medidas de seguridad técnicas y proceso recomendado para su cumplimiento
			periódicamente su actualización. **D)** Llenar formato 7 y colocar nombre y firma de quien realizó la acción.
8	1	Cuatro días hábiles	**Artículo 18. II. c) Instalar las actualizaciones de seguridad más recientes disponibles.**
			A) En función del sistema operativo, se debe revisar la vigencia y actualización de las herramientas de seguridad de la información. *Por ejemplo*, en el sistema operativo Linux ejecutar *apt-get update* para obtener la lista de actualizaciones, especialmente en el repositorio *security* de la respectiva distribución. **B)** Realizar un respaldo del sistema para garantizar retorno a versión anterior en caso de incompatibilidad con alguna aplicación de las actualizaciones de seguridad. **C)** Instalar las actualizaciones en el sistema operativo.

Núm. formato	Etapa	Duración estimada	Medidas de seguridad técnicas y proceso recomendado para su cumplimiento
			D) Llenar formato 8 y colocar nombre y firma de quien realizó la acción.
9	1	Cuatro días hábiles	**Artículo 19. I. a) Aplicar un mecanismo de autenticación para las personas autorizadas con base en el principio del menor privilegio.**
			A) Verificar el tipo de control de acceso al sistema, esto es: a través de contraseñas, claves, identificadores, nombres de usuario, nombres de dominio, entre otros. Según sea aplicable al sistema de información en lo particular. En caso de no tener un control de acceso establecer al menos uno como: usuarios de sistema operativo, cuenta y contraseña de sistema. **B)** Revisar que los privilegios de acceso sean los adecuados en función del rol del usuario. *Por ejemplo:* el usuario de conexión a la base de datos no

Núm. formato	Etapa	Duración estimada	Medidas de seguridad técnicas y proceso recomendado para su cumplimiento
			debe estar asignado a alguna cuenta del personal que tiene acceso al sistema. **D)** Llenar formato 9 y colocar nombre y firma de quien realizó la acción.
10	1	Dos días hábiles	**Artículo 19. II. b) Evitar la instalación de cualquier elemento de software que implique algún riesgo para el tratamiento de datos personales.**
			A) Dependiendo del sistema operativo, configurar las actualizaciones solamente para versiones maduras o revisiones certificadas de las aplicaciones. *Por ejemplo*: en sistemas Linux desactivar la instalación de versiones *beta, test, debug, non-official.* **B)** De la lista de software instalado, verificar el consumo de recursos de aplicaciones *TSR (Terminal and Stay Resident)*. Identificar demonios que ocupen excesiva RAM o tiempo de ejecución en el

Núm. formato	Etapa	Duración estimada	Medidas de seguridad técnicas y proceso recomendado para su cumplimiento
			procesador. *Por ejemplo*: En sistemas Windows usar el Administrador de Tareas para identificar programas de alto consumo. **C)** Desinstalar toda aquella aplicación, librería, programa, paquetería o servicio que no sea estrictamente necesario para la operación del sistema. *Por ejemplo*, si el servidor Linux no proporcionará direcciones IP, el demonio o servicio *dchpd* no debe estar instalado. **D)** Llenar formato 10 y colocar nombre y firma de quien realizó la acción.
11	1	Dos días hábiles	**Artículo 19. III. a) Establecer las medidas físicas de seguridad que controlen el acceso a los equipos.** **A)** Identificar las medidas físicas que restrinjan el acceso físico a equipos, tales como chapas, puertas, biométricos.

Núm. formato	Etapa	Duración estimada	Medidas de seguridad técnicas y proceso recomendado para su cumplimiento
			B) En función de la ubicación del equipo de cómputo, hacer una relación de las condiciones más adecuadas para su protección que aún sean necesarias implementar. **C)** Establecer y seguir un plan de mejoramiento de la protección física de equipos. *Por ejemplo*; cámaras de videovigilancia, bitácoras, vigilantes, cuartos cerrados, racks con puerta y chapa, candados en equipos, bloqueo o desconexión física de puertos USB, alarmas y sensores, según sea lo más conveniente como mínimo para la protección de los datos. **D)** Llenar formato 11 y colocar nombre y firma de quien realizó la acción.
12	1	Un día hábil	**Artículo 19. III. b) Restringir la salida de equipos de las instalaciones de cada área universitaria.**
			A) Diseñar una bitácora o formato para el registro de entrada y salida de

Núm. formato	Etapa	Duración estimada	Medidas de seguridad técnicas y proceso recomendado para su cumplimiento
			equipos de cómputo y periféricos asociados como discos duros, cintas, unidades flash, discos ópticos, monitores, teclados, ratones y en lo general todo componente de un equipo. **B)** La bitácora de entrada y salida debe incluir el registro de número de serie e inventario UNAM. responsable de ingreso o egreso del componente y firma autorizada del responsable del área. **C)** Incluir en el procedimiento la revisión periódica (al menos una vez al mes) de la consistencia del inventario registrado contra la bitácora de entrada y salida. **D)** Llenar 12 y colocar nombre y firma de quien realizó la acción.
13	1	Tres días hábiles	**Artículo 19. IV. a) Realizar la transmisión de datos personales a través de un canal cifrado.**
			A) Identificar, mediante el

Núm. formato	Etapa	Duración estimada	Medidas de seguridad técnicas y proceso recomendado para su cumplimiento
			administrador de aplicaciones que corresponda al sistema operativo, los protocolos y aplicaciones instalados para comunicación cifrada. *Por ejemplo*: *SFTP (Secure File Transfer Protocol), SSH (Secure Shell), SCP (Secure Copy*). **B)** Instalar con el administrador de aplicaciones o comando similar los protocolos de comunicación cifrada que sean necesarios para el tipo de transacciones y accesos del sistema. *Por ejemplo*, en el caso de requerir ejecutar comandos de forma remota en un servidor Linux, instalarlo con el comando *apt-get install openssh-server*. **C)** Activar los protocolos de comunicación encriptada en el servidor. *Por ejemplo*: en Linux con el comando *sudo systemctl enable ssh*. **D)** Llenar formato 13 y colocar nombre y

Núm. formato	Etapa	Duración estimada	Medidas de seguridad técnicas y proceso recomendado para su cumplimiento
			firma de quien realizó la acción.
14	1	Tres días hábiles	**Artículo 20. Aplicar el procedimiento de borrado seguro que impida la recuperación en las bases de datos y todos sus respaldos.**
			A) Realizar una copia integral del sistema de información y colocarla en un servicio temporal. *Por ejemplo:* máquina virtual o directorio temporal en el servidor. **B)** Ingresar a la copia del sistema de información y realizar el borrado de un registro. Verificar que el dato no persiste en la base de datos por medio de forma de consulta o comando. **C)** Realizar el mismo proceso del punto B para una tabla y finalmente para la base de datos completa. D) En caso de persistencia del dato, instalar y ejecutar herramientas para borrado seguro. *Por ejemplo*: en Linux se

Núm. formato	Etapa	Duración estimada	Medidas de seguridad técnicas y proceso recomendado para su cumplimiento
			dispone *de shred, wipe, secure-delete, srm, sfill, sswap, sdmem,* que se pueden instalar desde el administrador de aplicaciones. **D)** Llenar formato 14 y colocar nombre y firma de quien realizó la acción.
ETAPA 2			
15	2	Hito	**Artículo 18. I. a) Utilizar los datos personales preexistentes que estén disponibles, de acuerdo con sus respectivas políticas de uso y acceso, en bases de datos a cargo de otras áreas universitarias.**
			A) Disponer del inventario de datos del sistema de información, esto es: documento con la descripción de tablas, campos, tipo de datos, relaciones y consultas. **B)** Con el Área Universitaria que esté identificada como la instancia autoritativa en materia de datos personales, comparar el inventario de datos.

Núm. formato	Etapa	Duración estimada	Medidas de seguridad técnicas y proceso recomendado para su cumplimiento
			Por ejemplo: La Dirección General de Administración Escolar es la dependencia autoritativa en materia de datos personales de estudiantes. **C)** Establecer el acuerdo por escrito para el uso de campos específicos de datos personales de la instancia autoritativa. **D)** Establecer el mecanismo de comunicación entre el sistema de información y el de la instancia autoritativa. *Por ejemplo*: *Webservices*, transferencia *SFTP.* **E)** Llenar 15 y colocar nombre y firma de quien realizó la acción.
16	2	Ocho días hábiles	**Artículo 18. I. d) Permitir el acceso al código fuente de los sistemas exclusivamente a la administración del sistema y personal para el desarrollo.**
			A) Recopilar el código fuente y documentación del sistema de

Núm. formato	Etapa	Duración estimada	Medidas de seguridad técnicas y proceso recomendado para su cumplimiento
			información en todas sus versiones disponibles. **B)** Depositar en un equipo central de desarrollo todas las versiones de código fuente y su documentación (inventario de datos, manual de administración, manual de programador). **C)** Establecer control de acceso por usuario y contraseña hacia el equipo central de desarrollo. **D)** Activar bitácoras de acceso (*log*) hacia el equipo central de desarrollo. **E)** Proporcionar las credenciales de acceso al equipo central de desarrollo exclusivamente al personal a cargo de programación y mantenimiento de código y manuales. **F)** Llenar formato 16 y colocar nombre y firma de quien realizó la acción.
17	2	Cuatro días hábiles	**Artículo 19. I. b) Establecer las medidas de seguridad en los periodos de**

Núm. formato	Etapa	Duración estimada	Medidas de seguridad técnicas y proceso recomendado para su cumplimiento
			inactividad o mantenimiento.
			A) Elaborar documento con las medidas necesarias de seguridad para períodos vacacionales, contingencias y ventanas de mantenimiento, incluyendo: control de acceso físico y lógico a los equipos, ejecución de respaldos, sistemas de alta disponibilidad (redundancia). **B)** Incluir en el documento la descripción de los procedimientos en caso de contingencia por falla de servicio de red, falla de equipo de cómputo, falla lógica en sistema operativo. **C)** Incluir en el documento el directorio de responsables de cada uno de los puntos a atender: apagado seguro, apagado fortuito, apagado programado, verificación de integridad de información, activación de

Núm. formato	Etapa	Duración estimada	Medidas de seguridad técnicas y proceso recomendado para su cumplimiento
			servicios locales o de respaldo. **D)** Llenar formato 17 y colocar nombre y firma de quien realizó la acción.
18	2	Ocho días hábiles	**Artículo 19. I. c) Generar respaldos y aplicar los mecanismos de control y protección para su resguardo.**
			A) De acuerdo con el plan de respaldos establecido, ejecutar la secuencia de respaldos. **B)** Designar responsables de respaldos y responsables de verificación de respaldos. **C)** Completar bitácora de control de los respaldos, indicando fecha, hora, tipo de respaldo (integral, total, parcial de registros), ejecutor y revisor del respaldo, ubicación del respaldo, medio y etiqueta. **D)** Llenar formato 18 y colocar nombre y firma de quien realizó la acción.
19	2		**Artículo 19. I. d) Impedir el uso de**

Núm. formato	Etapa	Duración estimada	Medidas de seguridad técnicas y proceso recomendado para su cumplimiento
			cuentas y servicios gestionados por personas físicas para el tratamiento de los datos personales.
		Veinte días hábiles	**A)** Realizar revisión integral del sistema de información en materia de accesos, cuentas y servicios. *Por ejemplo*: En caso de consultar vía un *Webservice* a un sistema autoritativo de datos personales en la DGAE, identificar la cuenta de acceso a ese sistema. **B)** Determinar si las cuentas de acceso a servicios locales o remotos están bajo el control de la administración del sistema. *Por ejemplo*: Si la cuenta de acceso a un *Webservice* – su usuario y contraseña – está bajo el control del administrador del sistema, o si un respaldo que se realiza en un equipo remoto es con una cuenta y contraseña controlada por el administrador del sistema. **C)** Si las cuentas de acceso a servicios

Núm. formato	Etapa	Duración estimada	Medidas de seguridad técnicas y proceso recomendado para su cumplimiento
			locales o remotos pertenecen a personas del Área Universitaria, cambiarlas por cuentas institucionales dentro del control de la instancia universitaria. *Por ejemplo*: si la identificación para acceder a un respaldo remoto es del tipo xxx@google.com, deberá cambiarse por una cuenta del tipo xxxx@unam.mx. **D)** Llenar formato 19 y colocar nombre y firma de quien realizó la acción.
20	2	Cuatro días hábiles	**Artículo 19. II. a) Proteger ante manipulaciones indebidas y accesos no autorizados las bitácoras y los dispositivos donde se almacenan.** **A)** Elaborar una lista de las bitácoras relacionadas con el sistema de información, tanto en medio digital como físico. *Por ejemplo*: En el equipo de cómputo las bitácoras de

Núm. formato	Etapa	Duración estimada	Medidas de seguridad técnicas y proceso recomendado para su cumplimiento
			acceso de usuarios al sistema operativo y al sistema de información (*logs*), de forma física las bitácoras de acceso al área donde está el equipo de cómputo. **B)** Junto a la lista elaborar el cronograma de revisión de integridad y respaldo de las bitácoras. *Por ejemplo*: diario, semanal, mensual. **C)** Establecer en el documento el procedimiento de resguardo de las bitácoras. *Por ejemplo*: respaldo y protección de *logs* en el caso de equipo de cómputo o zonas seguras de almacenamiento de bitácoras en papel, digitalización de registros. **D)** Llenar formato 20 y colocar nombre y firma de quien realizó la acción.
21	2	Cuatro días hábiles	**Artículo 19. IV. b) Supervisar los controles de seguridad en la red de datos donde opere el sistema**

Núm. formato	Etapa	Duración estimada	Medidas de seguridad técnicas y proceso recomendado para su cumplimiento
			para tratamiento de datos personales.
			A) Identificar los equipos activos de red que permiten la conexión del equipo de cómputo con el sistema de información, incluyendo marca, modelo, versión de software, vigencia de mantenimiento y capacidades de protección de las comunicaciones. **B)** Determinar las reglas de seguridad físicas (acceso restringido, cuartos de telecomunicaciones) y lógicas (cuentas de acceso, puertos activos, protocolos activos) para el equipo de red. **C)** Incluir en las acciones para aseguramiento de la red de datos aquellas que sean necesarias en función de los controles actuales. Definir un plan de regularización de la seguridad en caso de ser aplicable. **D)** Mantener actualizados los equipos activos de red y con un

Núm. formato	Etapa	Duración estimada	Medidas de seguridad técnicas y proceso recomendado para su cumplimiento
			programa de mantenimiento. **E)** Identificar y en su caso programar la instalación de equipo para seguridad perimetral de la red de datos. **D)** Llenar formato 21 y colocar nombre y firma de quien realizó la acción.
22	2	Cuatro días hábiles	**Artículo 19. IV. c) Proporcionar el acceso exclusivamente desde redes y servicios autorizados.**
			A) Revisar los puertos de comunicación (*TCP y UDP*) que requiera el sistema de información para su operación. *Por ejemplo*: para servicios *Web* los puertos 80 y 8080 son los convencionales. **B)** Activar en el sistema operativo la herramienta correspondiente para el control de puertos de comunicación. *Por ejemplo*, en Linux puede tratarse de un *firewall* a nivel de software o las herramientas que

Núm. formato	Etapa	Duración estimada	Medidas de seguridad técnicas y proceso recomendado para su cumplimiento
			para tal efecto contenga la distribución correspondiente del sistema operativo. **C)** Dejar activos solamente los puertos necesarios para la operación del sistema. **D)** Activar el filtrado de la comunicación por direccionamiento IP en caso de ser posible para la operación del sistema. *Por ejemplo*: Permitir el acceso al puerto de *SSH* solamente a direcciones IP en una subred de la UNAM (132.248.x.y) o a un grupo de direcciones IP específicas. **E)** Llenar formato 22 y colocar nombre y firma de quien realizó la acción.
ETAPA 3			
23	3	Veinte días hábiles	**Artículo 18. I. b) Contar con entornos para desarrollo, pruebas y operación.** **A)** Instalar y configurar equipos similares en características, preferentemente virtuales, a los

Núm. formato	Etapa	Duración estimada	Medidas de seguridad técnicas y proceso recomendado para su cumplimiento
			equipos donde se instalará el sistema de información en su nueva o actualizada versión. **B)** Crear un repositorio en un equipo central de desarrollo para el resguardo de códigos, documentación, inventarios de datos y manuales de usuario, administrador y programador. **C)** Ejecutar las pruebas de nuevas versiones o actualizaciones del sistema de información en el equipo dispuesto para tal efecto. Nunca usar -equipos físicos o virtuales con el sistema actualmente en producción como las plataformas para evaluación de versiones en desarrollo. **D)** Llenar formato 23 y colocar nombre y firma de quien realizó la acción.
24	3	Veinte días hábiles	**Artículo 18. I. f) Cumplir con las especificaciones de seguridad informática previo**

Núm. formato	Etapa	Duración estimada	Medidas de seguridad técnicas y proceso recomendado para su cumplimiento
			a la puesta en operación.
			A) Una vez concluido el desarrollo o actualización de un sistema de información, solicitar al área de seguridad del Área Universitaria la revisión de seguridad informática del sistema, lo que incluye: pruebas de penetración, pruebas de estabilidad, pruebas de carga y endurecimiento de la seguridad. En caso de no contar con esa área, requerirlo a UNAM CERT al correo seguridad.tic@unam.mx . **B)** Una vez recibido el reporte del área de seguridad, aplicar las medidas de corrección que incluya el reporte. Regresar al punto A. **C)** Habiendo resuelto los hallazgos y sugerencias de mejora de la seguridad señalados por el área especializada, realizar la

Núm. formato	Etapa	Duración estimada	Medidas de seguridad técnicas y proceso recomendado para su cumplimiento
			instalación del sistema en la plataforma definitiva de cómputo, extrayéndolo del entorno de desarrollo. **D)** Llenar formato 24 y colocar nombre y firma de quien realizó la acción.
25	3	Hito	**Artículo 18. III. a) Utilizar equipos con componentes actualizados, protegidos con garantías y soporte, y con la capacidad suficiente para atender la demanda del servicio y de los usuarios.**
			A) Elaborar una lista del inventario de los equipos de cómputo, periféricos y de almacenamiento necesarios para la ejecución del sistema de información. **B)** Determinar la razón por la que el sistema de información requerirá estar localizado en un equipo físico y no en un servidor virtual. Con ello justificar

Núm. formato	Etapa	Duración estimada	Medidas de seguridad técnicas y proceso recomendado para su cumplimiento
			una adquisición o actualización. Por ejemplo: por incompatibilidad con hipervisores, necesidades de comunicación exclusivamente locales en la entidad y dependencia o el no necesitar de un entorno de alta disponibilidad automática. **C)** Identificar en el inventario versiones, introducción en el mercado, vida útil, contratos de mantenimiento y soporte para todos y cada uno de los componentes, en el caso de emplear equipo físico. **D)** Adquirir los componentes y elementos necesarios para la actualización, vigencia de soporte y capacidad para atención a los usuarios en el equipo de cómputo físico. **E)** Llenar formato 25 y colocar nombre y firma de quien realizó la acción.
26	3	Hito	**Artículo 18. III. b) Definir el programa**

Núm. formato	Etapa	Duración estimada	Medidas de seguridad técnicas y proceso recomendado para su cumplimiento
			de mantenimiento preventivo.
			A) De la lista de equipo de cómputo físico necesario para la operación del sistema de información, extraer las vigencias de mantenimiento. **B)** En caso de no estar en posibilidad de aplicar el mantenimiento preventivo por el personal del Área Universitaria, cotizar pólizas de mantenimiento de acuerdo con el tipo de componente, preferentemente una sola póliza para el conjunto del equipo físico. **C)** Adquirir las pólizas de mantenimiento preventivo y observar su vigencia. La vigencia no podrá ser menor de un año. **D)** Llenar formato 26 y colocar nombre y firma de quien realizó la acción.
27	3	Seis días hábiles	**Artículo 19. III. c) Aplicar el programa de mantenimiento**

Núm. formato	Etapa	Duración estimada	Medidas de seguridad técnicas y proceso recomendado para su cumplimiento
			preventivo a los equipos.
			A) En caso de que el personal del Área Universitaria pueda realizar el mantenimiento preventivo, definir el calendario de inactividad del sistema de información, notificar a los usuarios y aplicar el plan en caso de mantenimiento o inactividad. **B)** En caso de que sea a través de un proveedor que se proporcione el mantenimiento al equipo de cómputo, ejecutar el calendario de acciones preventivas en un período no superior a cada 3 meses hasta la conclusión del contrato o póliza respectivo. **C)** Llenar formato 27 y colocar nombre y firma de quien realizó la acción.
28	3	Hito	**Artículo 21. Solo se permitirá el uso de servicios de nube pública para el resguardo de archivos cifrados que contengan**

Núm. formato	Etapa	Duración estimada	Medidas de seguridad técnicas y proceso recomendado para su cumplimiento
			respaldos de la información.
			A) Identificar los respaldos que se tengan resguardados en servicios de nube pública. **B)** Verificar el cifrado en cada uno de los respaldos que se almacenen en nube pública. El cifrado no deberá ser de menor capacidad al equivalente a AES de 128 bits. **C)** Llenar formato 28 y colocar nombre y firma de quien realizó la acción.

ANEXO V. FORMATOS PARA CUMPLIMIENTO DE LAS MST

(Nombre del sistema A1)			Identificador único A1
Formato	**1**	**Verificación anual**	**Acción concluida**
Medida de seguridad técnica:	**Artículo 18. I. c) Utilizar datos no personales durante el desarrollo y pruebas de los sistemas.**		
Aplicable en:	I. Bases de datos y sistemas de tratamiento.		
Tiempo estimado:	Un día hábil.		
Importancia de la acción:	Evitar usar datos personales mientras se está desarrollando, actualizando o modificando el código fuente de un sistema de información.		
Proceso recomendado:	**A)** Realizar respaldo completo de la base de datos. **B)** Ejecutar consulta en el sistema de información, por medio de formato o comandos. **C)** Verificar que los datos usados en el desarrollo no correspondan a personas identificables. **D)** Si se usan datos de personas identificables, cambiar por datos genéricos o datos ficticios y regresar al punto B. **E)** Si no se usan datos de personas identificables, llenar formato con nombre y firma de quien realizó la acción, fecha de inicio y de conclusión.		
Mejores prácticas, referencias:	**1.-** Se recomienda al desarrollar un sistema de información no usar datos personales sino ficticios. **2.-** Se sugiere incluir en la documentación del desarrollo de un sistema de información el inventario de datos y el tipo de información de prueba.		
Conocimientos requeridos:	Administración de bases de datos. Consulta y actualización de tablas.		
Ejecución			**Fecha inicio**
Nombre y firma Programador, desarrollador o diseñador del sistema de información			**Fecha término**
Observaciones / anotaciones			

(Nombre del sistema A1)			Identificador único A1
Formato:		**Verificación anual**	**Acción concluida**
Medidas de seguridad técnicas:	**Artículo 18. I. e) Asignar o revocar los privilegios de acceso para los usuarios teniendo como base el principio del menor privilegio.**		
Aplicable en:	I. Bases de datos y sistemas de tratamiento.		
Tiempo estimado:	Un día hábil.		
Importancia de la acción:	No se deben asignar privilegios de acceso a los usuarios en niveles que no estén relacionados con su responsabilidad en el tratamiento de datos.		
Proceso recomendado:	**A)** Realizar respaldo completo de la base de datos. **B)** Ejecutar consulta en el sistema de información de la lista de usuarios y sus niveles o privilegios de acceso. **C)** Validar que los niveles de acceso son acordes a la relación del usuario con el tratamiento de datos personales. **D)** Si hay usuarios con privilegios mayores a los que les son necesarios, cambiar al mínimo indispensable e informarlo al usuario. Regresar al punto B. **E)** Si los privilegios de acceso son correctos para los usuarios, llenar formato con nombre y firma de quien realizó la acción, fecha de inicio y de conclusión.		
Mejores prácticas, referencias:	**1.-** Definir niveles de acceso adecuados para cada perfil o tipo de usuario. **2.-** Tener un mínimo de administradores o usuarios con altos privilegios en el sistema.		
Conocimientos requeridos:	Administración de bases de datos. Consulta y actualización de usuarios.		
Ejecución			**Fecha inicio**
Nombre y firma Administrador del sistema de información			**Fecha término**
Observaciones / anotaciones			

(Nombre del sistema A1)			Identificador único A1
Formato:	**3**	**Verificación anual**	**Acción concluida**
Medidas de seguridad técnicas:	**Artículo 18. I. g) Instalar y mantener vigentes certificados de comunicación segura SSL en el caso de servicios basados en Web.**		
Aplicable en:	I. Bases de datos y sistemas de tratamiento.		
Tiempo estimado:	Tres días hábiles.		
Importancia de la acción:	El instalar un certificado SSL en servidores web incrementa la seguridad al encriptar la transferencia de datos y la unicidad del sitio para los usuarios.		
Proceso recomendado:	**A)** En caso de no tener un certificado SSL vigente, enviar correo electrónico al Departamento de Firma Electrónica de DGTIC a firma.tic@unam.mx solicitando la asignación. **B)** El Departamento de Firma Electrónica Avanzada envía procedimiento para obtención de CSR del servidor, formato de la solicitud y costos de recuperación en función del tipo de certificado requerido (organizacional, comodín o corporativo). **C)** Completar documentación, proceso y pago de costo de recuperación. Enviar comprobantes a firma.tic@unam.mx. **D)** Al recibir el certificado SSL, instalarlo en el servidor de acuerdo con las instrucciones recibidas junto con el certificado.		
Mejores prácticas, referencias:	**1.-** Los certificados SSL deben tener una vigencia de al menos un año. **2.-** En caso de tener varios sistemas de información bajo un mismo dominio, se recomienda obtener un certificado SSL del tipo comodín (*wildcard*). **3.-** Se debe realizar el proceso de renovación del certificado al menos 10 días hábiles antes de su vencimiento.		
Conocimientos requeridos:	Administración de sistema operativo. Administración de servicios Web.		

Ejecución	**Fecha inicio**
Nombre y firma Administrador del sistema de información o servidor	**Fecha término**
Observaciones / anotaciones	

(Nombre del sistema A1)			Identificador único A1
Formato:	**4**	**Verificación anual**	**Acción concluida**
Medidas de seguridad técnicas:	**Artículo 18. I. h) Definir el plan de respaldos de la información, incluyendo periodicidad y alcance.**		
Aplicable en:	I. Bases de datos y sistemas de tratamiento.		
Tiempo estimado:	Dos días hábiles.		
Importancia de la acción:	En todo sistema de información es indispensable contar con un plan de respaldos periódicos, y especialmente en aquellos que contienen datos personales.		
Proceso recomendado:	**A)** Elaborar documento con la secuencia de respaldos al menos con el siguiente orden: - Diario – incremental. - Semanal – incremental. - Mensual – total. **B)** Establecer en el plan los medios para resguardo del respaldo y su forma de identificación: - En línea: mismo equipo donde se ejecuta el sistema. - Respaldo como servicio: otro equipo de almacenamiento. - Fuera de línea: medios magnéticos (cintas, discos) y/u ópticos. **C)** Incluir en el plan: - Responsables de cada tipo y medio de respaldo. - Rotación de respaldos y medios. - Áreas de resguardo. - Métodos de cifrado. - RTO: *Recovery Time Objective*. Tiempo objetivo de recuperación. - RPO: *Recovery Point Objective*: Punto objetivo de recuperación. **D)** Concluir este documento, adjuntarlo a SGPDP, llenar y firmar formato.		
Mejores prácticas, referencias:	**1.-** Se deben tener al menos 3 respaldos del sistema y sus bases de datos en distintos medios.		
Conocimientos requeridos:	Administración de sistema operativo. Gestión y programación de respaldos.		

Ejecución	Fecha inicio
Nombre y firma Administrador del sistema de información o servidor	**Fecha término**
Observaciones / anotaciones	

(Nombre del sistema A1)			Identificador único A1
Formato:	**5**	**Verificación anual**	**Acción concluida**
Medidas de seguridad técnicas:	**Artículo 18. I. i) Definir el procedimiento para el borrado seguro.**		
Aplicable en:	I. Bases de datos y sistemas de tratamiento.		
Tiempo estimado:	Un día hábil.		
Importancia de la acción:	Al igual que el procedimiento de respaldo, el borrado seguro de la información debe estar definido en cualquier sistema de información.		
Proceso recomendado:	**A)** Elaborar documento con el procedimiento y la herramienta para borrado seguro en función del tipo de base de datos para registros, tablas y base de datos. **B)** Incluir en el documento de borrado seguro el proceso de verificación de la no existencia del dato, generalmente por medio de consultas y de copias de respaldo. **C)** El borrado seguro debe incluirse en los respaldos incrementales y totales y en cualquiera de los medios de respaldo, así como máquinas virtuales o contenedores. **D)** Concluir este documento, adjuntarlo a SGPDP, llenar y firmar formato.		
Mejores prácticas, referencias:	**1.-** Para el caso de baja de equipo, se debe llenar el formato con la declaración de borrado seguro del Patronato Universitario, disponible en: http://www.patrimonio.unam.mx/patrimonio/descargas/formato_responsiva_borrado_datos.pdf **2.-** Se recomienda utilizar herramientas de borrado seguro por medio de sobre escritura aleatoria, llenado de ceros (0x00), llenado de unos o protocolos de borrado del estándar *DOD-5220.22-M*.		
Conocimientos requeridos:	Administración de sistema operativo. Comandos de borrado.		
Ejecución			**Fecha inicio**
Nombre y firma Administrador del sistema de información o servidor			**Fecha término**
Observaciones / anotaciones			

(Nombre del sistema A1)			Identificador único A1
Formato:	**6**	**Verificación anual**	**Acción concluida**
Medidas de seguridad técnicas:	**Artículo 18. II. a) Sincronizar la fecha y hora con el servidor NTP (Network Time Protocol) oficial de la UNAM**		
Aplicable en:	II. Sistemas operativos y servicios.		
Tiempo estimado:	Un día hábil.		
Importancia de la acción:	A fin de poseer información consistente, los sistemas de información deben estar sincronizados con una instancia central de tiempo, en este caso el servidor NTP de la UNAM.		
Proceso recomendado:	**A)** Realizar la verificación y configuración con privilegio de administrador del sistema operativo. **B)** En función del sistema operativo, acceder a la configuración de servidor de tiempo (NTP) en interfaz gráfica o por medio de línea de comandos. *Por ejemplo*, en el caso del sistema operativo Linux: - Verificar la existencia del archivo */etc/ntp.conf* - Editar el archivo *ntp.conf* incluyendo en la primera línea: *server ntpdgtic.redunam.unam.mx* ***ó*** *server 132.247.169.17* - Reiniciar el demonio del cliente NTP con el comando *sudo service ntp reload.* **C)** En caso de no tener el cliente NTP instalado, descargarlo del repositorio de aplicaciones del sistema operativo, instalarlo y regresar al punto B. **D)** Llenar y firmar formato.		
Mejores prácticas, referencias:	**1.-** Los servidores virtuales y contenedores hospedados en el Centro de Datos en DGTIC son configurados de origen con sincronización al servidor NTP de la UNAM. **2.-** No se deben usar otros servidores de NTP distintos al de UNAM.		
Conocimientos requeridos:	Administración de sistema operativo.		

Ejecución	Fecha inicio
Nombre y firma Administrador del sistema de información o servidor	**Fecha término**
Observaciones / anotaciones	

(Nombre del sistema A1)			Identificador único A1
Formato:	**7**	**Verificación anual**	**Acción concluida**
Medidas de seguridad técnicas:	**Artículo 18. II. b) Instalar y mantener actualizado el software antimalware.**		
Aplicable en:	II. Sistemas operativos y servicios.		
Tiempo estimado:	Dos días hábiles.		
Importancia de la acción:	El servidor que hospede el sistema de información debe tener protecciones instaladas para mitigar la inserción de *malware* (*rootkits, backdoors o* códigos maliciosos) que pueda alterar su operación o la integridad y seguridad de los datos.		
Proceso recomendado:	**A)** En función del sistema operativo, instalar uno o varios programas para la contención de malware. *Por ejemplo*, para el caso del sistema operativo Linux existen herramientas de código abierto y uso libre como *chkrootkit, rootkit hunter, bothunter, clamAV, avast*, entre otros, que se pueden instalar desde el repositorio correspondiente a la distribución de Linux en uso. **B)** Disponer de comandos para la localización de amenazas. *Por ejemplo*, para el caso de Linux, se recomienda usar el comando *grep* para la detección de cadenas regulares de texto en las invocaciones al *shell*. **C)** Una vez instalada la solución, verificar periódicamente su actualización **D)** Llenar y firmar formato.		
Mejores prácticas, referencias:	**1.-** UNAM-CERT puede asesorar en la selección de las herramientas *anti malware* más adecuadas para el servidor donde se aloje el sistema de información. Contactar al correo seguridad.tic@unam.mx.		
Conocimientos requeridos:	Administración de sistema operativo. Instalación de aplicaciones.		

Ejecución	**Fecha inicio**
Nombre y firma Administrador del sistema de información o servidor	**Fecha término**
Observaciones / anotaciones	

(Nombre del sistema A1)		Identificador único A1	
Formato:	**8**	**Verificación anual**	**Acción concluida**
Medidas de seguridad técnicas:	**Artículo 18. II. c) Instalar las actualizaciones de seguridad más recientes disponibles.**		
Aplicable en:	II. Sistemas operativos y servicios.		
Tiempo estimado:	Cuatro días hábiles.		
Importancia de la acción:	El servidor que hospede el sistema de información debe tener vigentes todas las actualizaciones de seguridad proporcionadas por el fabricante o desarrollador del sistema operativo.		
Proceso recomendado:	**A)** En función del sistema operativo, se debe revisar la vigencia y actualización de las herramientas de seguridad de la información. *Por ejemplo*, en el sistema operativo Linux ejecutar *apt-get update* para obtener la lista de actualizaciones, especialmente en el repositorio *security* de la respectiva distribución. **B)** Realizar un respaldo del sistema para garantizar retorno a versión anterior en caso de incompatibilidad con alguna aplicación de las actualizaciones de seguridad. **C)** Instalar las actualizaciones en el sistema operativo. **D)** Llenar y firmar formato.		
Mejores prácticas, referencias:	**1.-** Debe verificarse la actualización de seguridad del sistema operativo al menos una vez a la semana y configurar la actualización o notificación inmediata en caso de complementos de seguridad urgentes.		
Conocimientos requeridos:	Administración de sistema operativo. Instalación de aplicaciones.		
Ejecución		**Fecha inicio**	
Nombre y firma Administrador del sistema de información o servidor		**Fecha término**	
Observaciones / anotaciones			

(Nombre del sistema A1)			Identificador único A1
Formato:	**9**	**Verificación anual**	**Acción concluida**
Medidas de seguridad técnicas:	**Artículo 19. I. a) Aplicar un mecanismo de autenticación para las personas autorizadas con base en el principio del menor privilegio.**		
Aplicable en:	I. Bases de datos y sistemas de tratamiento.		
Tiempo estimado:	Cuatro días hábiles.		
Importancia de la acción:	Partiendo de la asignación o niveles de acceso a la información con el principio del menor privilegio, debe haber en operación en el sistema al menos un mecanismo para la validación de los usuarios autorizados.		
Proceso recomendado:	**A)** Verificar el tipo de control de acceso al sistema, esto es: a través de contraseñas, claves, identificadores, nombres de usuario, nombres de dominio, entre otros. Según sea aplicable al sistema de información en lo particular. En caso de no tener un control de acceso establecer al menos uno como: usuarios de sistema operativo, cuenta y contraseña de sistema. **B)** Revisar que los privilegios de acceso sean los adecuados en función del rol del usuario. *Por ejemplo:* el usuario de conexión a la base de datos no debe estar asignado a alguna cuenta del personal que tiene acceso al sistema. **D)** Llenar y firmar formato.		
Mejores prácticas, referencias:	**1.-** Se recomienda usar un esquema estándar de acceso a sistemas que están vinculados, por ejemplo: por medio de Directorio Activo (*Active Directory*), *LDAP* u *OpenAIM.* **2.-** Las contraseñas deben ser de 12 caracteres o más con uso de signos, letras mayúsculas y minúsculas y números.		
Conocimientos requeridos:	Administración de bases de datos. Consulta y actualización de usuarios.		
Ejecución			**Fecha inicio**
Nombre y firma Administrador del sistema de información o servidor			**Fecha término**
Observaciones / anotaciones			

(Nombre del sistema A1)		Identificador único A1	
Formato:	**10**	**Verificación anual**	**Acción concluida**
Medida de seguridad técnica:	**Artículo 19. II. b) Evitar la instalación de cualquier elemento de software que implique algún riesgo para el tratamiento de datos personales.**		
Aplicable en:	II. Sistemas operativos.		
Tiempo estimado:	Dos días hábiles.		
Importancia de la acción:	Por la relevancia de los sistemas de información con datos personales se debe minimizar o erradicar el riesgo de seguridad que implica instalar aplicaciones no verificadas.		
Proceso recomendado:	**A)** Dependiendo del sistema operativo, configurar las actualizaciones solamente para versiones maduras o revisiones certificadas de las aplicaciones. *Por ejemplo*: en sistemas Linux desactivar la instalación de versiones *beta, test, debug, non-official.* **B)** De la lista de software instalado, verificar el consumo de recursos de aplicaciones *TSR (Terminal and Stay Resident)*. Identificar demonios que ocupen excesiva RAM o tiempo de ejecución en el procesador. *Por ejemplo*: En sistemas Windows usar el Administrador de Tareas para identificar programas de alto consumo. **C)** Desinstalar toda aquella aplicación, librería, programa, paquetería o servicio que no sea estrictamente necesario para la operación del sistema. *Por ejemplo*, si el servidor Linux no proporcionará direcciones IP, el demonio o servicio *dchpd* no debe estar instalado. **D)** Llenar y firmar formato.		
Mejores prácticas, referencias:	**1.-** En ningún caso puede instalarse software de procedencia desconocida. Se debe impedir a los usuarios en sus privilegios de acceso instalar software o inyectar código a la aplicación del sistema de información. y se debe realizar un control estricto de los puertos de comunicación (USB, Red, etc) para evitar la extracción no autorizada de datos.		
Conocimientos requeridos:	Administración de sistema operativo. Instalación de aplicaciones.		

Ejecución	Fecha inicio
Nombre y firma Administrador del sistema de información o servidor	**Fecha término**
Observaciones / anotaciones	

(Nombre del sistema A1)		Identificador único A1	
Formato:	**11**	**Verificación anual**	**Acción concluida**
Medidas de seguridad técnicas:	**Artículo 19. III. a) Establecer las medidas físicas de seguridad que controlen el acceso a los equipos.**		
Aplicable en:	III. Equipo de cómputo.		
Tiempo estimado:	Dos días hábiles.		
Importancia de la acción:	Además de las protecciones de tipo lógico, deben implementarse medidas de seguridad para reducir el riesgo al sistema de información por accesos físicos no autorizados.		
Proceso recomendado:	**A)** Identificar las medidas físicas que restrinjan el acceso físico a equipos, tales como chapas, puertas, biométricos. **B)** En función de la ubicación del equipo de cómputo, hacer una relación de las condiciones más adecuadas para su protección que aún sean necesarias implementar. **C)** Establecer y seguir un plan de mejoramiento de la protección física de equipos. *Por ejemplo*; cámaras de videovigilancia, bitácoras, vigilantes, cuartos cerrados, racks con puerta y chapa, candados en equipos, bloqueo o desconexión física de puertos USB, alarmas y sensores, según sea lo más conveniente como mínimo para la protección de los datos. **D)** Llenar y firmar formato.		
Mejores prácticas, referencias:	**1.-** Las medidas físicas de seguridad deben revisarse regularmente y formar parte de plan de continuidad de operaciones, así como ser del conocimiento de la Comisión local de seguridad.		
Conocimientos requeridos:	Administración de bases de datos. Consulta y actualización de usuarios.		

Ejecución	Fecha inicio
Nombre y firma Administrador del sistema de información o servidor	**Fecha término**
Observaciones / anotaciones	

(Nombre del sistema A1)			Identificador único A1
Formato:	**1** **2**	**Verificación anual**	**Acción concluida**
Medidas de seguridad técnicas:	**Artículo 19. III. b) Restringir la salida de equipos de las instalaciones de cada área universitaria.**		
Aplicable en:	III. Equipo de cómputo.		
Tiempo estimado:	Un día hábil.		
Importancia de la acción:	Se debe tener un mecanismo de control para la entrada y salida de equipos de cómputo y eliminar extracciones no autorizadas.		
Proceso recomendado:	**A)** Diseñar una bitácora o formato para el registro de entrada y salida de equipos de cómputo y periféricos asociados como discos duros, cintas, unidades *flash*, discos ópticos, monitores, teclados, ratones y en lo general todo componente de un equipo. **B)** La bitácora de entrada y salida debe incluir el registro de número de serie e inventario UNAM. responsable de ingreso o egreso del componente y firma autorizada del responsable del área. **C)** Incluir en el procedimiento la revisión periódica (al menos una vez al mes) de la consistencia del inventario registrado contra la bitácora de entrada y salida. **D)** Llenar y firmar formato.		
Mejores prácticas, referencias:	**1.-** Se recomienda usar un formato estándar de control de entrada y salida de bienes proporcionado por las áreas administrativas de las entidades y dependencias y conservar una copia en el área responsable del equipo de cómputo. **2.-** En la bitácora se debe incluir la razón de la entrada o salida del equipo. En el caso de baja, se deberá firmar la declaración de borrado seguro de Patrimonio Universitario.		
Conocimientos requeridos:	Gestión de Tecnología de información, control de entrada y salida de equipo y materiales.		

Ejecución	**Fecha inicio**
Nombre y firma Administrador del sistema de información o servidor	**Fecha término**
Observaciones / anotaciones	

(Nombre del sistema A1)		Identificador único A1	
Formato:	**13**	**Verificación anual**	**Acción concluida**
Medidas de seguridad técnicas:	**Artículo 19. IV. a) Realizar la transmisión de datos personales a través de un canal cifrado.**		
Aplicable en:	IV. Red de datos.		
Tiempo estimado:	Tres días hábiles.		
Importancia de la acción:	La comunicación del sistema de información con otros sistemas o servicios, así como el acceso de administración para ejecución de procesos por comandos, debe estar encriptada para evitar el envío o recepción de datos susceptibles de ser interceptados en tránsito.		
Proceso recomendado:	**A)** Identificar, mediante el administrador de aplicaciones que corresponda al sistema operativo, los protocolos y aplicaciones instalados para comunicación cifrada. *Por ejemplo*: *SFTP (Secure File Transfer Protocol), SSH (Secure Shell), SCP (Secure Copy*). **B)** Instalar con el administrador de aplicaciones o comando similar los protocolos de comunicación cifrada que sean necesarios para el tipo de transacciones y accesos del sistema. *Por ejemplo*, en el caso de requerir ejecutar comandos de forma remota en un servidor Linux, instalarlo con el comando *apt-get install openssh-server.* **C)** Activar los protocolos de comunicación encriptada en el servidor. *Por ejemplo*: en Linux con el comando *sudo systemctl enable ssh*. **D)** Llenar y firmar formato.		
Mejores prácticas, referencias:	**1.-** Se deben mantener actualizados los protocolos de comunicación por canal cifrado al igual que las utilerías de seguridad. 2.- El protocolo de comunicación cifrada requiere puertos específicos TCP, los cuales deberán estar permitidos en la configuración del equipo activo de red.		
Conocimientos requeridos:	Administración de sistema operativo. Instalación de aplicaciones. Administración de red.		

Ejecución	**Fecha inicio**
Nombre y firma Administrador del sistema de información o servidor	**Fecha término**
Observaciones / anotaciones	

(Nombre del sistema A1)		Identificador único A1	
Formato:	**14**	**Verificación anual**	**Acción concluida**
Medidas de seguridad técnicas:	**Artículo 20. Aplicar el procedimiento de borrado seguro que impida la recuperación en las bases de datos y todos sus respaldos.**		
Aplicable en:	Bases de datos y sistemas de tratamiento.		
Tiempo estimado:	Tres días hábiles.		
Importancia de la acción:	Se debe verificar que el procedimiento de borrado seguro es funcional y que el dato no persiste en función del tipo de borrado (registro, tabla, base, sistema).		
Proceso recomendado:	**A)** Realizar una copia integral del sistema de información y colocarla en un servicio temporal. *Por ejemplo:* máquina virtual directorio temporal en el servidor. **B)** Ingresar a la copia del sistema de información y realizar el borrado de un registro. Verificar que el dato no persiste en la base de datos por medio de forma de consulta o comando. **C)** Realizar el mismo proceso del punto B para una tabla y finalmente para la base de datos completa. D) En caso de persistencia del dato, instalar y ejecutar herramientas para borrado seguro. *Por ejemplo*: en Linux se dispone *de shred, wipe, secure-delete, srm, sfill, sswap, sdmem,* que se pueden instalar desde el administrador de aplicaciones. **D)** Llenar y firmar este formato.		
Mejores prácticas, referencias:	**1.-** Se recomienda usar al menos un comando a nivel de sistema operativo para el borrado seguro de conformidad con el procedimiento establecido.		
Conocimientos requeridos:	Administración de sistema operativo. Instalación de aplicaciones. Gestión de archivos.		

Ejecución	Fecha inicio
Nombre y firma Administrador del sistema de información o servidor	**Fecha término**
Observaciones / anotaciones	

(Nombre del sistema A1)		Identificador único A1	
Formato:	**15**	**Verificación anual**	**Acción concluida**
Medidas de seguridad técnicas	**Artículo 18. I. a) Utilizar los datos personales preexistentes que estén disponibles, de acuerdo con sus respectivas políticas de uso y acceso en bases de datos a cargo de otras áreas universitarias.**		
Aplicable en:	I. Bases de datos y sistemas de tratamiento.		
Tiempo estimado:	Hito.		
Importancia de la acción:	Optimizar y consolidar el uso y la protección de datos personales al hacer referencia a instancias universitarias que sean las principales responsables de su obtención, resguardo y protección.		
Proceso recomendado:	**A)** Disponer del inventario de datos del sistema de información, esto es: documento con la descripción de tablas, campos, tipo de datos, relaciones y consultas. **B)** Con la Área Universitaria que esté identificada como la instancia autoritativa en materia de datos personales, comparar el inventario de datos. *Por ejemplo*: La Dirección General de Administración Escolar es la dependencia autoritativa en materia de datos personales de estudiantes. **C)** Establecer el acuerdo por escrito para el uso de campos específicos de datos personales de la instancia autoritativa. **D)** Establecer el mecanismo de comunicación entre el sistema de información y el de la instancia autoritativa. *Por ejemplo*: *Webservices*, transferencia *SFTP.* **E)** Llenar y firmar formato.		
Mejores prácticas, referencias:	**1.-** El hacer referencia a instancias a cargo de la obtención de los datos personales y su protección se garantiza la homogeneidad de la información.		
Conocimientos requeridos:	Administración de sistema de información. Gestión de bases de datos.		
Ejecución		**Fecha inicio**	
Nombre y firma Administrador del sistema de información o servidor		**Fecha término**	
Observaciones / anotaciones			

(Nombre del sistema A1)		Identificador único A1	
Formato:	**16**	**Verificación anual**	**Acción concluida**
Medidas de seguridad técnicas:	**Artículo 18. I. d) Permitir el acceso al código fuente de los sistemas exclusivamente a la administración del sistema y personal para el desarrollo.**		
Aplicable en:	I. Bases de datos y sistemas de tratamiento.		
Tiempo estimado:	Ocho días hábiles.		
Importancia de la acción:	Evitar el uso de códigos originales de los sistemas de información que posteriormente implique un riesgo a la seguridad de estos.		
Proceso recomendado:	**A)** Recopilar el código fuente y documentación del sistema de información en todas sus versiones disponibles. **B)** Depositar en un equipo central de desarrollo todas las versiones de código fuente y su documentación (inventario de datos, manual de administración, manual de programador). **C)** Establecer control de acceso por usuario y contraseña hacia el equipo central de desarrollo **D)** Activar bitácoras de acceso (*log*) hacia el equipo central de desarrollo. **E)** Proporcionar las credenciales de acceso al equipo central de desarrollo exclusivamente al personal a cargo de programación y mantenimiento de código y manuales. **F)** Llenar y firmar formato.		
Mejores prácticas, referencias:	**1.-** Se debe documentar todo el proceso de desarrollo y actualización de un sistema de información.		
Conocimientos requeridos:	Administración de sistema de información. Gestión de bases de datos.		

Ejecución	**Fecha inicio**
Nombre y firma Administrador del sistema de información o servidor	**Fecha término**
Observaciones / anotaciones	

(Nombre del sistema A1)		Identificador único A1	
Formato:	**17**	**Verificación anual**	**Acción concluida**
Medidas de seguridad técnicas:	**Artículo 19. I. b) Establecer las medidas de seguridad en los periodos de inactividad o mantenimiento.**		
Aplicable en:	I. Bases de datos y sistemas de tratamiento.		
Tiempo estimado:	Cuatro días hábiles.		
Importancia de la acción:	Garantizar la continuidad de la operación y disponibilidad de los sistemas de información especialmente durante períodos vacacionales, contingencias o ciclos de mantenimiento.		
Proceso recomendado:	**A)** Elaborar documento con las medidas necesarias de seguridad para períodos vacacionales, contingencias y ventanas de mantenimiento, incluyendo: control de acceso físico y lógico a los equipos, ejecución de respaldos, sistemas de alta disponibilidad (redundancia). **B)** Incluir en el documento la descripción de los procedimientos en caso de contingencia por falla de servicio de red, falla de equipo de cómputo, falla lógica en sistema operativo. **C)** Incluir en el documento el directorio de responsables de cada uno de los puntos a atender: apagado seguro, apagado fortuito, apagado programado, verificación de integridad de información, activación de servicios locales o de respaldo. **D)** Llenar y firmar formato.		
Mejores prácticas, referencias:	**1.-** Las medidas de seguridad durante períodos de mantenimiento deben formar parte de un plan de continuidad de operaciones y de recuperación ante desastres (**DRP**).		
Conocimientos requeridos:	Administración de sistema de información. Administración de sistema operativo.		
Ejecución		**Fecha inicio**	
Nombre y firma Administrador del sistema de información o servidor		**Fecha término**	
Observaciones / anotaciones			

(Nombre del sistema A1)		Identificador único A1	
Formato:	**18**	**Verificación anual**	**Acción concluida**
Medidas de seguridad técnica:	**Artículo 19. I. c) Generar respaldos y aplicar los mecanismos de control y protección para su resguardo.**		
Aplicable en:	I. Bases de datos y sistemas de tratamiento.		
Tiempo estimado:	Ocho días hábiles.		
Importancia de la acción:	Verificar que el plan de respaldos opera adecuadamente para su utilización en caso de contingencia.		
Proceso recomendado:	**A)** De acuerdo con el plan de respaldos establecido, ejecutar la secuencia de respaldos. **B)** Designar responsables de respaldos y responsables de verificación de respaldos. **C)** Completar bitácora de control de los respaldos, indicando fecha, hora, tipo de respaldo (integral, total, parcial de registros), ejecutor y revisor del respaldo, ubicación del respaldo, medio y etiqueta. **D)** Llenar y firmar formato.		
Mejores prácticas, referencias:	**1.-** La generación de respaldos, su control y protección deben formar parte de un plan de continuidad de operaciones y de recuperación ante desastres (**DRP**).		
Conocimientos requeridos:	Administración de sistema de información. Administración de sistema operativo.		
Ejecución		**Fecha inicio**	
Nombre y firma Administrador del sistema de información o servidor		**Fecha término**	
Observaciones / anotaciones			

(Nombre del sistema A1)			Identificador único A1
Formato:	**19**	**Verificación anual**	**Acción concluida**
Medidas de seguridad técnicas:	**Artículo 19. I. d) Impedir el uso de cuentas y servicios gestionados por personas físicas para el tratamiento de los datos personales.**		
Aplicable en:	I. Bases de datos y sistemas de tratamiento.		
Tiempo estimado:	Veinte días hábiles.		
Importancia de la acción:	Debe evitarse el riesgo que implica el depender de cuentas de control personal para acceder a servicios, fuentes de información o cualquier elemento del sistema de información que ponga en riesgo su estabilidad y confiabilidad.		
Proceso recomendado:	**A)** Realizar revisión integral del sistema de información en materia de accesos, cuentas y servicios. *Por ejemplo*: En caso de consultar vía un *Webservice* a un sistema autoritativo de datos personales en la DGAE, identificar la cuenta de acceso a ese sistema. **B)** Determinar si las cuentas de acceso a servicios locales o remotos están bajo el control de la administración del sistema. *Por ejemplo*: Si la cuenta de acceso a un *Webservice* – su usuario y contraseña – está bajo el control del administrador del sistema, o si un respaldo que se realiza en un equipo remoto es con una cuenta y contraseña controlada por el administrador del sistema. **C)** Si las cuentas de acceso a servicios locales o remotos pertenecen a personas del Área Universitaria, cambiarlas por cuentas institucionales dentro del control de la instancia universitaria. *Por ejemplo*: si la identificación para acceder a un respaldo remoto es del tipo xxx@google.com, deberá cambiarse por una cuenta del tipo xxxx@unam.mx **D)** Llenar y firmar formato.		
Mejores prácticas, referencias:	**1.-** Nunca deben usarse cuentas, servicios, suscripciones, licencias o cualquier otro elemento informático cuyo control dependa de una sola persona.		
Conocimientos requeridos:	Administración de sistema de información. Gestión de bases de datos.		
Ejecución			**Fecha inicio**
Nombre y firma Administrador del sistema de información o servidor			**Fecha término**
Observaciones / anotaciones			

(Nombre del sistema A1)			Identificador único A1
Formato:	**20**	**Verificación anual**	**Acción concluida**

Medidas de seguridad técnicas:	**Artículo 19. II. a) Proteger ante manipulaciones indebidas y accesos no autorizados las bitácoras y los dispositivos donde se almacenan.**
Aplicable en:	II. Sistemas operativos.
Tiempo estimado:	Cuatro días hábiles.
Importancia de la acción:	Las bitácoras son un elemento esencial para determinar acciones que atentan contra la estabilidad del sistema de información y la protección de los datos personales.
Proceso recomendado:	**A)** Elaborar una lista de las bitácoras relacionadas con el sistema de información, tanto en medio digital como físico. *Por ejemplo*: En el equipo de cómputo las bitácoras de acceso de usuarios al sistema operativo y al sistema de información (*logs*), de forma física las bitácoras de acceso al área donde está el equipo de cómputo. **B)** Junto a la lista elaborar el cronograma de revisión de integridad y respaldo de las bitácoras. *Por ejemplo*: diario, semanal, mensual. **C)** Establecer en el documento el procedimiento de resguardo de las bitácoras. *Por ejemplo*: respaldo y protección de *logs* en el caso de equipo de cómputo o zonas seguras de almacenamiento de bitácoras en papel, digitalización de registros. **D)** Llenar y firmar formato.
Mejores prácticas, referencias:	**1.-** Las bitácoras digitales y en papel deben resguardarse preferentemente en una zona independiente de la ubicación del sistema de información.
Conocimientos requeridos:	Administración de sistema de información. Administración de sistema operativo.

Ejecución	**Fecha inicio**
Nombre y firma Administrador del sistema de información o servidor	**Fecha término**
Observaciones / anotaciones	

(Nombre del sistema A1)			Identificador único A1
Formato:	**21**	**Verificación anual**	**Acción concluida**
Norma Complementaria Técnica	**Artículo 19. IV. b) Supervisar los controles de seguridad en la red de datos donde opere el sistema para tratamiento de datos personales.**		
Aplicable en:	IV. Red de datos.		
Tiempo estimado:	Cuatro días hábiles.		
Importancia de la acción:	El control de seguridad de los equipos activos de red que suministran la conectividad al sistema de información es un elemento básico para la protección de los datos.		
Proceso recomendado:	**A)** Identificar los equipos activos de red que permiten la conexión del equipo de cómputo con el sistema de información, incluyendo marca, modelo, versión de software, vigencia de mantenimiento y capacidades de protección de las comunicaciones. **B)** Determinar las reglas de seguridad físicas (acceso restringido, cuartos de telecomunicaciones) y lógicas (cuentas de acceso, puertos activos, protocolos activos) para el equipo de red. **C)** Incluir en las acciones para aseguramiento de la red de datos aquellas que sean necesarias en función de los controles actuales. Definir un plan de regularización de la seguridad en caso de ser aplicable. **D)** Mantener actualizados los equipos activos de red y con un programa de mantenimiento. **E)** Identificar y en su caso programar la instalación de equipo para seguridad perimetral de la red de datos. **D)** Llenar y firmar formato.		
Mejores prácticas, referencias:	**1.-** Las ubicaciones físicas de los equipos activos de red deben estar protegidas con cerraduras y controles de acceso, cumplir las normas de operación y no emplearse para ningún otro equipo o uso.		
Conocimientos requeridos:	Administración de redes de datos.		
Ejecución			**Fecha inicio**
Nombre y firma Administrador del sistema de información o servidor			**Fecha término**
Observaciones / anotaciones			

(Nombre del sistema A1)			Identificador único A1
Formato:	**22**	**Verificación anual**	**Acción concluida**

Medidas de seguridad técnicas:	**Artículo 19. IV. c) Proporcionar exclusivamente el acceso desde redes y servicios autorizados.**
Aplicable en:	IV. Red de datos.
Tiempo estimado:	Cuatro días hábiles.
Importancia de la acción:	Es necesario reducir el mínimo necesario los puertos de comunicación para el funcionamiento del sistema de información.
Proceso recomendado:	**A)** Revisar los puertos de comunicación (*TCP y UDP*) que requiera el sistema de información para su operación. *Por ejemplo*: para servicios *Web* los puertos 80 y 8080 son los convencionales. **B)** Activar en el sistema operativo la herramienta correspondiente para el control de puertos de comunicación. *Por ejemplo*, en Linux puede tratarse de un *firewall* a nivel de software o las herramientas que para tal efecto contenga la distribución correspondiente del sistema operativo. **C)** Dejar activos solamente los puertos necesarios para la operación del sistema. **D)** Activar el filtrado de la comunicación por direccionamiento IP en caso de ser posible para la operación del sistema. *Por ejemplo*: Permitir el acceso al puerto de *SSH* solamente a direcciones IP en una subred de la UNAM (132.248.x.y) o a un grupo de direcciones IP específicas. **E)** Llenar y firmar formato.
Mejores prácticas, referencias:	**1.-** No se deben tener activos accesos que no son necesarios vía la red de datos.
Conocimientos requeridos:	Administración de sistema de información. Administración de sistema operativo.

Ejecución	Fecha inicio
Nombre y firma Administrador del sistema de información o servidor	**Fecha término**
Observaciones / anotaciones	

(Nombre del sistema A1)			Identificador único A1
Formato:	**23**	**Verificación anual**	**Acción concluida**

Medidas de seguridad técnicas:	**Artículo 18. I. b) Contar con entornos para desarrollo, pruebas y operación.**
Aplicable en:	I. Bases de datos y sistemas de tratamiento.
Tiempo estimado:	Veinte días hábiles.
Importancia de la acción:	Para evitar riesgos innecesarios a la información, el desarrollo y actualización de los mismos deberá ser realizado siempre en una plataforma y ambientes por separado.
Proceso recomendado:	**A)** Instalar y configurar equipos similares en características, preferentemente virtuales, a los equipos donde se instalará el sistema de información en su nueva o actualizada versión. **B)** Crear un repositorio en un equipo central de desarrollo para el resguardo de códigos, documentación, inventarios de datos y manuales de usuario, administrador y programador. **C)** Ejecutar las pruebas de nuevas versiones o actualizaciones del sistema de información en el equipo dispuesto para tal efecto. Nunca usar - equipos físicos o virtuales con el sistema actualmente en producción como las plataformas para evaluación de versiones en desarrollo. **D)** Llenar y firmar formato.
Mejores prácticas, referencias:	**1.-** Se deben realizar respaldos de la información en los sistemas en desarrollo del mismo modo que como se realicen con el sistema en producción.
Conocimientos requeridos:	Administración de sistema de información. Desarrollo de aplicaciones.

Ejecución	**Fecha inicio**
Nombre y firma Administrador del sistema de información o servidor	**Fecha término**
Observaciones / anotaciones	

(Nombre del sistema A1)			Identificador único A1
Formato:	**24**	**Verificación anual**	**Acción concluida**
Medidas de seguridad técnicas:	**Artículo 18. I. f) Cumplir con las especificaciones de seguridad informática previo a la puesta en operación.**		
Aplicable en:	I. Bases de datos y sistemas de tratamiento.		
Tiempo estimado:	Veinte días hábiles.		
Importancia de la acción:	Solo los sistemas de información revisados integralmente en su seguridad y estabilidad pueden ser publicados bajo el dominio .unam.mx .		
Proceso recomendado:	**A)** Una vez concluido el desarrollo o actualización de un sistema de información, solicitar al área de seguridad del Área Universitaria la revisión de seguridad informática del sistema, lo que incluye: pruebas de penetración, pruebas de estabilidad, pruebas de carga y endurecimiento de la seguridad. En caso de no contar con esa área, requerirlo a UNAM CERT al correo seguridad.tic@unam.mx . **B)** Una vez recibido el reporte del área de seguridad, aplicar las medidas de corrección que incluya el reporte. Regresar al punto A. **C)** Habiendo resuelto los hallazgos y sugerencias de mejora de la seguridad señalados por el área especializada, realizar la instalación del sistema en la plataforma definitiva de cómputo, extrayéndolo del entorno de desarrollo. **D)** Llenar y firmar formato.		
Mejores prácticas, referencias:	**1.-** El equipo de UNAM CERT puede asesorar a las entidades y dependencias en la aplicación de las medidas de corrección y mitigación a partir de los resultados de la revisión de seguridad.		
Conocimientos requeridos:	Administración de aplicaciones. Administración de sistema operativo.		
Ejecución			**Fecha inicio**
Nombre y firma Administrador del sistema de información o servidor			**Fecha término**
Observaciones / anotaciones			

(Nombre del sistema A1)			Identificador único A1
Formato:	**25**	**Verificación anual**	**Acción concluida**
Medidas de seguridad técnicas:	**Artículo 18. III. a) Utilizar equipos con componentes actualizados, protegidos con garantías y soporte, y con la capacidad suficiente para atender la demanda del servicio y de los usuarios.**		
Aplicable en:	III. Equipos de cómputo.		
Tiempo estimado:	Hito.		
Importancia de la acción:	Mantener en adecuada condición de operación el equipo de cómputo incrementa la estabilidad y seguridad del sistema de información.		
Proceso recomendado:	**A)** Elaborar una lista del inventario de los equipos de cómputo, periféricos y de almacenamiento necesarios para la ejecución del sistema de información. **B)** Determinar la razón por la que el sistema de información requerirá estar localizado en un equipo físico y no en un servidor virtual. Con ello justificar una adquisición o actualización. Por ejemplo: por incompatibilidad con hipervisores, necesidades de comunicación exclusivamente locales en la entidad y dependencia o el no necesitar de un entorno de alta disponibilidad automática. **C)** Identificar en el inventario versiones, introducción en el mercado, vida útil, contratos de mantenimiento y soporte para todos y cada uno de los componentes, en el caso de emplear equipo físico. **D)** Adquirir los componentes y elementos necesarios para la actualización, vigencia de soporte y capacidad para atención a los usuarios en el equipo de cómputo físico. **E)** Llenar y firmar formato.		
Mejores prácticas, referencias:	**1.-** El mantenimiento preventivo debe contar con medidas de verificación.		
Conocimientos requeridos:	Administración de infraestructura.		
Ejecución			**Fecha inicio**
Nombre y firma Administrador del sistema de información o servidor			**Fecha término**
Observaciones / anotaciones			

(Nombre del sistema A1)			Identificador único A1
Formato:	**26**	**Verificación anual**	**Acción concluida**
Medidas de seguridad técnicas:	**Artículo 18. III. b) Definir el programa de mantenimiento preventivo.**		
Aplicable en:	III. Equipos de cómputo.		
Tiempo estimado:	Hito.		
Importancia de la acción:	Garantizar que el plan de mantenimiento de equipo se realiza en tiempo y forma.		
Proceso recomendado:	**A)** De la lista de equipo de cómputo físico necesario para la operación del sistema de información, extraer las vigencias de mantenimiento. **B)** En caso de no estar en posibilidad de aplicar el mantenimiento preventivo por el personal del Área Universitaria, cotizar pólizas de mantenimiento de acuerdo con el tipo de componente, preferentemente una sola póliza para el conjunto del equipo físico. **C)** Adquirir las pólizas de mantenimiento preventivo y observar su vigencia. La vigencia no podrá ser menor de un año. **D)** Llenar y firmar formato.		
Mejores prácticas, referencias:	**1.-** El programa de mantenimiento debe considerar los costos de contratos, refacciones, partes, actualizaciones y reemplazos.		
Conocimientos requeridos:	Administración de infraestructura.		
Ejecución			**Fecha inicio**
Nombre y firma Administrador del sistema de información o servidor			**Fecha término**
Observaciones / anotaciones			

(Nombre del sistema A1)			Identificador único A1
Formato:	**27**	**Verificación anual**	**Acción concluida**
Medidas de seguridad técnicas:	**Artículo 19. III. c) Aplicar el programa de mantenimiento preventivo a los equipos.**		
Aplicable en:	III. Equipos de cómputo.		
Tiempo estimado:	Seis días hábiles.		
Importancia de la acción:	Garantizar que el plan de mantenimiento de equipo se realiza en tiempo y forma.		
Proceso recomendado:	**A)** En caso de que el personal del Área Universitaria pueda realizar el mantenimiento preventivo, definir el calendario de inactividad del sistema de información, notificar a los usuarios y aplicar el plan en caso de mantenimiento o inactividad. **B)** En caso de que sea a través de un proveedor que se proporcione el mantenimiento al equipo de cómputo, ejecutar el calendario de acciones preventivas en un período no superior a cada 3 meses hasta la conclusión del contrato o póliza respectivo. **C)** Llenar y firmar formato.		
Mejores prácticas, referencias:	**1.-** Debe actualizarse el equipo de cómputo de manera suficiente para continuar la operación del sistema y considerar en el mantenimiento preventivo sistemas paralelos de manera temporal hasta la conclusión de los trabajos.		
Conocimientos requeridos:	Administración de infraestructura.		

Ejecución	Fecha inicio
Nombre y firma Administrador del sistema de información o servidor	**Fecha término**
Observaciones / anotaciones	

(Nombre del sistema A1)			Identificador único A1
Formato:	**28**	**Verificación anual**	**Acción concluida**
Medidas de seguridad técnicas:	**Artículo 21. Solo se permitirá el uso de servicios de nube pública para el resguardo de archivos cifrados que contengan respaldos de la información.**		
Aplicable en:	Servicios en la nube pública.		
Tiempo estimado:	Hito.		
Importancia de la acción:	No pueden conservarse o usarse datos personales que sean tratados por la UNAM en servicios de nube pública. Estos servicios sólo se permiten para el respaldo de archivos cifrados, no en producción.		
Proceso recomendado:	**A)** Identificar los respaldos que se tengan resguardados en servicios de nube pública. **B)** Verificar el cifrado en cada uno de los respaldos que se almacenen en nube pública. El cifrado no deberá ser de menor capacidad al equivalente a AES de 128 bits.		
Mejores prácticas, referencias:	**1.-** La DGTIC proporciona el servicio de respaldos en el Centro de Datos, por lo que se sugiere utilizarlo en lugar de respaldos en la nube pública.		
Conocimientos requeridos:	Administración de respaldos. Administración de sistema operativo.		
Ejecución			**Fecha inicio**
Nombre y firma Administrador del sistema de información o servidor			**Fecha término**
Observaciones / anotaciones			


UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO
POR MI RAZA HABLARA EL ESPIRITU

UNAM

CANADÁ

1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

UNAM-Canadá	
Identificador único*	628.03
(Nombre del sistema A1) *	Servescol
Datos personales (sensibles o no) contenidos en el sistema*:	Nombres Apellidos Email Genero Fecha de nacimiento Teléfonos de contacto Dirección Contacto de emergencia Nivel de escolaridad Pasaporte Historial académico
Responsable*:	
Nombre*:	Constantino de Jesús Macías Garcia
Cargo*:	Director UNAM - Canadá
Funciones*:	Como responsable de la Dirección es el encargado del control general de los prosesos asociados a la sede.
Obligaciones*:	Promover y velar por el uso correcto de la información sin que exista riesgos asociados como la difusión, modificación o copias sin previa autorización.
	Encargados:
(Nombre del Encargado 1*)	Alex Méndez
Cargo*:	Delegado Administrativo
Funciones*:	Gestiona el correcto funcionamiento del sistema y garantiza el cumplimiento de las normas de seguridad asociadas al desarrollo del sistema
Obligaciones*:	Procurar la protección de los datos personales contenidos en el sistema mediante la implementación de estrategias y mecanismos de seguridad en su desarrollo y mantenimiento.
	Usuarios:
(Nombre del Usuario 1*)	Verónica Lomelí
Cargo*:	Jefa del departamento de registro y servicios estudiantiles
Funciones*:	Controlar los procesos de registro de estudiantes
Obligaciones*:	Establecer los procesos para la captación de información de los aspirantes y la captación de los historiales académicos
(Nombre del Usuario 2*)	Beatriz Olvera
Cargo*:	Asistente
Funciones*:	Realizar el registro de estudiantes del sistema
Obligaciones*:	Ingresar los datos en el sistema de acuerdo con los procedimientos.
(Nombre del Usuario 3*)	Isabelle Bellanger
Cargo*:	Asistente
Funciones*:	Realizar el registro de estudiantes del sistema
Obligaciones*:	Ingresar los datos en el sistema de acuerdo con los

	procedimientos.
Sistema (Nombre del A2)*:	ACOMBA Sistema contable
Datos personales contenidos en el sistema*:	Nombres Apellidos NAS (Número de identificación social) Email Genero Fecha de nacimiento Teléfonos de contacto Dirección
	Responsable:
Nombre*:	Constantino de Jesús Macías Garcia
Cargo*:	Director UNAM - Canadá
Funciones*:	Como responsable de la Dirección es el encargado del control general de los prosesos asociados a la sede.
Obligaciones*:	Promover y velar por el uso correcto de la información sin que exista riesgos asociados como la difusión, modificación o copias sin previa autorización.
	Encargados:
(Nombre del Encargado 1*)	Alex Méndez
Cargo*:	Delegado Administrativo
Funciones*:	Establece comunicación con el proveedor del sistema a fin de establecer los procedimientos requeridos para la operación del sistema.
Obligaciones*:	Establece las actividades requeridas para la elaboración de respaldos.
	Usuarios:
(Nombre del Usuario 1*)	Brenda Colín
Cargo*:	Jefe Contable
Funciones*:	Ingresar la información requerida para el desarrollo de las actividades contables
Obligaciones*:	Transmitir la información requerida a los entes gubernamentales. Mantener la privacidad de la información registrada.
(Nombre del Usuario 2*)	Cinthya Gamboa
Cargo*:	Jefe Contable
Funciones*:	Ingresar la información requerida para el desarrollo de las actividades contables
Obligaciones*:	Mantener la privacidad de la información registrada.
Sistema (Nombre del A3)*:	Formulario Web
Datos personales contenidos en el sistema*:	Nombres Apellidos Email Genero Fecha de nacimiento Teléfonos de contacto Curso de interes
	Responsable:

Nombre*:	Constantino de Jesús Macías Garcia
Cargo*:	Director UNAM - Canadá
Funciones*:	Como responsable de la Dirección es el encargado del control general de los prosesos asociados a la sede.
Obligaciones*:	Promover y velar por el uso correcto de la información sin que exista riesgos asociados como la difusión, modificación o copias sin previa autorización.
	Encargados:
(Nombre del Encargado 1*)	Alex Méndez
Cargo*:	Delegado Administrativo
Funciones*:	Usuario administrador
Obligaciones*:	Generar contraseñas Modificar el formulario
	Usuarios:
(Nombre del Usuario 1*)	Andres Castañeda
Cargo*:	Asistente
Funciones*:	Modificaciones al formulario
Obligaciones*:	Realizar las modificaciones solicitadas a los campos del formulario
(Nombre del Usuario 2*)	Anabel Ferrer
Cargo*:	Jefe Comunicaciones
Funciones*:	Acceso a la base de datos para procesos de mercadeo
Obligaciones*:	No difundir información de los datos personales No modificar la información almacenada en el servidor Hacer respaldos de la información de datos personales en Microsoft-Onedrive
(Nombre del Usuario 3*)	Verónica Lomelí
Cargo*:	Jefa del departamento de registro y servicios estudiantiles
Funciones*:	Acceso a la base de datos para procesos de contacto y seguimiento
Obligaciones*:	No difundir información de los datos personales No modificar la información almacenada en el servidor Hacer respaldos de la información de datos personales en Microsoft-Onedrive

2. ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

UNAM-Canadá	
Identificador único¨*	628.03
(Nombre del sistema A1*)	Servescol
Tipo de soporte:*	Electrónico
Descripción:*	Base de datos
Características del lugar donde se resguardan los soportes:*	Alojamiento de la base de datos en el servidor de DGTIC
(Nombre del sistema A2*)	ACOMBA
Tipo de soporte*:	Electónico
Descripción*:	Base de datos
Características del lugar donde se resguardan los soportes*:	Microsoft – Onedrive UNAM-Canadá
(Nombre del sistema A3*)	Formulario WEB
Tipo de soporte*:	Electónico
Descripción*:	Base de datos
Características del lugar donde se resguardan los soportes*:	WordPress

3. ANÁLISIS DE RIESGOS

UNAM-Canadá		
Identificador único*	*628.03*	
(Nombre del sistema A1) *	*Servescol*	
Riesgo*	**Impacto***	**Mitigación***
Modificaciones o daño en la base de datos por los procesos de desarrollo.	*ALTO: Perdida de la integridad de los datos*	*Trabajar los desarrollos del sistema en ambientes de pruebas.*
Ataque con herramientas automatizadas para modificar la base de datos.	ALTO: Perdida de la integridad de los datos.	Limitar el número de operaciones por usuario durante un periodo de tiempo.
Acceso no autorizado al sistema mediante ataques de diccionario o fuerza bruta.	*ALTO: Perdida de la confidencialidad de los datos.*	*Implementar un Captcha para evitar el uso de herramientas automatizadas.*
Ataque de denegación de servicio (DoS) que provoque una sobrecarga de solicitudes.	*ALTO: Perdida de la disponibilidad de los datos.*	*Uso de herramientas para el monitoreo continuo del tráfico hacia el sistema.* *Configuración de Firewalls mediante reglas de bloqueo por región o rangos de IP.*
Aprovisionamiento.	*ALTO: Caída del sistema.*	*Uso de contenedores.*
Alojamiento de múltiples servicios en el mismo servidor.	*ALTO: Caída del servidor por un solo un servicio.*	*Desplegar los servicios en diferentes servidores.*
Tráfico inseguro de datos.	*ALTO: Robo de datos sensibles.*	*Encriptación de datos sensibles.*
(Nombre del sistema A1) *	*ACOMBA*	
Riesgo*	**Impacto***	**Mitigación***
Modificaciones o daño en la base de datos.	*ALTO: Riesgo de la integridad de los datos.*	*Verificar los respaldos y el correcto registro de la misma en OneDrive – Microsoft.*

Acceso no autorizado a la cuenta Microsoft-OneDrive de la UNAM-Canadá.	*ALTO: Perdida de la confidencialidad de los datos.*	*Activar la verificación en 2 pasos de la cuenta de Microsoft de la UNAM-Canadá.*
Ataque de Phishing a los usuarios con acceso al sistema.	*ALTO: Perdida de la confidencialidad de los datos.*	*Campaña de concientización sobre el Phishing.*
(Nombre del sistema A1) *	*Formulario Web*	
Riesgo*	**Impacto***	**Mitigación***
Modificaciones o perdida de registros en la base de datos.	*ALTO: Riesgo de la integridad de los datos.*	*Realizar respaldos peiodicos de la base de datos.*
Ataque con heramientas automatizadas para modificar la base de datos.	*ALTO: Perdida de la integridad de los datos.*	*Limitar el número de operaciones por dirección IP durante un periodo de tiempo.*
Ataque SQL Injection.	*ALTO: Perdida de la integridad de los datos.*	*Utilizar archivos centrales de WordPress actualizados.*

4. ANÁLISIS DE BRECHA

UNAM-Canadá		
Identificador único*	*628.03*	
(Nombre del sistema A1) *	*Servescol*	
Medida de seguridad actual*	**Medida de seguridad necesaria***	**Acciones para remediación***
Resguardo en servidor de DGTIC, con los protocolos de respaldo establecidos por esta entidad y respaldos locales.	*No aplica.*	*No aplica.*
Uso de protocolo HTTPS para la transmisión segura de datos.	*No aplica.*	*No aplica.*
Roles de usuario que siguen el Principio del Mínimo Privilegio.	*No aplica.*	*No aplica.*
Inicio de sesión sin límite de intentos inválidos.	*Definir un límite de intentos inválidos para el inicio de sesión.*	*Hacer la solicitud para que se modifiqué el código fuente del sistema.*
Inicio de sesión solicitando nombre de usuario y contraseña.	*Agregar un Captcha para evitar inicios de sesión automatizados.*	*Hacer la solicitud para que se modifiqué el código fuente del sistema.*
Cambio de contraseñas.	*Definir un periodo aproximado de 3 meses para cambiar la contraseña de los usuarios.*	*Solicitar al administrador que envíe emails a los usuarios periódicamente.*
(Nombre del sistema A2) *	*ACOMBA*	
Medida de seguridad actual*	**Medida de seguridad necesaria***	**Acciones para remediación***
Resguardo en OneDrive – Microsoft o equipo local.	*Resguardo de la base datos en la nube para conexión de usuarios vía web.*	*Contactar al proveedor para contratar los servicios de cloud.*
Acceso a la cuenta Microsoft-OneDrive de la UNAM-Canadá solicitando	*Activar la verificación en 2 pasos para acceder a la cuenta.*	*Solicitar al administrador del sistema que active la verificación en 2 pasos.*

correo electrónico y contraseña.		
(Nombre del sistema A3) *	*Formulario Web*	
Medida de seguridad actual*	**Medida de seguridad necesaria***	**Acciones para remediación***
Resguardo en Word-Press.	*No aplica.*	*No aplica.*
Uso de un mecanismo Captcha.	*No aplica.*	*No aplica.*
Envío de datos seguro.	*No aplica.*	*No aplica.*
Respaldo semanal de la página de WordPress.	*No aplica.*	*No aplica.*
Acceso al panel de administración de WordPress con correo electrónico o usuario y contraseña.	*Activar la verificación en 2 pasos para acceder al panel de administración.*	*Solicitar al administrador que habilité plugins que permitan la verificación en 2 pasos.*

5. PLAN DE TRABAJO

UNAM-Canadá			
Identificador único*	*628.03*		
(Nombre del sistema A1) *	*Servescol*		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Aumentar la seguridad de las contraseñas.	*Implementar políticas de seguridad robustas.*	*6 meses.*	*Se protege el acceso de los usuarios autorizados por medio de contraseñas seguras.*
Aumentar la seguridad de las contraseñas.	*Cambiar las contraseñas periódicamente para evitar accesos no autorizados.*	*3 meses.*	*Se protegen los datos de inicio de sesión de los usuarios.*
Aumentar la seguridad del acceso al sistema.	*Implementación de un Captcha para evitar el acceso no autorizado al sistema mediante ataques de fuerza bruta.*	*1 mes.*	*Se garantiza que los datos solo sean manejados por los usuarios autorizados.*
Aumentar la seguridad del acceso al sistema.	*Implementación de un límite de intentos inválidos para evitar el acceso no autorizado al sistema.*	*3 semanas.*	*Se garantiza que los datos solo sean manejados por los usuarios autorizados.*
Cambiar los servicios a diferentes servidores.	*Implementar los servicios en diferentes servidores.*	*1 año.*	*Se garantiza que si un servicio sufre una caída los demás sigan trabajando y así se mantenga la disponibilidad de los datos.*
(Nombre del sistema A2) *	*ACOMBA*		
Actividad*	**Descripción***	**Duración***	**Cobertura***

Transferir el sistema al cloud suministrado por el proveedor.	*Contactar al proveedor para contratar el sistema en Icloud.*	*1 año*	*Se protege la integridad de los datos registrados en la base de datos con la encriptación que provee el proveedor de servicio.*
Aumentar la seguridad del acceso a la cuenta Microsoft-OneDrive de la UNAM-Canadá	*Activar la verificación en 2 pasos para garantizar que el usuario es autorizado.*	*1 semana.*	*Se protege la confidencialidad de los datos contables de la UNAM-Canadá.*
Campaña de concientización sobre los ataques de Phishing.	*Impartir cursos con técnicas para detectar ataques de Phishing y evitar la divulgación de la información contable de la UNAM-Canadá.*	*1 mes.*	*Se protege la confidencialidad de los datos contables de la UNAM-Canadá.*
(Nombre del sistema A3) *	*Formulario Web*		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Aumentar la seguridad de las contraseñas	*Implementar políticas de seguridad robustas*	*6 meses*	*Se protege el acceso de los usuarios autorizados por medio de contraseñas seguras.*
Cambiar las contraseñas.	*Cambiar las contraseñas periódicamente para evitar ataques y mejorar la seguridad.*	*3 meses.*	*Se protegen los datos de inicio de sesión de los usuarios.*
Aumentar la seguridad de WordPress.	*Realizar revisiones periódicas para garantizar que todos los archivos y plugins utilizados estén actualizados y cuenten con soporte.*	*Permanentemente.*	*Se protege WordPress de posibles vulnerabilidades que puedan atentar contra la integridad, confidencialidad y disponibilidad de los datos de los usuarios.*

Aumentar la seguridad del panel de administración de WordPress.	*Habilitar plugins que permitan la verificación en 2 pasos para garantizar que solo el administrador tenga acceso a la configuración de WordPress.*	*1 semana.*	*Se mantiene la configuración de seguridad para la protección de la integridad y confidencialidad de los datos de los usuarios.*
Aumentar la seguridad del archivo de configuración de la base de datos.	*Proteger el directorio wp-includes y el archivo wp-config.php para que solo se le permita el acceso al administrador y así evitar modificaciones en la configuración de la base de datos.*	*2 semanas.*	*Se protege la base de datos para garantizar la integridad, confidencialidad y disponibilidad de los datos de los usuarios.*

6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

I. TRANSFERENCIAS DE DATOS PERSONALES

UNAM-Canadá	
Identificador único*	*628.03*
(Nombre del sistema A1)*	*Servescol*
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado sobre redes electrónicos:	**a)** Se envía la información por medio del sistema drive de Google con usuarios específicos. **b)** Se envía correo electronico mediante oficio y en PDF. **c)** Se solicita confirmación de recibido. **d)** Contienen datos de población para estadisticas **e)** Indicar si las transferencias de datos personales se formalizaron mediante oficio de acuerdo con las entregas programadas.

II. RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS

No aplica.

III. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

No aplica.

IV. REGISTRO DE INCIDENTES:

Se realiza de acuerdo con la pólitica para la protección de datos de la sede.

V. ACCESO A LAS INSTALACIONES

1. Seguridad perimetral exterior:

Se utiliza el sistema de control de acceso mediante un videoportero en caso que el edificio no se encuentre abierto al publico.

2. Seguridad perimetral interior:

No cuenta con sistema de seguridad perimetral al interior.

VI. ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

La información se actualiza a solicitud de la persona interesada y está a acargo del área de Servicios Escolares.

Las medidas de seguridad previstas a continuación en los incisos VII al IX, sólo aplican para soportes electrónicos

VII. PERFILES DE USUARIO Y CONTRASEÑAS

La sede cuenta con la suite Microsoft 365 la cual es accecible mediante usuario y contraseña Microsoft, esta controla el acceso a la gestión de correos, como el acceso a los archivos del cloud (OneDrive) y los archivos de office.

1. Modelo de control de acceso (alguno de los siguientes):

- **a)** Es obligatoria
- **b)** Se adquiere al momento de su vinculación con la sede bajo autorización de la dirección
- **c)** No es discrecional y tiene accesos restringidos
- **d)** Cuenta con acceso restringido de acuerdo con el tipo de vinculación con la sede

2. Perfiles de usuario y contraseñas en el sistema operativo de red:

- **a)** Se cuenta con un usuarios y contraseñas para los equipos así como el usuario de microsoft para los archivos de office.
- **b)** Este proporciona un manejo riguroso de usuario y contraseñas.

3. Perfiles de usuario y contraseñas manejados por el software aplicativo del sistema de tratamiento de datos personales:

- **a)** Los sistemas de la sede cuentan con un manejo riguroso de perfiles de usuario y contraseñas.

b) Los sistemas cifran los nombres de usuario y las contraseñas cuando los almacena.

4. Administración de perfiles de usuario y contraseñas:

a) El Delegado Administrativo da de alta nuevos perfiles.

b) La Dirección de la sede autoriza la creación de nuevos perfiles.

c) El Delegado Administrativo lleva registro de la creación de nuevos perfiles.

5. Acceso remoto al sistema de tratamiento de datos personales:

a) Los usuarios no requieren acceso remoto al equipo de cómputo ya que los sistemas de la sede cuentan con acceso web.

b) No se requiere acceso remoto para el mantenimiento; se cuenta con acceso web.

c) ¿Cómo se evita el acceso remoto no autorizado? Unicamente cuenta con acceso a los sistemas de la sede los autorizados por la dirección bajo contraseña Microsoft 365.

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

1. Señalar si realiza respaldos

a) Completos;

b) De forma Manual,

c) Periodicidad con que los realiza: mensualmente.

2. Se almacenan en la nube.

3. Se carga y almacena en la Agora de informática, y

4. El responsable de realizar estas operaciones es el área de Gestión y Desarrollo.

IX. PLAN DE CONTINGENCIA

1. Presentar el plan de contingencia con el cual garantiza la continuidad de la operación del sistema o informar si no lo tiene, pero se encuentra desarrollándolo.

No se tiene plan de contingencia, pero se está desarrollando. Esto debido a que Servescol y el formulario web están alojados en servidores administrados por el centro de datos de DGTIC.

2. Si cuenta con plan de contingencia y lo ha implementado, deberá indicar si realiza pruebas de eficiencia de este.

No aplica.

3. Informar si cuenta con un sitio redundante (alterno) y señalar lo siguiente:

No aplica.

I. TRANSFERENCIAS DE DATOS PERSONALES

UNAM-Canadá	
(Nombre del sistema A2)*	*ACOMBA*
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado medios electrónicos:	**a)** Se reporta la información por medio del sistema ACOMBA al sistema de registro de Revenue Canada y Revenue Quebec. **b)** Se envía mediante tranferencia electronica. **c)** Se recibe confirmación de envio. **d)** Contienen datos de población por reporte de impuestos.

II. RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS

No aplica.

III. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

No aplica.

IV. REGISTRO DE INCIDENTES:

Se realiza de acuerdo con la pólitica para la protección de datos de la sede.

V. ACCESO A LAS INSTALACIONES

1. Seguridad perimetral exterior:

No aplica.

2. Seguridad perimetral interior:

No aplica.

VI. ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

La información se actualiza cuando hay algun cambio en los datos de nomina y esta a cargo del área contable.

Las medidas de seguridad previstas a continuación en los incisos VII al IX, sólo aplican para soportes electrónicos

VII. PERFILES DE USUARIO Y CONTRASEÑAS

La sede cuenta con la suite Microsoft 365 la cual es accecible mediante usuario y contraseña Microsoft, esta controla el acceso a la gestión de correos, como el acceso a los archivos del cloud (OneDrive) y los archivos de office.

1. Modelo de control de acceso (alguno de los siguientes):

- **a)** Es obligatoria
- **b)** Se adquiere al momento de su vinculación con la sede bajo autorización de la dirección
- **c)** No es discrecional y tiene accesos restringidos
- **d)** Cuenta con acceso restringido de acuerdo con el tipo de vinculación con la sede

2. Perfiles de usuario y contraseñas en el sistema operativo de red:

- **a)** Se cuenta con un usuarios y contraseñas para los equipos así como el usuario de microsoft para los archivos de office.
- **b)** Este proporciona un manejo riguroso de usuario y contraseñas?

3. Perfiles de usuario y contraseñas manejados por el software aplicativo del sistema de tratamiento de datos personales:

- **a)** Los sistemas de la sede cuentan con un manejo riguroso de perfiles de usuario y contraseñas.
- **b)** Los sistemas cifran los nombres de usuario y las contraseñas cuando los almacena.

4. Administración de perfiles de usuario y contraseñas:

a) El Delegado Administrativo da de alta nuevos perfiles.
b) La Dirección de la sede autoriza la creación de nuevos perfiles.
c) El Delegado Administrativo lleva registro de la creación de nuevos perfiles.

5. Acceso remoto al sistema de tratamiento de datos personales:

a) Los usuarios no requieren acceso remoto al equipo de cómputo ya que los sistemas de la sede cuentan con acceso web.
b) No se requiere acceso remoto para el mantenimiento; se cuenta con acceso web.
c) ¿Cómo se evita el acceso remoto no autorizado? Unicamente cuenta con acceso a los sistemas de la sede los autorizados por la dirección bajo contraseña Microsoft 365.

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

1. Señalar si realiza respaldos

a) Completos;
b) De forma Automática,
c) Periodicidad con que los realiza: diariamente

2. Se almacena en OneDrive.
3. El software al momento de terminar, envía un correo con el backup encriptado y luego se guarda en una carpeta llamada “respaldos”, y
4. El responsable de realizar estas operaciones es el área de Contabilidad.

IX. PLAN DE CONTINGENCIA

1. Presentar el plan de contingencia con el cual garantiza la continuidad de la operación del sistema o informar si no lo tiene, pero se encuentra desarrollándolo.

No se tiene plan de contingencia.

2. Si cuenta con plan de contingencia y lo ha implementado, deberá indicar si realiza pruebas de eficiencia de este.

No aplica.

3. Informar si cuenta con un sitio redundante (alterno) y señalar lo siguiente:

a) Tipo de sitio tibio;
b) Subcontratado con un tercero;
c) No aplica.
d) No aplica.

I. TRANSFERENCIAS DE DATOS PERSONALES

UNAM-Canadá	
(Nombre del sistema A3)*	*Formulario Web / No aplica.*

Ninguno de los puntos aplica.

7. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

7.1. Herramientas y recursos para monitoreo de la protección de datos personales

UNAM-Canadá		
Identificador único*	*628.03*	
(Nombre del sistema A1) *	*Servescol*	
Recurso*	**Descripción***	**Control***
Antivirus.	*Software que protege el envío y almacenamiento de datos personales.*	Verificar que el antivirus este activado. *Responsable: Área de Gestión y Desarrollo.* *Tipo de licencia: Antivirus Bitdefender, Malwarebites y Avg.*
UNAM-Canadá		
Identificador único*	*628.03*	
(Nombre del sistema A2) *	*ACOMBA*	
Recurso*	**Descripción***	**Control***
Antivirus.	*Software que protege el envío y almacenamiento de datos personales.*	Verificar que el antivirus este activado. *Responsable: Área de Gestión y Desarrollo.* *Tipo de licencia: Antivirus Bitdefender, Malwarebites y Avg.*
UNAM-Canadá		

Identificador único*	*628.03*	
(Nombre del sistema A3) *	*Formulario web*	
Recurso*	**Descripción***	**Control***
Antivirus.	*Software que protege el envío y almacenamiento de datos personales.*	Verificar que el antivirus este activado. *Responsable: Área de Gestión y Desarrollo.* *Tipo de licencia: Antivirus Bitdefender, Malwarebites y Avg.*

7.2. Procedimiento para la revisión de las medidas de seguridad

UNAM-Canadá		
Identificador único*	*628.03*	
(Nombre del sistema A1)*	*Servescol*	
Medida de seguridad*	**Procedimiento***	**Responsable***
Enviar la información por medio del sistema drive de Google con usuarios específicos.	*Antes de enviar los datos mediante el sistema drive de Google, se revisa que los destinatarios sean los correctos.*	*a) Área de Gestión y Desarrollo y área de Servicios escolares.* *b) 1 día.*
(Nombre del sistema A2)*	*ACOMBA*	
Medida de seguridad*	**Procedimiento***	**Responsable***
Recepción de confirmación de envió.	*Después de reportar la información por medio del sistema siempre se debe recibir una confirmación de envío.*	*a) Área de Contabilidad.* *b) 1 día.*
(Nombre del sistema A3)*	*Formulario Web / No aplica*	

7.3. Resultados de la evaluación y pruebas a las medidas de seguridad

UNAM-Canadá	
Identificador único*	*628.03*
(Nombre del sistema A1)*	*Servescol / No aplica*
(Nombre del sistema A2)*	*ACOMBA / No aplica*
(Nombre del sistema A3)*	*Formulario Web / No aplica*

7.4. Acciones para la corrección y actualización de las medidas de seguridad

UNAM-Canadá		
Identificador único*	*628.03*	
(Nombre del sistema A1)*	*Servescol*	
Medida de seguridad*	**Acciones***	**Responsable***
Enviar la información por medio del sistema drive de Google con usuarios específicos.	a) Resguardar los datos expuestos b) Mantener actualizada la lista de usuarios a los que se les debe enviar la información.	*a) Área de Gestión y Desarrollo y área de Servicios escolares.* *b) No aplica*
(Nombre del sistema A2) *	*ACOMBA*	
Medida de seguridad*	**Acciones***	**Responsable***
Recepción de confirmación de envió.	a) Solicitar la confirmación. b) Saber con quién comunicarse en caso de no recibir la confirmación	*a) Área de Contabilidad.* *b) No aplica.*
(Nombre del sistema A3) *	*Formulario Web / No aplica*	

8. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

8.1. Programa de capacitación a los responsables de tratamiento de datos personales

UNAM-Canadá			
Identificador único*	*628.03*		
(Nombre del sistema A1)*	***Servescol***		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Evitar el uso de medios externos.	*Enviar archivos sensibles por medios no autorizados (WhatsApp, Facebook, correos personales…)*	Indefinido	*Se protegen los datos sensibles de la institución.*
Curso ataque SQL Injection.	*Curso sobre cómo evitar ataques de SQL Injection*	*1 mes*	*Se evitan modificaciones a la Base de Datos o bien el robo de información.*
Capacitación sobre sistema.	*Capacitación con anteriores responsables de los datos.*	*1 semana*	*Mantener informados a los nuevos responsables sobre el manejo del sistema y por tanto de los datos.*
Curso sobre el manejo de datos sensibles.	*El personal comprenderá y aplicará la forma correcta sobre el manejo de datos.*	*1 mes*	*Evitar manejar inadecuadamente los datos y el ropo de la información personal.*

(Nombre del sistema A2) *	***ACOMBA***

Actividad*	**Descripción***	**Duración***	**Cobertura***
Evitar el uso de medios externos.	Enviar archivos sensibles por medios no autorizados (WhatsApp, Facebook, correos personales…)	Indefinido	*Se protegen los datos sensibles de la institución.*
Capacitación sobre sistema.	*Capacitación con anteriores responsables de los datos.*	*1 semana*	*Mantener informados a los nuevos responsables sobre el manejo del sistema y por tanto de los datos.*
Curso sobre el manejo de datos sensibles.	*El personal comprenderá y aplicará la forma correcta sobre el manejo de datos.*	*1 mes*	*Evitar manejar inadecuadamente los datos y el ropo de la información personal.*

(Nombre del sistema A3) *	***Formulario Web***

Actividad*	**Descripción***	**Duración***	**Cobertura***
Curso sobre ciberseguridad.	Curso sobre inicios de sesión malintencionados	*1 mes*	*Se mantienen informados sobre los nuevos.*
Curso ataque SQL Injection.	*Curso sobre cómo evitar ataques de SQL Injection*	*1 mes*	*Se evitan modificaciones a la Base de Datos o bien el robo de información.*
Acceso al panel de administración de WordPress con correo electrónico o usuario y contraseña	*Activar la verificación en 2 pasos para acceder al panel de administración.*	*Indefinido*	*Activar plugin que permitan el uso de verificación en 2 pasos para evitar el robo de identidad.*

8.2. Programa de difusión de la protección a los datos personales

UNAM-Canadá			
Identificador único*	*628.03*		
(Nombre del sistema A1)*	***Servescol***		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Aviso de Privacidad Integral	*La Escuela de Extensión Universitaria UNAM-Canadá de la Universidad Nacional Autónoma de México (UNAM), tiene un apartado en el cual redacta y difunde cuales son los usos de los datos personales recabados.*	*Indefinido*	*Si es alumno, docente, personal de la entidad académica, conferencista o invitado externo a la Universidad (nacional o extranjero), visitante, proveedor o cliente de servicios universitarios, puede saber las finalidades de los datos personales recabados.*
UNAM-Canadá			
(Nombre del sistema A2) *	***ACOMBA***		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Aviso de Privacidad Integral	*La Escuela de Extensión Universitaria UNAM-Canadá de la Universidad Nacional Autónoma de México (UNAM), tiene un apartado en el cual redacta y difunde cuales son los usos de los datos personales recabados.*	*Indefinido*	*Si es alumno, docente, personal de la entidad académica, conferencista o invitado externo a la Universidad (nacional o extranjero), visitante, proveedor o cliente de servicios universitarios, puede saber las finalidades de los datos personales recabados.*
UNAM-Canadá			
(Nombre del sistema A3) *	***Formulario Web***		

Actividad*	Descripción*	Duración*	Cobertura*
Aviso de Privacidad Integral	*La Escuela de Extensión Universitaria UNAM-Canadá de la Universidad Nacional Autónoma de México (UNAM), tiene un apartado en el cual redacta y difunde cuales son los usos de los datos personales recabados.*	*Indefinido*	*Si es alumno, docente, personal de la entidad académica, conferencista o invitado externo a la Universidad (nacional o extranjero), visitante, proveedor o cliente de servicios universitarios, puede saber las finalidades de los datos personales recabados.*

9. MEJORA CONTINUA

9.1. Actualización y mantenimiento de sistemas de información

UNAM-Canadá			
Identificador único*	628.03		
(Nombre del sistema A1)*	Servescol		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Mantenimiento correctivo	*Se realiza a cabo para corregir los errores detectados durante la explotación del sistema. No identificados durante la fase de pruebas y ejecución.*	*1 semana*	*Solución de vistas, filtros en las búsquedas en las bases de datos o diseño.*
Mantenimiento evolutivo	*Modificar algo que funcionaba o estaba correcto, con el objeto de aumentar, disminuir o cambiar las funcionalidades del sistema.*	*3-6 meses*	*mejora a nivel diseño, cambios a nivel normativo o nuevas funcionalidades del sistema.*
UNAM-Canadá			
Identificador único*	628.03		
(Nombre del sistema A2)*	Acomba		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Mantenimiento correctivo	*Se realiza a cabo para corregir los errores detectados durante la explotación del sistema. No identificados durante la fase de*	*No aplica*	*Estas tareas son realizadas por el proveedor del servicio.*

	pruebas y ejecución.		
Mantenimiento evolutivo	*Modificar algo que funcionaba o estaba correcto, con el objeto de aumentar, disminuir o cambiar las funcionalidades del sistema.*	*No Aplica*	*Estas tareas son realizadas por el proveedor del servicio.*
UNAM-Canadá			
Identificador único*	628.03		
(Nombre del sistema A3)*	Formulario Web		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Mantenimiento correctivo	*Se realiza a cabo para corregir los errores detectados durante la explotación del sistema. No identificados durante la fase de pruebas y ejecución.*	*1 semana*	*Se asegura que los todos los campos del formulario, el catcha,y la base de datos se actualice correctamente.*
Mantenimiento evolutivo	*Modificar algo que funcionaba o estaba correcto, con el objeto de aumentar, disminuir o cambiar las funcionalidades del sistema.*	*1 mes*	*Agrega una mejora visual, o quitan campos según las directivas.*

9.2. Actualización y mantenimiento de equipo de cómputo

UNAM-Canadá			
Identificador único*	628.03		
(Nombre del sistema A1)*	**Servescol**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Solicitud de actualización o mantenimiento.	*Se recibe una solicitud de revisión teniendo en cuenta si presenta alguna falla o requiere alguna actualización o si se tiene planeado un mantenimiento preventivo del equipo.*	*1 día*	*Identificación del equipo por realizar el mantenimiento o actualización y determinar el procedimiento a seguir.*
Recepción del equipo	*Se establece con una fecha y hora para la actividad.*	*1 hora*	*Se determina la disponibilidad del equipo a actualizar y se establece si es necesario entregar de un equipo de repuesto.*
Respaldo del equipo	*Se realiza una copia de seguridad al equipo*	*2 horas*	*Se evita perdidas de información para poder proceder de forma segura.*
Instalación de actualizaciones o mantenimiento	*Se procede a instalar las paqueterías necesarias para actualizar el equipo y se revisan el estado de otras aplicaciones.*	*1 hora*	*Optimizar el rendimiento y funcionamiento del equipo.*
UNAM-Canadá			
Identificador único*	628.03		
(Nombre del sistema A2)*	Acomba		
Actividad*	**Descripción***	**Duración***	**Cobertura***

Solicitud de actualización o mantenimiento.	*Se recibe una solicitud de revisión teniendo en cuenta si presenta alguna falla o requiere alguna actualización o si se tiene planeado un mantenimiento preventivo del equipo.*	*1 día*	*Identificación del equipo por realizar el mantenimiento o actualización y determinar el procedimiento a seguir.*
Recepción del equipo	*Se establece con una fecha y hora para la actividad.*	*1 hora*	*Se determina la disponibilidad del equipo a actualizar y se establece si es necesario entregar de un equipo de repuesto.*
Respaldo del equipo	*Se realiza una copia de seguridad al equipo*	*2 horas*	*Se evita perdidas de información para poder proceder de forma segura.*
Instalación de actualizaciones o mantenimiento	*Se procede a instalar las paqueterías necesarias para actualizar el equipo y se revisan el estado de otras aplicaciones.*	*1 hora*	*Optimizar el rendimiento y funcionamiento del equipo.*
UNAM-Canadá			
Identificador único*	628.03		
(Nombre del sistema A3)*	Formulario Web		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Solicitud de actualización o mantenimiento.	*Se recibe una solicitud de revisión teniendo en cuenta si presenta alguna falla o requiere alguna actualización o si se tiene planeado un mantenimiento preventivo del equipo.*	*1 día*	*Identificación del equipo por realizar el mantenimiento o actualización y determinar el procedimiento a seguir.*
Recepción del equipo	*Se establece con una fecha y hora para la actividad.*	*1 hora*	*Se determina la disponibilidad del equipo a actualizar y se establece si es necesario*

			entregar de un equipo de repuesto.
Respaldo del equipo	*Se realiza una copia de seguridad al equipo*	*2 horas*	*Se evita perdidas de información para poder proceder de forma segura.*
Instalación de actualizaciones o mantenimiento	*Se procede a instalar las paqueterías necesarias para actualizar el equipo y se revisan el estado de otras aplicaciones.*	*1 hora*	*Optimizar el rendimiento y funcionamiento del equipo.*

9.3. Procesos para la conservación, preservación y respaldos de información

UNAM-Canadá		
Identificador único*	628.03	
(Nombre del sistema A1)*	**Servescol**	
Proceso*	**Descripción***	**Responsable***
Proceso de conservación, preservación y respaldo de información.	*La información contenida en este sistema se aloja en un servidor administrado por DGTIC.*	*Todas las acciones son realizadas por el cuerpo de Centro de Datos de DGTIC*
UNAM-Canadá		
Identificador único*	628.03	
(Nombre del sistema A2)*	Acomba	
Proceso*	**Descripción***	**Responsable***
Proceso de conservación, preservación y respaldo de información.	*Este software contiene una función de respaldo automático todos los días en las mañanas.* *Una vez hecho el respaldo, se envía una copia de la información encriptada que luego es resguardada en un repositorio de Cloud de Microsoft.*	*Jefe contable.*
UNAM-Canadá		
Identificador único*	628.03	
(Nombre del sistema A3)*	Formulario Web	
Proceso*	**Descripción***	**Responsable***
Proceso de conservación, preservación y respaldo de información.	*La información contenida en este sistema se aloja en un servidor administrado por DGTIC.*	*Todas las acciones son realizadas por el cuerpo de Centro de Datos de DGTIC*

	Como segunda medida de respaldo. Cada viernes se realiza una copia de seguridad del sitio web y se conservan los últimos 6 meses de copias de seguridad en el mismo servidor de administrado por DGTIC.	*Las copias de seguridad son realizadas por Departamento de Gestión y Desarrollo*

9.4. Procesos de borrado seguro y disposición final de equipos y componentes informáticos

UNAM-Canadá		
Identificador único*	*628.03*	
(Nombre del sistema A1)*	**Servescol**	
Proceso*	**Descripción***	**Responsable***
Borrado seguro	*Servescol es una herramienta cloud por lo no guarda 1archivos del sistema ni bases de datos en la computadora.* *En caso de necesitar el borrado del sistema operativo, se procede con el formateo de datos completo y reinstalación del mismo, creación de usuarios e instalación de aplicaciones.* *La sobreescritura reduce la posibilidad de recuperar información.*	*a) Departamento de Gestión y Desarrollo* *b) 1 día*
UNAM-Canadá		
Identificador único*	*628.03*	
(Nombre del sistema A2)*	**Acomba**	
Proceso*	**Descripción***	**Responsable***
Borrado seguro	*Servescol es una herramienta cloud por lo no guarda archivos del sistema ni bases de datos en la computadora.* *En caso de necesitar el borrado del sistema operativo, se procede con el formateo de datos completo y reinstalación de este, creación de usuarios e instalación de aplicaciones.*	*a) Departamento de Gestión y Desarrollo* *b) 1 día*

	La sobreescritura reduce la posibilidad de recuperar información.	
UNAM-Canadá		
Identificador único*	*628.03*	
(Nombre del sistema A3)*	**Formulario Web**	
Proceso*	**Descripción***	**Responsable***
Borrado seguro	*Servescol es una herramienta cloud por lo no guarda archivos del sistema ni bases de datos en la computadora.* *En caso de necesitar el borrado del sistema operativo, se procede con el formateo de datos completo y reinstalación de este, creación de usuarios e instalación de aplicaciones.* *La sobreescritura reduce la posibilidad de recuperar información.*	*a) Departamento de Gestión y Desarrollo* *b) 1 día*

10. PROCEDIMIENTO PARA LA CANCELACIÓN DE UN SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

(Informar y describir el procedimiento para la cancelación de un sistema de tratamiento de datos personales.)

Cuando la totalidad de los datos personales contenidos en un Sistema de tratamiento de datos personales de la UNAM-Canadá haya dejado de ser necesarios por obsolescencia de be ser cancelado. El procedimiento de cancelación inicia con el bloqueo de los datos personales por un periodo que será acordado por el responsable del sistema de datos y le corresponde también identificar los datos personales que han dejado de ser útiles e iniciar y solicitar el bloqueo mediante notificación al encargado de los Sistemas informáticos.

Dicho bloqueo tiene por objetivo impedir el tratamiento del Sistema de Datos Personales y su acceso por cualquier persona para evitar pérdidas, destrucción o extravío. La única persona autorizada a acceder es el responsable del sistema de datos personales.

Durante el periodo de bloqueo, el responsable deberá mantener todas las copias y/o reproducciones que se tengan del Sistema de Datos Personales, con las mismas medidas de seguridad que el original, para evitar su tratamiento, alteración, destrucción o acceso no autorizado.

Transcurrido el periodo de bloqueo del Sistema de Datos Personales, el responsable deberá solicitar al Staff Directivo, la autorización de la cancelación del Sistema. La solicitud debe ser mediante un oficio que incluya la justificación de la cancelación del sistema y aseguramiento de que los datos del no hay sufrido algún cambio o alteración durante el periodo de bloqueo.

Los sistemas de datos personales electrónicos almacenados en equipos de cómputo o dispositivos deberán ser formateados en presencia del responsable y del encargado del sistema ofimáticos. Para eliminar la información con herramientas propias del sistema operativo utilizando el eliminado seguro, herramientas de software para verificar la posibilidad de recuperación de la información eliminada, utilizar herramientas de software para sobrescribir la información eliminada y verificar nuevamente si es posible recuperar la información eliminada.

Luego de eliminar los datos del sistema, se deberá generar un acta con los presentes para finalizar el procedimiento de cancelación del sistema de datos.

11. APROBACIÓN DEL DOCUMENTO DE SEGURIDAD

		Nombre y firma de quienes revisaron el presente documento:
Responsable del desarrollo:	(Señalar nombre, puesto, teléfono y correo electrónico del servidor público que elaboró el documento de seguridad)	Andrés Castañeda Gestión y Desarrollo acastaneda@unamcanada.com
Revisó:	(Señalar nombre, puesto, teléfono y correo electrónico del servidor público que revisó el documento de seguridad)	Alex Méndez Delegado Administrativo amendez@unamcanada.com
Autorizó:	(Señalar nombre, puesto, teléfono y correo electrónico del servidor público que autorizó el documento de seguridad)	Constantino Macías Garcia Director maciasg@unamcanada.com
Fecha de aprobación:	(Incluir la fecha de liberación del documento)	Noviembre 09 de 2022
Fecha de actualización:	(Incluir la primera versión e ir agregando las subsiguientes del documento)	Noviembre 09 de 2022

ANEXO II. FORMATO UNIVERSITARIO DE "SOLICITUD DE EJERCICIO DE DERECHOS ARCO"

Formato de solicitud de ejercicio de derechos Acceso, Rectificación, Cancelación y Oposición (ARCO)

Con fundamento en el artículo 54 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, esta área universitaria le solicita llenar el presente formato para ejercer sus derechos de Acceso, Rectificación, Cancelación y Oposición.

1. Datos del Área Universitaria de la UNAM responsable de tratar los datos personales*:

2. Datos del Titular de los Datos Personales*:

Primer apellido:	Segundo apellido:	Nombre(s):
CURP (para evitar homónimos):		

3. Datos del solicitante:

Primer apellido:	Segundo apellido:	Nombre(s):
Indicar si los datos corresponden a:		
☐Titular		
☐Menor de edad		
☐Persona que se encuentren en estado de interdicción o incapacidad establecida por ley.		
☐Fallecida		
Datos de identidad y representación legal (opcional, solo si usted no es el titular de los datos personales)		
☐Persona física:		
☐Nombre completo del representante:		
☐Representación de un menor de edad:		
☐Representación de una persona que se encuentren en estado de interdicción o incapacidad establecida por ley.		
☐Persona moral:		
☐Nombre o razón social del representante:		
Registro Federal de Contribuyentes (RFC):		
Documento con el que acredita la representación:		
☐Poder notarial ☐Carta poder simple signada ante dos testigos (con copia de los documentos que acrediten la identidad de los testigos y titular) ☐Declaración en comparecencia del Titular (en las instalaciones del área universitaria).		

4. Documento oficial de identificación del titular o solicitante (sólo originales) *:

☐Credencial para votar (INE)	☐Pasaporte	☐Licencia de conducir
☐Cédula profesional	☐Cartilla del Servicio militar nacional	☐Documento migratorio
☐Acta de nacimiento	☐Acta de defunción	☐Otra identificación con fotografía (especifique):

5. Medio por el cual prefiere que le sea notificada la puesta a disposición de la respuesta*:

☐Acudir al área universitaria donde presentó este formato	☐Correo electrónico (especificar):

6. Modalidad en la cual prefiere le sean entregados los datos, en caso de ser procedente. *

☐Copia simple	☐Correo electrónico
☐Copia certificada	☐ Otro medio electrónico como USB/CD ROOM/ DVD *(previo depósito de ficha de pago):*
☐Consultas directas	☐Yo proporciono el medio magnético o electrónico para reproducir los datos personales.

7. Tipo de solicitud de ejercicio de Derechos Acceso, Rectificación, Cancelación y Oposición (ARCO) a datos personales*:

☐ACCESO
Describir la información datos personales que obran en posesión del área universitaria y a los que requiere tener acceso*: _____ _____ _____

Señalar el nombre y ubicación del archivo o registro de datos personales*: _____ _____ _____
☐RECTIFICACIÓN
☐Son inexactos.
☐Son incompletos.
☐Requieren ser actualizados
Justificación y documentación original que acompaña para motivar su petición*: _____ _____ _____
CANCELACIÓN (supresión o eliminación)
Causas que motivan la cancelación*:
OPOSICIÓN (cese del tratamiento)
Causas que motivan la oposición (daño o perjuicio que le causa la persistencia del tratamiento de sus datos)*:_____ _____
Señalar si es para una finalidad específica o para todos los sistemas de información que obren en el área universitaria*._____
Documentación original que acompaña para motivar su petición*: _____
Señalar la referencia o documento que facilite la localización de sus datos personales*
_____ _____

Leí el Aviso de privacidad del área universitaria a la que acudo y en este acto otorgo el consentimiento para que mis datos personales sean tratados conforme al mismo.

_____

Firma o huella dactilar*

Plazos y procedimiento para la atención de las solicitudes de ejercicio de derechos ARCO:
Una vez que se presentó la solicitud, esta área universitaria cuenta con:

- Un plazo de 20 días hábiles, contados a partir del día siguiente a la recepción de la solicitud, para informarle si procede o no el ejercicio del derecho solicitado.
- Un plazo de 15 días hábiles, contados a partir del día siguiente en el que le haya notificado la respuesta anterior, en caso de que haya procedido el ejercicio del derecho, deberá llevar a cabo las acciones necesarias para hacerlo efectivo.

El ejercicio de los derechos ARCO será sencillo y gratuito, siempre que no rebase las 20 hojas simples, por lo que las áreas universitarias realizarán el cobro del costo de reproducción de acuerdo con los Lineamientos para la determinación de los costos de reproducción y envío en el marco de solicitudes de acceso a Información y entrega de datos personales en la Universidad Nacional Autónoma de México.

ANEXO III. CARTA DE CONFIDENCIALIDAD

Carta compromiso de confidencialidad, no divulgación, reserva y resguardo de información y datos personales

(Este documento debe firmarse por todas aquellas personas que por su empleo, cargo o comisión en la Universidad reciban y traten información confidencial de otras personas)

CIUDAD DE _____, A (DD-MM-AAAA)

(Nombre completo), *(cargo)*, adscrita(o) *(dependencia/entidad de adscripción)* de la Universidad Nacional Autónoma de México (en adelante la UNAM) acepto los términos y condiciones, que se describen más adelante, de resguardo, reserva, custodia y protección de la seguridad y confidencialidad de la información, datos personales y de todo tipo de documentos propiedad de la UNAM de los que tenga conocimiento, con motivo de las funciones que desempeño en la Universidad.

El presente compromiso me responsabiliza respecto de la información que me sea proporcionada por la UNAM, ya sea de forma oral, escrita, impresa, sonora, visual, electrónica, informática u holográfica, contenida en cualquier tipo de documento, que puede consistir en: expedientes, reportes, estudios, actas, resoluciones, oficios, correspondencia, acuerdos, directivas, directrices, circulares, contratos, convenios, instructivos, notas, memorandos, estadísticas, o bien, cualquier otro registro en medio conocido o por conocer que documente el ejercicio de las facultades, funciones y competencias del área universitaria y de los servidores universitarios, sin importar su fuente o fecha de elaboración.

La información que me sea proporcionada podría ser considerada, según el caso, como reservada, privilegiada y confidencial, en los términos de las leyes aplicables, por lo que me obligo a protegerla, reservarla, resguardarla y no divulgarla, utilizándola única y exclusivamente para llevar a cabo y cumplir con las actividades y obligaciones que expresamente me sean conferidas por la Universidad.

Es mi responsabilidad no reproducir, hacer pública o divulgar a terceros la información objeto de la presente Carta, y de cumplir con las medidas de seguridad adecuadas al tipo de documento con el que se trabaje.

Mi obligación de confidencialidad no es aplicable en los siguientes casos:

a) Cuando la información se encuentre en el dominio público en el momento en que me sea suministrada o, una vez suministrada, ésta se haga pública.
b) Cuando la legislación vigente o un mandato judicial exija su divulgación.
c) Cuando la información se desarrolle o reciba legítimamente de terceros, de forma totalmente independiente a mi relación con la Universidad.

A t e n t a m e n t e

_____
Firma o huella dactilar

UNAM

ALEMANIA

1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

UNAM-Alemania (Centro de Estudios Mexicanos)	
Identificador único*	RAAC/ALE
(Nombre del sistema A1) *	**Registro de Actividades Académicas y Culturales**
Datos personales (sensibles o no) contenidos en el sistema*:	Nombre Correo electrónico Entidad académica a la que pertenece (si aplica) Grado académico (si aplica) Área de estudios (si aplica)
Responsable*:	
Nombre*:	**José Alejandro Velázquez Montes**
Cargo*:	**Director**
Funciones*:	Coordinar las actividades académicas y culturales
Obligaciones*:	Asegurar el correcto uso y almacenamiento/eliminación de los datos personales
	Encargados:
(Nombre del Encargado 1*)	**Andrea Guillén de la Rosa**
Cargo*:	**Coordinadora de Relaciones y Gestión**
Funciones*:	Recopilar la información relativa a los asistentes a actividades académicas y culturales, así como reportar las mismas a las instancias centrales de la universidad.
Obligaciones*:	Integrar los registros de asistentes y resguardar la información.
(Nombre del Encargado 2*)	**Alejandra Fregoso Domínguez**
Cargo*:	**Coordinadora de Vinculación Intra e Interinstitucional**
Funciones*:	Recopilar la información relativa a los asistentes a actividades académicas y culturales
Obligaciones*:	Entregar a la coordinadora de Relaciones y Gestión los registros de asistentes a actividades académicas y culturales.
	Usuarios:
(Nombre del Usuario 1*)	**Paola Mendieta Verdejo**
Cargo*:	Jefa del departamento de apoyo académico a las sedes en el extranjero
Funciones*:	Comprobar la información vertida en el formato de Actividades Académicas y Culturales.
Obligaciones*:	No difundir información de los datos personales; no modificar la información almacenada en el servidor; no hacer respaldos en equipo personal de la información de datos personales.

2. ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

UNAM-Alemania (Centro de Estudios Mexicanos)	
Identificador único¨*	RAAC/ALE
(Nombre del sistema A1*)	**Registro de Actividades Académicas y Culturales**
Tipo de soporte:*	Electrónico
Descripción:*	Base de datos
Características del lugar donde se resguardan los soportes:*	Alojamiento en el disco duro de la coordinación de relaciones y gestión de UNAM-Alemania y en el Google Drive de la Coordinación de Relaciones y Asuntos Internacionales.

3. ANÁLISIS DE RIESGOS

UNAM-Alemania (Centro de Estudios Mexicanos)		
Identificador único*	RAAC/ALE	
(Nombre del sistema A1) *	**Registro de Actividades Académicas y Culturales**	
Riesgo*	**Impacto***	**Mitigación***
Que la persona utilice su correo privado para acceder al Google Drive y tenga acceso a la información incluso después de desprenderse del cargo.	*Alto. La persona haga uso de la información para fines personales.*	*Generar acceso solamente a cuentas institucionales.*

4. ANÁLISIS DE BRECHA

UNAM-Alemania (Centro de Estudios Mexicanos)		
Identificador único*	RAAC/ALE	
(Nombre del sistema A1) *	**Registro de Actividades Académicas y Culturales**	
Medida de seguridad actual*	**Medida de seguridad necesaria***	**Acciones para remediación***
Eliminar acceso a la información de las personas que ya no laboran en la dependencia	*Dar acceso a la información solamente a personal activo de la UNAM y con cuenta de correo institucional.*	*Crear accesos personalizados para personal UNAM que no trabaje con la suite de Google.*

5. PLAN DE TRABAJO

UNAM-Alemania (Centro de Estudios Mexicanos)			
Identificador único*	RAAC/ALE		
(Nombre del sistema A1) *	**Registro de Actividades Académicas y Culturales**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
No aplica	No aplica	*No aplica*	*No aplica*

6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

I. TRANSFERENCIAS DE DATOS PERSONALES

UNAM-Alemania (Centro de Estudios Mexicanos)	
Identificador único*	RAAC/ALE
(Nombre del sistema A1)*	**Registro de Actividades Académicas y Culturales**
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	**a)** No aplica
Transferencias mediante el traslado de soportes electrónicos:	**a)** No aplica
Transferencias mediante el traslado sobre redes electrónicas:	**a)** No aplica

II. RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS

1. Señalar las medidas de seguridad que ha implementado el área universitaria para el resguardo de los soportes físicos del sistema de manera que evite la alteración, pérdida o acceso no autorizado a los mismos.

No aplica

2. Señalar en un listado las personas (nombre, cargo, funciones y obligaciones) que tienen acceso a lossoportes físicos del sistema.

No aplica

III. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

1. Los datos que se registran en las bitácoras:

- **a)** Quién accede a los datos personales, fecha y hora en la que se realiza el acceso o seintenta el mismo, propósito del acceso, así como fecha y hora de salida;
- **b)** Para soportes físicos: Número o clave del expediente utilizado, y
- **c)** Para soportes electrónicos: Operaciones o acciones llevadas a cabo y registros utilizados de la base de datos.

2. Si las bitácoras están en soporte físico o en soporte electrónico;
3. Lugar dónde almacena las bitácoras y por cuánto tiempo;
4. La manera en que asegura la integridad de las bitácoras, y
5. Respecto del análisis de las bitácoras:

- **a)** Quién es el responsable de analizarlas (si es el área universitaria o si es un tercero) y cadacuándo las analiza, y
- **b)** Para el caso de que las bitácoras estén en soporte electrónico: las herramientas de análisis utilizadas.

IV. REGISTRO DE INCIDENTES:

Describir el procedimiento de atención de incidentes que tiene implementado el área universitaria y especificar si lleva registro de los incidentes relativos a soportes físicos, como lo son la pérdida o alteración no autorizada de expedientes, y para el caso de soportes electrónicos, ofrecer detalles sobre el registro de incidentes en el cual consigne los procedimientos realizados para la recuperación de los datos o para permitir la disponibilidad del proceso.

1. Los datos que registra:

- **a)** La persona que resolvió el incidente;
- **b)** La metodología aplicada;
- **c)** Para soportes físicos: Los oficios, documentos, expedientes, estantes o archiveros, tanto los dañados como los recuperados, y
- **d)** Para soportes electrónicos: Los campos, registros, tablas, bases de datos o archivos electrónicos, tanto dañados como recuperados, el nombre de los sistemas y la infraestructura afectada, indicar si el incidente afectó el servidor principal y los servidores de respaldo, etc.

2. Si el registro está en soporte físico o en soporte electrónico;
3. Cómo asegura la integridad de dicho registro, y
4. Para el caso de soportes electrónicos, quién autoriza la recuperación de datos.

V. ACCESO A LAS INSTALACIONES

1. Seguridad perimetral exterior (las instalaciones del área universitaria):

¿Qué medidas ha implementado para controlar el acceso de personas a sus instalaciones? Por ejemplo, se espera que describa si cuenta con uno o más puntos de control de acceso y quienes los operan, si tiene vigilancia las 24 horas, si ha levantado bardas o cercas, si existe un sistema de tratamiento de datos personales de video vigilancia, entre otras posibles medidas.

Las instalaciones no son propias de la Universidad. Nos encontramos dentro de un edificio de la Universidad Libre de Berlín. El acceso al edificio es abierto a toda persona de 9:00 a 20:00 h. El acceso de personas depende de la institución de educativa ya mencionada.

Para las personas que acceden a sus instalaciones:

a) No aplica
b) No aplica
c) No aplica

2. Seguridad perimetral interior (oficina, almacén o bodega para soportes físicos, centro de datos para soportes electrónicos):

¿Qué medidas de seguridad ha implementado para controlar el acceso a los espacios donde almacena los soportes físicos o electrónicos del sistema? Por ejemplo, se espera que precise el tipo de puertas y cerraduras instaladas, si tiene instalados controles biométricos, si administra la asignación de llaves y/o claves de acceso para abrir puertas y/o estantería, si cuenta con vigilancia las 24 horas, si hayun sistema de tratamiento de datos personales de video vigilancia, entre otras medidas.

El ingreso a la oficina es mediante una llave electrónica (transponder) solo el personal actual de la sede que reside en Berlín tiene acceso a la oficina, así como el personal de limpieza de la Universidad Libre de Berlín. El control de las llaves electrónicas depende de la entidad educativa ya mencionada.

Para las personas que acceden a dichos espacios interiores:

1. No aplica
2. No aplica

c) En caso de robo o extravío de datos personales, el responsable del sistema de tratamiento de datos personales, al tener conocimiento del incidente, da vista al titular de la dependencia o entidad para su conocimiento y al titular del área jurídica o aquél que tenga facultades para presentar denuncias o querellas ante el Ministerio Público para que, en el ámbito de sus atribuciones, determine lo conducente.
d) A no más de 3 días naturales de haber ocurrido el incidente, el responsable del sistema de tratamiento de datos personales da aviso al público mediante un desplegado de prensa que difunde el hecho por diversos medios, según la gravedad del caso, a escala local, regional o nacional.
e) En caso de robo o extravío de datos personales, se alerta a los titulares de los datos afectados para que tomen sus precauciones ante el posible uso ilegal de su información. Para tal efecto, el responsable del sistema de tratamiento de datos personales da aviso por escrito a dichos titulares, a

más tardar cinco días naturales de haber ocurrido el incidente, recabando el acuse de recibo de esta notificación. Adicionalmente, se da aviso por correo electrónico o por teléfono.

3. No aplica

VI. ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

En este apartado se deberá establecer un mecanismo o procedimiento institucional para la actualización de la información personal contenida en el sistema, en donde se establezca la frecuencia con la que se efectúa y la forma en que se está solicitando al titular acreditar de manera idónea sus requerimientos de rectificación de datos inexactos).

Las medidas de seguridad previstas a continuación en los incisos VII al IX, sólo aplican para soportes electrónicos

VII. PERFILES DE USUARIO Y CONTRASEÑAS

En este rubro el área universitaria deberá describir el esquema de perfiles de usuario y contraseñas que tiene implementado para control de acceso mediante una red electrónica.

No se cuenta con un esquema de perfiles de usuario y contraseñas. Toda gestión a la suite de Google se gestiona a través del departamento de TIC's de la Coordinación de Relaciones y Asuntos Internacionales.

1. Modelo de control de acceso (alguno de los siguientes):

- **a)** ¿Es obligatorio (etiquetas para objetos y acreditación para sujetos)?
- **b)** ¿Es discrecional (matriz de control de acceso)?
- **c)** ¿Está basado en roles (perfiles) o grupos?
- **d)** ¿Está basado en reglas?

2. Perfiles de usuario y contraseñas en el sistema operativo de red:

- **a)** ¿Cuenta con un sistema operativo de red instalado en sus equipos?
- **b)** ¿Proporciona dicho sistema operativo un manejo riguroso de perfiles de usuario y contraseñas?
- **c)** ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?

3. Perfiles de usuario y contraseñas manejados por el software aplicativo del sistema de tratamiento de datos personales:

- **a)** ¿Ofrece dicho software un manejo riguroso de perfiles de usuario y contraseñas?
- **b)** ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando losalmacena?

4. Administración de perfiles de usuario y contraseñas:
    a) ¿Quién da de alta nuevos perfiles?
    b) ¿Quién autoriza la creación de nuevos perfiles?
    c) ¿Se lleva registro de la creación de nuevos perfiles?

5. Acceso remoto al sistema de tratamiento de datos personales:
    a) ¿Requieren los usuarios acceso remoto al equipo de cómputo que por lo general utilizan paratrabajar con el sistema?
    b) ¿Requiere el administrador acceso remoto al equipo donde reside el sistema para realizar tareasde mantenimiento?
    c) ¿Cómo se evita el acceso remoto no autorizado?

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

1. Señalar si realiza respaldos: No se han realizado, se pretende iniciar a finales de 2022.
    a) Completos__, diferenciales_____o incrementales;
    b) De forma automática_____o Manual_,
    c) Periodicidad con que los realiza:__.
2. El tipo de medios (por ejemplo: cintas magnéticas, discos duros, CD-ROM, entre otros) queutiliza para almacenar las copias de seguridad
3. Cómo y dónde archiva esos medios, y
4. Quién es el responsable de realizar estas operaciones (el área universitaria o un tercero).

IX. PLAN DE CONTINGENCIA

No se cuenta con un plan de contingencia. Toda gestión a la suite de Google se gestiona a través del departamento de TIC's de la Coordinación de Relaciones y Asuntos Internacionales.

1. Presentar el plan de contingencia con el cual garantiza la continuidad de la operación del sistema o informar si no lo tiene, pero se encuentra desarrollándolo.
2. Si cuenta con plan de contingencia y lo ha implementado, deberá indicar si realiza pruebas de eficiencia de este.
3. Informar si cuenta con un sitio redundante (alterno) y señalar lo siguiente:
    a) El tipo de sitio (caliente, tibio o frío);
    b) Si el sitio es propio o subcontratado con un tercero;
    c) Los procedimientos, el equipo y el personal que designa para poner en marcha tal sitio y
    d) Tiempo que le lleva poner en marcha el sitio, según las pruebas de eficiencia.

Continuar los mismos pasos con el siguiente SISTEMA A2. (Nombre del sistema A2), B1. (Nombredel sistema B1), etc.

I. Transferencias de datos personales
II. Resguardo de sistemas de tratamiento de datos personales con soportes físicos
III. Bitácoras para accesos y operación cotidiana
IV. Registro de incidentes
V. Acceso a las instalaciones
VI. Actualización del sistema de tratamiento de datos personales
VII. Perfiles de usuario y contraseñas
VIII. Procedimientos de respaldo y recuperación de datos
IX. Plan de contingencia

7. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

7.1. Herramientas y recursos para monitoreo de la protección de datos personales

UNAM-Alemania (Centro de Estudios Mexicanos)		
Identificador único*	RAAC/ALE	
(Nombre del sistema A1)*	**Registro de Actividades Académicas y Culturales**	
Recurso*	**Descripción***	**Control***
No aplica	*No aplica*	*No aplica*

7.2. Procedimiento para la revisión de las medidas de seguridad

UNAM-Alemania (Centro de Estudios Mexicanos)		
Identificador único*	RAAC/ALE	
(Nombre del sistema A1)*	**Registro de Actividades Académicas y Culturales**	
Medida de seguridad*	**Procedimiento***	**Responsable***
No aplica	*aplica*	*a) No aplica*

7.3 Procedimiento para la revisión de las medidas de seguridad

UNAM-Alemania (Centro de Estudios Mexicanos)		
Identificador único*	RAAC/ALE	
(Nombre del sistema A1)*	**Registro de Actividades Académicas y Culturales**	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***
No aplica	*No aplica*	*a) No aplica*

7.4. Acciones para la corrección y actualización de las medidas de seguridad

UNAM-Alemania (Centro de Estudios Mexicanos)		
Identificador único*	RAAC/ALE	
(Nombre del sistema A1)*	**Registro de Actividades Académicas y Culturales**	
Medida de seguridad*	**Acciones***	**Responsable***
No aplica	*No aplica*	*a) No aplica*

8. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

8.1. Programa de capacitación a los responsables de tratamiento de datos personales

UNAM-Alemania (Centro de Estudios Mexicanos)			
Identificador único*	RAAC/ALE		
(Nombre del sistema A1)*	**Registro de Actividades Académicas y Culturales**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
No aplica	*No aplica*	*No aplica*	*No aplica*

8.2. Programa de difusión de la protección a los datos personales

UNAM-Alemania (Centro de Estudios Mexicanos)			
Identificador único*	RAAC/ALE		
(Nombre del sistema A1)*	**Registro de Actividades Académicas y Culturales**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
No aplica	*No aplica*	*No aplica*	*No aplica*

9. MEJORA CONTINUA

9.1. Actualización y mantenimiento de sistemas de información

UNAM-Alemania (Centro de Estudios Mexicanos)			
Identificador único*	RAAC/ALE		
(Nombre del sistema A1)*	**Registro de Actividades Académicas y Culturales**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
No aplica	*No aplica*	*No aplica*	*No aplica*

9.2. Actualización y mantenimiento de equipo de cómputo

UNAM-Alemania (Centro de Estudios Mexicanos)			
Identificador único*	RAAC/ALE		
(Nombre del sistema A1)*	**Registro de Actividades Académicas y Culturales**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
No aplica	*No aplica*	*No aplica*	*No aplica*

9.3. Procesos para la conservación, preservación y respaldos de información

UNAM-Alemania (Centro de Estudios Mexicanos)		
Identificador único*	RAAC/ALE	
(Nombre del sistema A1)*	**Registro de Actividades Académicas y Culturales**	
Proceso*	**Descripción***	**Responsable***
No aplica	*No aplica*	*a) No aplica*

9.4. Procesos de borrado seguro y disposición final de equipos y componentes informáticos

UNAM-Alemania (Centro de Estudios Mexicanos)		
Identificador único*	RAAC/ALE	
(Nombre del sistema A1)*	**Registro de Actividades Académicas y Culturales**	
Proceso*	**Descripción***	**Responsable***
No aplica	*No aplica*	*a) No aplica*

10. PROCEDIMIENTO PARA LA CANCELACIÓN DE UN SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

A) DATOS DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES QUE SERÁ CANCELADO:

No aplica

B) PLAZOS Y CONDICIONES PARA EL BLOQUEO DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES:[15]

No aplica

C) MEDIDAS DE SEGURIDAD PARA EL BLOQUEO Y POSTERIOR SUPRESIÓN DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES:

No aplica

D) PROCEDIMIENTO PARA LA SUPRESIÓN DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

No aplica

E) MECANISMOS PARA LA SUPRESIÓN DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

No aplica

11. APROBACIÓN DEL DOCUMENTO DE SEGURIDAD

		Nombre y firma de quienes revisaron el presente documento:
Responsable del desarrollo:	Andrea Guillén de la Rosa Coordinadora de Relaciones y Gestión +49 30 83852853 andrea.guillen@alemania.unam.mx	
Revisó:	José Alejandro Velázquez Montes Director +49 30 83852861 avelazquez@alemania.unam.mx	
Autorizó:	José Alejandro Velázquez Montes Director +49 30 83852861 avelazquez@alemania.unam.mx	
Fecha de aprobación:	11 de noviembre de 2022	
Fecha de actualización:	11 de noviembre de 2022	

UNAM-CHINA

CENTRO DE ESTUDIOS MEXICANOS

7.MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

7.1. Herramientas y recursos para monitoreo de la protección de datos personales

(Denominación del área específica del Área Universitaria A)*		
Identificador único*	*628.06 UNAM/Chn-AsistPart*	
(Nombre del sistema A1)*	**Sistema de registro de asistentes y participantes en las actividades académicas y culturales organizadas por la sede**	
Recurso*	**Descripción***	**Control***
Se utilizan los servicios de Google Drive y se gestionan las contraseñas con el cifrado de los buscadores Chrome, Firefox. Se utiliza VPN para acceder a los servicios.	*Se realizan pruebas de vulneración de contraseñas con las herramientas provistas por los servicios de Google.* *Se utiliza VPN para una navegación segura en la red*	*Se utiliza el sistema VPN Astrill con una licencia contratada por la Sede. Puede ser aplicable hasta 5 dispositivos al mismo tiempo.*

7.2. Procedimiento para la revisión de las medidas de seguridad

(Denominación del área específica del Área Universitaria A)*		
Identificador único*	*628.06 UNAM/Chn-AsistPart*	
(Nombre del sistema A1)*	**Sistema de registro de asistentes y participantes en las actividades académicas y culturales organizadas por la sede**	
Medida de seguridad*	**Procedimiento***	**Responsable***
Revisar acceso a espacios físicos donde se resguardan documentos con datos personales. Restringir el acceso a los documentos personales de los colaboradores de la Sede	*Corroborar que las entradas y salidas estén debidamente cerradas* *Resguardar la información con un tratamiento confidencial y corroborar que sólo los titulares y personal autorizado tenga acceso sólo para los fines que se recaba la información.*	*) Edmundo Borja, coordinador de Relaciones Institucionales y Gestión* *2 días*
Restringir acceso al correo institucional de la Sede *Restringir el acceso a las claves de las redes sociales y el manejo del sitio web*	*Corroborar que sólo tenga acceso el personal autorizado y tener autentificación de dos pasos para el uso del correo* *Corroborar que sólo tenga acceso el personal autorizado Acceder con dispositivos seguros, preferentemente evitar el uso de teléfonos móviles para reducir el riesgo de vulnerabilidad o hackeo de las cuentas institucionales.*	*) Raúl L Parra, coordinador de Comunicación y Vinculación* *1 semana*

Restringir el acceso a los listados de alumnos *Restringir el acceso a los listados de participantes en las actividades académicas y culturales*	*Corroborar que sólo tenga acceso el personal autorizado y resguardar la información en dispositivos físicos, así como en el drive de google de la UNAM-China.*	*) Pablo Mendoza, coordinador Académico y Cultural* *1 semana*

7.3. Resultados de la evaluación y pruebas a las medidas de seguridad

(Denominación del área específica del Área Universitaria A)*		
Identificador único*	*628.06 UNAM/Chn-AsistPart*	
(Nombre del sistema A1)*	**Sistema de registro de asistentes y participantes en las actividades académicas y culturales organizadas por la sede**	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***
Revisar acceso a espacios físicos donde se resguardan documentos con datos personales.	*Los accesos se encuentran de entradas y salidas se encuentran en óptimo funcionamiento. Solo personal autorizado puede ingresar al edificio donde se encuentran las oficinas, lo que reduce el riesgo de intrusiones externas*	*) Edmundo Borja, coordinador de Relaciones Institucionales y Gestión* *1 semana*
Restringir el acceso a los documentos personales de los colaboradores de la Sede	*La información se encuentra respaldada en discos duros, a los cuales tiene acceso solo el personal autorizado. Se solicita borrar correos electrónicos que contengan documentación con datos personales. Se solicita no compartir información personal a través de servicios de mensajería instantánea*	
Restringir acceso al correo institucional de la Sede	*El correo cuenta con una contraseña que cumple los estándares de seguridad recomendados. Existe un sistema automático de doble autentificación para identificar accesos que puedan vulnerar la seguridad. Se recomienda no acceder al correo con el uso de dispositivos móviles, con el fin de reducir riesgos de vulnerabilidad.* *Se otorga permisos para editar contenidos a personal*	*) Raúl L Parra, coordinador de Comunicación y Vinculación* *1 semana*

Restringir el acceso a las claves de las redes sociales y el manejo del sitio web	*autorizado, pero sólo la persona designada tiene las credenciales de administrador de las cuentas institucionales.* *Se cuenta con sistemas automatizados de doble autentificación para reducir riesgos de vulnerabilidad.*	
Restringir el acceso a los listados de alumnos *Restringir el acceso a los listados de participantes en las actividades académicas y culturales*	*La información se almacena en el equipo de cómputo de la Sede y en la nube con acceso restringido. Se respalda la información en discos duros,* *Se recomienda solicitar a las contrapartes que no envíen datos de listados que contengan nombres y datos personales por mensajería instantánea. Los listados de los participantes son principalmente estadísticos, por lo que no se contiene información personal que pueda ser de riesgo. Sólo tiene acceso a la información personal autorizado.*	*Pablo Mendoza, coordinador Académico y Cultural* *1 semana*

7.4. Acciones para la corrección y actualización de las medidas de seguridad

(Denominación del área específica del Área Universitaria A)*		
Identificador único*	*628.06 UNAM/Chn-AsistPart*	
(Nombre del sistema A1)*	**Sistema de registro de asistentes y participantes en las actividades académicas y culturales organizadas por la sede**	
Medida de seguridad*	**Acciones***	**Responsable***
Revisar acceso a espacios físicos donde se resguardan documentos con datos personales.	a) Acciones correctivas. No aplica b) Precisar las acciones preventivas. Revisar al cerrar los espacios de trabajo que las puertas y ventanas estén debidamente cerradas. Al abrir los espacios de trabajo, revisar que no exista ninguna anomalía en los accesos a los espacios de trabajo.	*) Edmundo Borja, coordinador de Relaciones Institucionales y Gestión* *1 semana*
Restringir el acceso a los documentos personales de los colaboradores de la Sede	a) Acciones correctivas. Borrar los documentos personales confidenciales que se envíen mediante correo y resguardarlos en discos duros o en los servicios de almacenamiento en la nube con acceso restringido. b) Precisar las acciones preventivas. En la medida de lo posible evitar que se mantengan los documentos confidenciales o de datos personales en formatos electrónicos en línea. Resguardar en discos duros con acceso restringido	

Restringir el acceso a los listados de alumnos *Restringir el acceso a los listados de participantes en las actividades académicas y culturales*	a) Acciones correctivas. Evitar el uso de dispositivos móviles para la recepción o transferencia de información que contenga datos personales de alumnos o participantes en las actividades académicas y culturales. Borrar la información recibida en correo electrónico para reducir riesgos de vulnerabilidad y mantener el resguardo en discos duros, así como en el drive de google de la UNAM-China. b) Precisar las acciones preventivas. No enviar ni recibir información con datos personales mediante servicios de mensajería instantánea. En caso de que se dé esta acción, se debe procurar el uso de servicios que cuenta con encriptación. *Debe darse prioridad al correo electrónico institucional como la vía para recibir y enviar información con datos personales.*	*) Pablo Mendoza, coordinador Académico y Cultural* *1 semana*

8. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

8.1. Programa de capacitación a los responsables de tratamiento de datos personales

(Denominación del área específica del Área Universitaria A)*			
Identificador único*	*628.06 UNAM/Chn-AsistPart*		
(Nombre del sistema A1)*	**Sistema de registro de asistentes y participantes en las actividades académicas y culturales organizadas por la sede**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Cursos para el manejo de datos personales impartidos por la Dirección General de Cómputo y de Tecnologías de Información y Comunicación	*La Sede participa en la red de Responsables TIC de la UNAM para recibir capacitación*	*Programa permanente a lo largo del año académico*	*Personal de la Sede*

8.2. Programa de difusión de la protección a los datos personales

(Denominación del área específica del Área Universitaria A)*			
Identificador único*	*628.06 UNAM/Chn-AsistPart*		
(Nombre del sistema A1)*	**Sistema de registro de asistentes y participantes en las actividades académicas y culturales organizadas por la sede**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Publicación del Aviso de Privacidad Integral de la Sede de la UNAM en China (Centro de Estudios Mexicanos)	*Dar a conocer al público la normativa, y el tipo de información que se recaba, así como su fin seguimiento al resguardo de las medidas de privacidad y protección de datos personales.*	*Permanente*	*Alumnos, docentes, personal de la entidad académica, conferencista o invitado externo a la Universidad (nacional o extranjero), visitante, proveedor o cliente de servicios universitarios*
Elaboración de un documento guía con las normativas para el resguardo de datos personales	*Resumen de las acciones que deben seguirse para el tratamiento, resguardo y protección de datos personales*	*Una vez con actualizaciones permanentes*	*Personal de la Sede*

9. MEJORA CONTINUA

9.1. Actualización y mantenimiento de sistemas de información

(Denominación del área específica del Área Universitaria A)*			
Identificador único*	*628.06 UNAM/Chn-AsistPart*		
(Nombre del sistema A1)*	**Sistema de registro de asistentes y participantes en las actividades académicas y culturales organizadas por la sede**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Actualizar los sistemas de cómputos con las versiones más recientes de los programas utilizados	*Con el fin de garantizar las seguridad de los sistemas informáticos, se debe actualizar de forma constantes las versiones de los programas de cómputo utilizados por la Sede*	*Permanente*	*Se resuelve de forma total el óptimo funcionamiento de los sistemas informáticos* *Se resuelve parcialmente las medidas de seguridad al utilizar los sistemas actualizados con el fin de evitar brechas de seguridad por el uso de sistemas incompatibles*

9.2. Actualización y mantenimiento de equipo de cómputo

(Denominación del área específica del Área Universitaria A)*			
Identificador único*	*628.06 UNAM/Chn-AsistPart*		
(Nombre del sistema A1)*	**Sistema de registro de asistentes y participantes en las actividades académicas y culturales organizadas por la sede**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Realizar una actualización anual de los equipos de cómputo	*Se refiere a la revisión técnica de los equipo de cómputo para optimizar su funcionamiento*	*Una semana*	*Se cubre totalmente la optimización de los equipos de cómputo*

9.3. Procesos para la conservación, preservación y respaldos de información

(Denominación del área específica del Área Universitaria A)*		
Identificador único*	*628.06 UNAM/Chn-AsistPart*	
(Nombre del sistema A1)*	**Sistema de registro de asistentes y participantes en las actividades académicas y culturales organizadas por la sede**	
Proceso*	**Descripción***	**Responsable***
Respaldo de Bases de datos e información y documentos con datos personales	*Los archivos digitales o documentos impresos deberán ser almacenados considerando medidas de seguridad para el resguardo de los datos personales.* *En el caso de documentos impresos, se almacenarán en los espacios de oficina con acceso restringido y debidamente protegidos para evitar daños relacionados con cuestiones ambientales (evitar espacios húmedos o con exposición al sol que puedan dañar los documentos).* *En el caso de las bases de datos e información digital que contenga datos personales deberá almacenarse en discos duros con acceso restringido a los usuarios de la información autorizados.* *Deberá realizarse un respaldo mensual de la información que se almacene en los servicios de nube institucionales.* *Deberán almacenarse la información en discos duros en espacios protegidos ante los cambios medioambientales*	*Coordinador de cada área que recibe y transmite información con datos personales* *a) Coordinación Académica y Cultural* *b) Coordinación de Relaciones Institucionales y Gestión* *c) Coordinación de Comunicación y Vinculación*

	(evitar espacios húmedos y exposición al sol). *Revisar anualmente el buen funcionamiento de los discos duros para detectar posibles fallos en la lectura de los mismos.*	

9.4. Procesos de borrado seguro y disposición final de equipos y componentes informáticos

(Denominación del área específica del Área Universitaria A)*		
Identificador único*	*628.06 UNAM/Chn-AsistPart*	
(Nombre del sistema A1)*	**Sistema de registro de asistentes y participantes en las actividades académicas y culturales organizadas por la sede**	
Proceso*	**Descripción***	**Responsable***
Borrado seguro de la información que contenga datos personales	*Borrado de correo electrónico. Una vez recibida información que contengan datos personales, se procederá a su borrado del correo hasta una semana después de haberla recibido. Antes de proceder al borrado, debe cerciorarse que la información ya se encuentre debidamente almacenada en el sistema de cómputo y con su debido respaldo en disco duro. Debe cerciorarse que los documentos queden eliminados también de la papelera del correo.* *Borrado de sistemas de cómputos. Una vez que haya concluido el motivo por el cual se recabó información personal, ésta deberá ser eliminada del sistema de cómputo. Deberá cerciorarse de que el documento quede borrado también en la papelera,* *Aquellos datos personales, que la Sede conserve como parte de los archivos que forman parte de la estructura institucional, (por ejemplo, los datos de los colaboradores), estos deberán conservarse en discos duros debidamente resguardados. Una vez que el prestador de servicios*	*Coordinador de cada área que recibe y transmite información con datos personales* *a) Coordinación Académica y Cultural* *b) Coordinación de Relaciones Institucionales y Gestión* *c) Coordinación de Comunicación y Vinculación.*

	ya no tenga relación con la Sede, se procederá al borrado de su información personal en un plazo no mayor a 10 diez días al momento de concluir dicha relación.	

10. PROCEDIMIENTO PARA LA CANCELACIÓN DE UN SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

(Informar y describir el procedimiento para la cancelación de un sistema de tratamiento de datos personales.)

A) DATOS DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES QUE SERÁ CANCELADO:

- **a)** Denominación
- **b)** Motivo de la cancelación

B) PLAZOS Y CONDICIONES PARA EL BLOQUEO DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES:

El bloqueo de los datos se realizará cuando proceda a su rectificación o supresión.

En el caso de rectificación, puede generarse a solicitud del titular de la información

El bloqueo para la supresión de datos personales se realizará a solicitud expresa del titular o cuando el periodo o los fines para los que se solicitó la información hayan concluido.

C) MEDIDAS DE SEGURIDAD PARA EL BLOQUEO Y POSTERIOR SUPRESIÓN DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES:

En el caso de los documentos impresos: se procederá a la supresión o destrucción total de los documentos mediante máquinas trituradoras de documentos y deberá cerciorarse de que el impreso quede debidamente destruido.

En el caso de los documentos digitales, se procederá a su eliminación en tres formas

1. Los contenidos en los sistemas en línea como correo electrónico o servicios en la nube
2. Los contenidos en los sistemas de cómputo de la oficina
3. Los contenidos en los discos duros a resguardo en la oficina.

Para cada caso deberá realizarse una doble revisión para corroborar que los documentos fueron debidamente borrados y no queden almacenados en la memoria caché de los sistemas.

D) PROCEDIMIENTO PARA LA SUPRESIÓN DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

Una vez cumplido el plazo de bloqueo se procederá a eliminar la información que contiene los datos personales tanto en formatos físicos como digitales.

E) MECANISMOS PARA LA SUPRESIÓN DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

Se realizará la supresión de la información con datos personales del sistema contenida en formato digital mediante el uso de software especializado que posea los estándares de borrado seguro.

La acción se realizará en los siguientes pasos:

1. Selección de los documentos o archivos que serán borrados
2. Registrar la información que será borrada del sistema
3. Corroborar que se haya cumplido el plazo para el borrado de datos
4. Proceder al borrado de la información
5. Registrar que la información ha sido borrada del sistema para llevar un control de los datos que ya nos están en custodia de la Sede.

11. APROBACIÓN DEL DOCUMENTO DE SEGURIDAD

		Nombre y firma de quienes revisaron el presente documento:
Responsable del desarrollo:	Nombre: Raúl López Parra Cargo: Coordinador de Comunicación y Vinculación Tel: (+86) 8881 5379 Correo electrónico: rlparra@china.unam.mx	
Revisó:	Nombre: Edmundo Borja Navarro Cargo: Coordinador de Relaciones Institucionales y Gestión Tel: (+86) 8881 5379 Correo electrónico: eborja@china.unam.mx	
	Nombre: Pablo Mendoza Ruiz Cargo: Coordinador Académico y Cultural Tel: (+86) 8881 5379 Correo electrónico: pmendoza@china.unam.mx	
Autorizó:	Nombre: Adalberto Noyola Cargo: Director Tel: (+86) 8881 5379 Correo electrónico: noyola@china.unam.mx	
Fecha de aprobación:	30 de noviembre de 2022	
Fecha de actualización:	30 de noviembre de 2022	

ANEXO II. FORMATO UNIVERSITARIO DE “SOLICITUD DE EJERCICIO DE DERECHOS ARCO”

Formato de solicitud de ejercicio de derechos Acceso, Rectificación, Cancelación y Oposición (ARCO)

Con fundamento en el artículo 54 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, esta área universitaria le solicita llenar el presente formato para ejercer sus derechos de Acceso, Rectificación, Cancelación y Oposición.

1. Datos del Área Universitaria de la UNAM responsable de tratar los datos personales*:

2. Datos del Titular de los Datos Personales*:

Primer apellido:	Segundo apellido:	Nombre(s):
CURP (para evitar homónimos):		

3. Datos del solicitante:

Primer apellido:	Segundo apellido:	Nombre(s):
Indicar si los datos corresponden a:		
☐Titular		
☐Menor de edad		
☐Persona que se encuentren en estado de interdicción o incapacidad establecida por ley.		
☐Fallecida		
Datos de identidad y representación legal (opcional, solo si usted no es el titular de los datos personales)		

☐Persona física:
☐Nombre completo del representante:
☐Representación de un menor de edad:
☐Representación de una persona que se encuentren en estado de interdicción o incapacidad establecida por ley.
☐Persona moral:
☐Nombre o razón social del representante:
Registro Federal de Contribuyentes (RFC):
Documento con el que acredita la representación:
☐Poder notarial ☐Carta poder simple signada ante dos testigos (con copia de los documentos que acrediten la identidad de los testigos y titular) ☐Declaración en comparecencia del Titular (en las instalaciones del área universitaria).

4. Documento oficial de identificación del titular o solicitante (sólo originales) *:

☐Credencial para votar (INE)	☐Pasaporte	☐Licencia de conducir
☐Cédula profesional	☐Cartilla del Servicio militar nacional	☐Documento migratorio
☐Acta de nacimiento	☐Acta de defunción	☐Otra identificación con fotografía (especifique):

5. Medio por el cual prefiere que le sea notificada la puesta a disposición de la respuesta*:

☐Acudir al área universitaria donde presentó este formato	☐Correo electrónico (especificar):

6. Modalidad en la cual prefiere le sean entregados los datos, en caso de ser procedente. *

☐Copia simple	☐Correo electrónico
☐Copia certificada	☐ Otro medio electrónico como USB/CD ROOM/ DVD *(previo depósito de ficha de pago):*
☐Consultas directas	☐Yo proporciono el medio magnético o electrónico para reproducir los datos personales.

7. Tipo de solicitud de ejercicio de Derechos Acceso, Rectificación, Cancelación y Oposición (ARCO) a datos personales*:

☐ACCESO
Describir la información datos personales que obran en posesión del área universitaria y a los que requiere tener acceso*: _____ _____ _____
Señalar el nombre y ubicación del archivo o registro de datos personales*: _____ _____ _____
☐RECTIFICACIÓN
☐Son inexactos.
☐Son incompletos.
☐Requieren ser actualizados
Justificación y documentación original que acompaña para motivar su petición*: _____ _____ _____
CANCELACIÓN (supresión o eliminación)

Causas que motivan la cancelación*:
OPOSICIÓN (cese del tratamiento)
Causas que motivan la oposición (daño o perjuicio que le causa la persistencia del tratamiento de sus datos)*:_____ _____
Señalar si es para una finalidad específica o para todos los sistemas de información que obren en el área universitaria*._____
Documentación original que acompaña para motivar su petición*: _____
Señalar la referencia o documento que facilite la localización de sus datos personales*
_____ _____

Leí el Aviso de privacidad del área universitaria a la que acudo y en este acto otorgo el consentimiento para que mis datos personales sean tratados conforme al mismo.

_____

Firma o huella dactilar*****

Plazos y procedimiento para la atención de las solicitudes de ejercicio de derechos ARCO:
Una vez que se presentó la solicitud, esta área universitaria cuenta con:

- Un plazo de 20 días hábiles, contados a partir del día siguiente a la recepción de la solicitud, para informarle si procede o no el ejercicio del derecho solicitado.
- Un plazo de 15 días hábiles, contados a partir del día siguiente en el que le haya notificado la respuesta anterior, en caso de que haya procedido el ejercicio del derecho, deberá llevar a cabo las acciones necesarias para hacerlo efectivo.

El ejercicio de los derechos ARCO será sencillo y gratuito, siempre que no rebase las 20 hojas simples, por lo que las áreas universitarias realizarán el cobro del costo de reproducción de acuerdo con los Lineamientos para la determinación de los costos de reproducción y envío en el marco de solicitudes de acceso a Información y entrega de datos personales en la Universidad Nacional Autónoma de México.

ANEXO III. CARTA DE CONFIDENCIALIDAD

Carta compromiso de confidencialidad, no divulgación, reserva y resguardo de información y datos personales

(Este documento debe firmarse por todas aquellas personas que por su empleo, cargo o comisión en la Universidad reciban y traten información confidencial de otras personas)

CIUDAD DE _____, A (DD-MM-AAAA)

(Nombre completo), *(cargo)*, adscrita(o) *(dependencia/entidad de adscripción)* de la Universidad Nacional Autónoma de México (en adelante la UNAM) acepto los términos y condiciones, que se describen más adelante, de resguardo, reserva, custodia y protección de la seguridad y confidencialidad de la información, datos personales y de todo tipo de documentos propiedad de la UNAM de los que tenga conocimiento, con motivo de las funciones que desempeño en la Universidad.

El presente compromiso me responsabiliza respecto de la información que me sea proporcionada por la UNAM, ya sea de forma oral, escrita, impresa, sonora, visual, electrónica, informática u holográfica, contenida en cualquier tipo de documento, que puede consistir en: expedientes, reportes, estudios, actas, resoluciones, oficios, correspondencia, acuerdos, directivas, directrices, circulares, contratos, convenios, instructivos, notas, memorandos, estadísticas, o bien, cualquier otro registro en medio conocido o por conocer que documente el ejercicio de las facultades, funciones y competencias del área universitaria y de los servidores universitarios, sin importar su fuente o fecha de elaboración.

La información que me sea proporcionada podría ser considerada, según el caso, como reservada, privilegiada y confidencial, en los términos de las leyes aplicables, por lo que me obligo a protegerla, reservarla, resguardarla y no divulgarla, utilizándola única y exclusivamente para llevar a cabo y cumplir con las actividades y obligaciones que expresamente me sean conferidas por la Universidad.

Es mi responsabilidad no reproducir, hacer pública o divulgar a terceros la información objeto de la presente Carta, y de cumplir con las medidas de seguridad adecuadas al tipo de documento con el que se trabaje.

Mi obligación de confidencialidad no es aplicable en los siguientes casos:

a) Cuando la información se encuentre en el dominio público en el momento en que me sea suministrada o, una vez suministrada, ésta se haga pública.
b) Cuando la legislación vigente o un mandato judicial exija su divulgación.
c) Cuando la información se desarrolle o reciba legítimamente de terceros, de forma totalmente independiente a mi relación con la Universidad.

A t e n t a m e n t e

_____
Firma o huella dactilar

ANEXO IV. RUTA CRÍTICA PARA CUMPLIMIENTO DE LAS MEDIDAS DE SEGURIDAD TÉCNICAS (MST)

A continuación, se presentan los requisitos técnicos para sistemas de información, descritos en las MST del capítulo II de las Normas Complementarias, por orden de prioridad, esto es: de los mínimos indispensables para asegurar los datos personales hasta los necesarios para incrementar la protección de dichos datos.

Dada la complejidad de diversos sistemas en la UNAM, se ha dispuesto la ruta crítica para el cumplimiento de las MST en tres etapas para los sistemas de información que a la fecha de publicación de esta guía estén en producción o funcionamiento. Todo sistema de información deberá satisfacer a cabalidad el 100% de las MST en un tiempo máximo de un año contado a partir de la publicación de las MST para conservar su registro y publicación dentro del dominio institucional.***unam.mx***.

A) **Etapa 1. Corto plazo**. Requisitos de misión crítica y mínimos indispensables para la protección de datos personales y datos personales sensibles. Cumplimiento obligatorio en menos de treinta días hábiles.
B) **Etapa 2. Mediano plazo**. Requisitos importantes para garantizar la protección de datos personales y datos personales sensibles. Ejecución estimada entre un mes y seis meses.
C) **Etapa 3. Largo plazo**. Requisitos necesarios para reforzar la seguridad en la protección de datos personales y datos personales sensibles. Ejecución estimada entre seis y doce meses.

Instrucciones

- Para cada MST se ha diseñado un formato, el cual está numerado en correspondencia con la ruta crítica de cumplimiento.
- Se deberán completar todos los formatos aplicables por cada uno de los sistemas de información a cargo del Área Universitaria.
- Todos los formatos deberán integrar el anexo del documento de seguridad de datos personales.
- En el caso de los sistemas que estén en desarrollo al momento de la publicación de las Normas complementarias, deberán cumplir con el 100% de las MST, previo a su publicación como sistema en producción.
- Es requisito indispensable el cumplimiento de las MST para conservar el registro dominio institucional ***.unam.mx*** en el caso de servicios Web.

Núm. formato	Etapa	Duración estimada	Medidas de seguridad técnicas y proceso recomendado para su cumplimiento
ETAPA 1			
Anexo I, numerales 1 y 2	1	Un día hábil	**Generar el inventario de sistemas de tratamiento de datos personales y la Estructura de descripción de los sistemas de tratamiento de datos personales.**
			A) Integrar la información correspondiente a todos los sistemas que dan tratamiento de datos personales en el área universitaria. **B)** Llenar formatos y colocar nombre y firma de quien realizó la acción.
1	1	Un día hábil	**Artículo 18. I. c) Utilizar datos no personales durante el desarrollo y pruebas de los sistemas.**
			A) Realizar respaldo completo de la base de datos. **B)** Ejecutar consulta en el sistema de información, por medio de formato o comandos. **C)** Verificar que los datos usados en el desarrollo no correspondan a personas identificables. **D)** Si se usan datos de personas identificables, cambiar por datos genéricos o datos ficticios y regresar al punto B. **E)** Si no se usan datos de personas identificables, llenar formato 1 con nombre y firma de quien realizó la acción, fecha de inicio y de conclusión.
2	1	Un día hábil	**Artículo 18. I. e) Asignar o revocar los privilegios de acceso para los usuarios teniendo como base el principio del menor privilegio.**
			A) Realizar respaldo completo de la base de datos. **B)** Ejecutar consulta en el sistema de información de la lista de usuarios y sus niveles o privilegios de acceso.

Núm. formato	Etapa	Duración estimada	Medidas de seguridad técnicas y proceso recomendado para su cumplimiento
			C) Validar que los niveles de acceso son acordes a la relación del usuario con el tratamiento de datos personales. **D)** Si hay usuarios con privilegios mayores a los que les son necesarios, cambiar al mínimo indispensable e informarlo al usuario. Regresar al punto B. **E)** Si los privilegios de acceso son correctos para los usuarios, llenar formato 2 con nombre y firma de quien realizó la acción, fecha de inicio y de conclusión.
3	1	Tres días hábiles	**Artículo 18. I. g) Instalar y mantener vigentes certificados de comunicación segura SSL en el caso de servicios basados en Web.**
			A) En caso de no tener un certificado SSL vigente, enviar correo electrónico al Departamento de Firma Electrónica de DGTIC a firma.tic@unam.mx solicitando la asignación. **B)** El Departamento de Firma Electrónica Avanzada envía procedimiento para obtención de CSR del servidor, formato de la solicitud y costos de recuperación en función del tipo de certificado requerido (organizacional, comodín o corporativo). **C)** Completar documentación, proceso y pago de costo de recuperación. Enviar comprobantes a firma.tic@unam.mx. **D)** Al recibir el certificado SSL, instalarlo en el servidor de acuerdo con las instrucciones recibidas junto con el certificado. **E)** Llenar formato 3 y colocar nombre y firma de quien realizó la acción.
4	1	Dos días hábiles	**Artículo 18. I. h) Definir el plan de respaldos de la información, incluyendo periodicidad y alcance.**
			A) Elaborar documento con la secuencia de respaldos al menos con el siguiente orden: - Diario – incremental. - Semanal – incremental. - Mensual – total.

Núm. formato	Etapa	Duración estimada	Medidas de seguridad técnicas y proceso recomendado para su cumplimiento
			B) Establecer en el plan los medios para resguardo del respaldo y su forma de identificación: - En línea: mismo equipo donde se ejecuta el sistema. - Respaldo como servicio: otro equipo de almacenamiento. - Fuera de línea: medios magnéticos (cintas, discos) y/u ópticos. **C)** Incluir en el plan: - Responsables de cada tipo y medio de respaldo. - Rotación de respaldos y medios. - Áreas de resguardo. - Métodos de cifrado. - RTO: *Recovery Time Objective*. Tiempo objetivo de recuperación. - RPO: *Recovery Point Objective*: Punto objetivo de recuperación. **D)** Concluir este documento, adjuntarlo a SGPDP, llenar formato 4 y colocar nombre y firma de quien realizó la acción.
5	1	Un día hábil	**Artículo 18. I. i) Definir el procedimiento para el borrado seguro.** **A)** Elaborar documento con el procedimiento y la herramienta para borrado seguro en función del tipo de base de datos para registros, tablas y base de datos. **B)** Incluir en el documento de borrado seguro el proceso de verificación de la no existencia del dato, generalmente por medio de consultas y de copias de respaldo. **C)** El borrado seguro debe incluirse en los respaldos incrementales y totales y en cualquiera de los medios de respaldo, así como máquinas virtuales o contenedores. **D)** Concluir este documento, adjuntarlo a SGPDP llenar formato 5 y colocar nombre y firma de quien realizó la acción.
6	1	Un día hábil	**Artículo 18. II. a) Sincronizar la fecha y hora con el servidor NTP (Network Time Protocol) oficial de la UNAM**

Núm. formato	Etapa	Duración estimada	Medidas de seguridad técnicas y proceso recomendado para su cumplimiento
			A) Realizar la verificación y configuración con privilegio de administrador del sistema operativo. **B)** En función del sistema operativo, acceder a la configuración de servidor de tiempo (NTP) en interfaz gráfica o por medio de línea de comandos. *Por ejemplo*, en el caso del sistema operativo Linux: - Verificar la existencia del archivo */etc/ntp.conf* - Editar el archivo *ntp.conf* incluyendo en la primera línea: *server ntpdgtic.redunam.unam.mx* ***ó*** *server 132.247.169.17* - Reiniciar el demonio del cliente NTP con el comando *sudo service ntp reload.* **C)** En caso de no tener el cliente NTP instalado, descargarlo del repositorio de aplicaciones del sistema operativo, instalarlo y regresar al punto B. **D)** Llenar formato 6 y colocar nombre y firma de quien realizó la acción.
7	1	Dos días hábiles	**Artículo 18. II. b) Instalar y mantener actualizado el software antimalware.** **A)** En función del sistema operativo, instalar uno o varios programas para la contención de malware. *Por ejemplo*, para el caso del sistema operativo Linux existen herramientas de código abierto y uso libre como *chkrootkit, rootkit hunter, bothunter, clamAV, avast*, entre otros, que se pueden instalar desde el repositorio correspondiente a la distribución de Linux en uso. **B)** Disponer de comandos para la localización de amenazas. *Por ejemplo*, para el caso de Linux, se recomienda usar el comando *grep* para la detección de cadenas regulares de texto en las invocaciones al *shell*. **C)** Una vez instalada la solución, verificar periódicamente su actualización. **D)** Llenar formato 7 y colocar nombre y firma de quien realizó la acción.

Núm. formato	Etapa	Duración estimada	Medidas de seguridad técnicas y proceso recomendado para su cumplimiento
8	1	Cuatro días hábiles	**Artículo 18. II. c) Instalar las actualizaciones de seguridad más recientes disponibles.** **A)** En función del sistema operativo, se debe revisar la vigencia y actualización de las herramientas de seguridad de la información. *Por ejemplo*, en el sistema operativo Linux ejecutar *apt-get update* para obtener la lista de actualizaciones, especialmente en el repositorio *security* de la respectiva distribución. **B)** Realizar un respaldo del sistema para garantizar retorno a versión anterior en caso de incompatibilidad con alguna aplicación de las actualizaciones de seguridad. **C)** Instalar las actualizaciones en el sistema operativo. **D)** Llenar formato 8 y colocar nombre y firma de quien realizó la acción.
9	1	Cuatro días hábiles	**Artículo 19. I. a) Aplicar un mecanismo de autenticación para las personas autorizadas con base en el principio del menor privilegio.** **A)** Verificar el tipo de control de acceso al sistema, esto es: a través de contraseñas, claves, identificadores, nombres de usuario, nombres de dominio, entre otros. Según sea aplicable al sistema de información en lo particular. En caso de no tener un control de acceso establecer al menos uno como: usuarios de sistema operativo, cuenta y contraseña de sistema. **B)** Revisar que los privilegios de acceso sean los adecuados en función del rol del usuario. *Por ejemplo:* el usuario de conexión a la base de datos no debe estar asignado a alguna cuenta del personal que tiene acceso al sistema. **D)** Llenar formato 9 y colocar nombre y firma de quien realizó la acción.
10	1	Dos días hábiles	**Artículo 19. II. b) Evitar la instalación de cualquier elemento de software que implique algún riesgo para el tratamiento de datos personales.**

Núm. formato	Etapa	Duración estimada	Medidas de seguridad técnicas y proceso recomendado para su cumplimiento
			A) Dependiendo del sistema operativo, configurar las actualizaciones solamente para versiones maduras o revisiones certificadas de las aplicaciones. *Por ejemplo*: en sistemas Linux desactivar la instalación de versiones *beta, test, debug, non-official.* **B)** De la lista de software instalado, verificar el consumo de recursos de aplicaciones *TSR (Terminal and Stay Resident)*. Identificar demonios que ocupen excesiva RAM o tiempo de ejecución en el procesador. *Por ejemplo*: En sistemas Windows usar el Administrador de Tareas para identificar programas de alto consumo. **C)** Desinstalar toda aquella aplicación, librería, programa, paquetería o servicio que no sea estrictamente necesario para la operación del sistema. *Por ejemplo*, si el servidor Linux no proporcionará direcciones IP, el demonio o servicio *dchpd* no debe estar instalado. **D)** Llenar formato 10 y colocar nombre y firma de quien realizó la acción.
11	1	Dos días hábiles	**Artículo 19. III. a) Establecer las medidas físicas de seguridad que controlen el acceso a los equipos.** **A)** Identificar las medidas físicas que restrinjan el acceso físico a equipos, tales como chapas, puertas, biométricos. **B)** En función de la ubicación del equipo de cómputo, hacer una relación de las condiciones más adecuadas para su protección que aún sean necesarias implementar. **C)** Establecer y seguir un plan de mejoramiento de la protección física de equipos. *Por ejemplo*; cámaras de videovigilancia, bitácoras, vigilantes, cuartos cerrados, racks con puerta y chapa, candados en equipos, bloqueo o desconexión física de puertos USB, alarmas y sensores, según sea lo más conveniente como mínimo para la protección de los datos. **D)** Llenar formato 11 y colocar nombre y firma de quien realizó la acción.
12	1	Un día hábil	**Artículo 19. III. b) Restringir la salida de equipos de las instalaciones de cada área universitaria.**

Núm. formato	Etapa	Duración estimada	Medidas de seguridad técnicas y proceso recomendado para su cumplimiento
			A) Diseñar una bitácora o formato para el registro de entrada y salida de equipos de cómputo y periféricos asociados como discos duros, cintas, unidades flash, discos ópticos, monitores, teclados, ratones y en lo general todo componente de un equipo. **B)** La bitácora de entrada y salida debe incluir el registro de número de serie e inventario UNAM. responsable de ingreso o egreso del componente y firma autorizada del responsable del área. **C)** Incluir en el procedimiento la revisión periódica (al menos una vez al mes) de la consistencia del inventario registrado contra la bitácora de entrada y salida. **D)** Llenar 12 y colocar nombre y firma de quien realizó la acción.
13	1	Tres días hábiles	**Artículo 19. IV. a) Realizar la transmisión de datos personales a través de un canal cifrado.**
			A) Identificar, mediante el administrador de aplicaciones que corresponda al sistema operativo, los protocolos y aplicaciones instalados para comunicación cifrada. *Por ejemplo*: *SFTP (Secure File Transfer Protocol), SSH (Secure Shell), SCP (Secure Copy*). **B)** Instalar con el administrador de aplicaciones o comando similar los protocolos de comunicación cifrada que sean necesarios para el tipo de transacciones y accesos del sistema. *Por ejemplo*, en el caso de requerir ejecutar comandos de forma remota en un servidor Linux, instalarlo con el comando *apt-get install openssh-server.* **C)** Activar los protocolos de comunicación encriptada en el servidor. *Por ejemplo*: en Linux con el comando *sudo systemctl enable ssh*. **D)** Llenar formato 13 y colocar nombre y firma de quien realizó la acción.
14	1	Tres días hábiles	**Artículo 20. Aplicar el procedimiento de borrado seguro que impida la recuperación en las bases de datos y todos sus respaldos.**

Núm. formato	Etapa	Duración estimada	Medidas de seguridad técnicas y proceso recomendado para su cumplimiento
			A) Realizar una copia integral del sistema de información y colocarla en un servicio temporal. *Por ejemplo:* máquina virtual o directorio temporal en el servidor. **B)** Ingresar a la copia del sistema de información y realizar el borrado de un registro. Verificar que el dato no persiste en la base de datos por medio de forma de consulta o comando. **C)** Realizar el mismo proceso del punto B para una tabla y finalmente para la base de datos completa. D) En caso de persistencia del dato, instalar y ejecutar herramientas para borrado seguro. *Por ejemplo*: en Linux se dispone *de shred, wipe, secure-delete, srm, sfill, sswap, sdmem,* que se pueden instalar desde el administrador de aplicaciones. **D)** Llenar formato 14 y colocar nombre y firma de quien realizó la acción.
ETAPA 2			
15	2	Hito	**Artículo 18. I. a) Utilizar los datos personales preexistentes que estén disponibles, de acuerdo con sus respectivas políticas de uso y acceso, en bases de datos a cargo de otras áreas universitarias.** **A)** Disponer del inventario de datos del sistema de información, esto es: documento con la descripción de tablas, campos, tipo de datos, relaciones y consultas. **B)** Con el Área Universitaria que esté identificada como la instancia autoritativa en materia de datos personales, comparar el inventario de datos. *Por ejemplo*: La Dirección General de Administración Escolar es la dependencia autoritativa en materia de datos personales de estudiantes. **C)** Establecer el acuerdo por escrito para el uso de campos específicos de datos personales de la instancia autoritativa. **D)** Establecer el mecanismo de comunicación entre el sistema de información y el de la instancia autoritativa. *Por ejemplo*: *Webservices*, transferencia *SFTP.* **E)** Llenar 15 y colocar nombre y firma de quien realizó la acción.

Núm. formato	Etapa	Duración estimada	Medidas de seguridad técnicas y proceso recomendado para su cumplimiento
16	2	Ocho días hábiles	**Artículo 18. I. d) Permitir el acceso al código fuente de los sistemas exclusivamente a la administración del sistema y personal para el desarrollo.** **A)** Recopilar el código fuente y documentación del sistema de información en todas sus versiones disponibles. **B)** Depositar en un equipo central de desarrollo todas las versiones de código fuente y su documentación (inventario de datos, manual de administración, manual de programador). **C)** Establecer control de acceso por usuario y contraseña hacia el equipo central de desarrollo. **D)** Activar bitácoras de acceso (*log*) hacia el equipo central de desarrollo. **E)** Proporcionar las credenciales de acceso al equipo central de desarrollo exclusivamente al personal a cargo de programación y mantenimiento de código y manuales. **F)** Llenar formato 16 y colocar nombre y firma de quien realizó la acción.
17	2	Cuatro días hábiles	**Artículo 19. I. b) Establecer las medidas de seguridad en los periodos de inactividad o mantenimiento.** **A)** Elaborar documento con las medidas necesarias de seguridad para períodos vacacionales, contingencias y ventanas de mantenimiento, incluyendo: control de acceso físico y lógico a los equipos, ejecución de respaldos, sistemas de alta disponibilidad (redundancia). **B)** Incluir en el documento la descripción de los procedimientos en caso de contingencia por falla de servicio de red, falla de equipo de cómputo, falla lógica en sistema operativo. **C)** Incluir en el documento el directorio de responsables de cada uno de los puntos a atender: apagado seguro, apagado fortuito, apagado programado, verificación de integridad de información, activación de servicios locales o de respaldo. **D)** Llenar formato 17 y colocar nombre y firma de quien realizó la acción.

Núm. formato	Etapa	Duración estimada	Medidas de seguridad técnicas y proceso recomendado para su cumplimiento
18	2	Ocho días hábiles	**Artículo 19. I. c) Generar respaldos y aplicar los mecanismos de control y protección para su resguardo.** **A)** De acuerdo con el plan de respaldos establecido, ejecutar la secuencia de respaldos. **B)** Designar responsables de respaldos y responsables de verificación de respaldos. **C)** Completar bitácora de control de los respaldos, indicando fecha, hora, tipo de respaldo (integral, total, parcial de registros), ejecutor y revisor del respaldo, ubicación del respaldo, medio y etiqueta. **D)** Llenar formato 18 y colocar nombre y firma de quien realizó la acción.
19	2	Veinte días hábiles	**Artículo 19. I. d) Impedir el uso de cuentas y servicios gestionados por personas físicas para el tratamiento de los datos personales.** **A)** Realizar revisión integral del sistema de información en materia de accesos, cuentas y servicios. *Por ejemplo*: En caso de consultar vía un *Webservice* a un sistema autoritativo de datos personales en la DGAE, identificar la cuenta de acceso a ese sistema. **B)** Determinar si las cuentas de acceso a servicios locales o remotos están bajo el control de la administración del sistema. *Por ejemplo*: Si la cuenta de acceso a un *Webservice* – su usuario y contraseña – está bajo el control del administrador del sistema, o si un respaldo que se realiza en un equipo remoto es con una cuenta y contraseña controlada por el administrador del sistema. **C)** Si las cuentas de acceso a servicios locales o remotos pertenecen a personas del Área Universitaria, cambiarlas por cuentas institucionales dentro del control de la instancia universitaria. *Por ejemplo*: si la identificación para acceder a un respaldo remoto es del tipo xxx@google.com, deberá cambiarse por una cuenta del tipo xxxx@unam.mx. **D)** Llenar formato 19 y colocar nombre y firma de quien realizó la acción.

Núm. formato	Etapa	Duración estimada	Medidas de seguridad técnicas y proceso recomendado para su cumplimiento
20	2	Cuatro días hábiles	**Artículo 19. II. a) Proteger ante manipulaciones indebidas y accesos no autorizados las bitácoras y los dispositivos donde se almacenan.** **A)** Elaborar una lista de las bitácoras relacionadas con el sistema de información, tanto en medio digital como físico. *Por ejemplo*: En el equipo de cómputo las bitácoras de acceso de usuarios al sistema operativo y al sistema de información (*logs*), de forma física las bitácoras de acceso al área donde está el equipo de cómputo. **B)** Junto a la lista elaborar el cronograma de revisión de integridad y respaldo de las bitácoras. *Por ejemplo*: diario, semanal, mensual. **C)** Establecer en el documento el procedimiento de resguardo de las bitácoras. *Por ejemplo*: respaldo y protección de *logs* en el caso de equipo de cómputo o zonas seguras de almacenamiento de bitácoras en papel, digitalización de registros. **D)** Llenar formato 20 y colocar nombre y firma de quien realizó la acción.
21	2	Cuatro días hábiles	**Artículo 19. IV. b) Supervisar los controles de seguridad en la red de datos donde opere el sistema para tratamiento de datos personales.** **A)** Identificar los equipos activos de red que permiten la conexión del equipo de cómputo con el sistema de información, incluyendo marca, modelo, versión de software, vigencia de mantenimiento y capacidades de protección de las comunicaciones. **B)** Determinar las reglas de seguridad físicas (acceso restringido, cuartos de telecomunicaciones) y lógicas (cuentas de acceso, puertos activos, protocolos activos) para el equipo de red. **C)** Incluir en las acciones para aseguramiento de la red de datos aquellas que sean necesarias en función de los controles actuales. Definir un plan de regularización de la seguridad en caso de ser aplicable. **D)** Mantener actualizados los equipos activos de red y con un programa de mantenimiento. **E)** Identificar y en su caso programar la instalación de equipo para seguridad perimetral de la red de datos.

Núm. formato	Etapa	Duración estimada	Medidas de seguridad técnicas y proceso recomendado para su cumplimiento
			D) Llenar formato 21 y colocar nombre y firma de quien realizó la acción.
22	2	Cuatro días hábiles	**Artículo 19. IV. c) Proporcionar el acceso exclusivamente desde redes y servicios autorizados.** **A)** Revisar los puertos de comunicación (*TCP y UDP*) que requiera el sistema de información para su operación. *Por ejemplo*: para servicios *Web* los puertos 80 y 8080 son los convencionales. **B)** Activar en el sistema operativo la herramienta correspondiente para el control de puertos de comunicación. *Por ejemplo*, en Linux puede tratarse de un *firewall* a nivel de software o las herramientas que para tal efecto contenga la distribución correspondiente del sistema operativo. **C)** Dejar activos solamente los puertos necesarios para la operación del sistema. **D)** Activar el filtrado de la comunicación por direccionamiento IP en caso de ser posible para la operación del sistema. *Por ejemplo*: Permitir el acceso al puerto de *SSH* solamente a direcciones IP en una subred de la UNAM (132.248.x.y) o a un grupo de direcciones IP específicas. **E)** Llenar formato 22 y colocar nombre y firma de quien realizó la acción.
ETAPA 3			
23	3	Veinte días hábiles	**Artículo 18. I. b) Contar con entornos para desarrollo, pruebas y operación.** **A)** Instalar y configurar equipos similares en características, preferentemente virtuales, a los equipos donde se instalará el sistema de información en su nueva o actualizada versión. **B)** Crear un repositorio en un equipo central de desarrollo para el resguardo de códigos, documentación, inventarios de datos y manuales de usuario, administrador y programador.

Núm. formato	Etapa	Duración estimada	Medidas de seguridad técnicas y proceso recomendado para su cumplimiento
			C) Ejecutar las pruebas de nuevas versiones o actualizaciones del sistema de información en el equipo dispuesto para tal efecto. Nunca usar -equipos físicos o virtuales con el sistema actualmente en producción como las plataformas para evaluación de versiones en desarrollo. **D)** Llenar formato 23 y colocar nombre y firma de quien realizó la acción.
24	3	Veinte días hábiles	**Artículo 18. I. f) Cumplir con las especificaciones de seguridad informática previo a la puesta en operación.**
			A) Una vez concluido el desarrollo o actualización de un sistema de información, solicitar al área de seguridad del Área Universitaria la revisión de seguridad informática del sistema, lo que incluye: pruebas de penetración, pruebas de estabilidad, pruebas de carga y endurecimiento de la seguridad. En caso de no contar con esa área, requerirlo a UNAM CERT al correo seguridad.tic@unam.mx . **B)** Una vez recibido el reporte del área de seguridad, aplicar las medidas de corrección que incluya el reporte. Regresar al punto A. **C)** Habiendo resuelto los hallazgos y sugerencias de mejora de la seguridad señalados por el área especializada, realizar la instalación del sistema en la plataforma definitiva de cómputo, extrayéndolo del entorno de desarrollo. **D)** Llenar formato 24 y colocar nombre y firma de quien realizó la acción.
25	3	Hito	**Artículo 18. III. a) Utilizar equipos con componentes actualizados, protegidos con garantías y soporte, y con la capacidad suficiente para atender la demanda del servicio y de los usuarios.**
			A) Elaborar una lista del inventario de los equipos de cómputo, periféricos y de almacenamiento necesarios para la ejecución del sistema de información. **B)** Determinar la razón por la que el sistema de información requerirá estar localizado en un equipo físico y no en un servidor

Núm. formato	Etapa	Duración estimada	Medidas de seguridad técnicas y proceso recomendado para su cumplimiento
			virtual. Con ello justificar una adquisición o actualización. Por ejemplo: por incompatibilidad con hipervisores, necesidades de comunicación exclusivamente locales en la entidad y dependencia o el no necesitar de un entorno de alta disponibilidad automática. **C)** Identificar en el inventario versiones, introducción en el mercado, vida útil, contratos de mantenimiento y soporte para todos y cada uno de los componentes, en el caso de emplear equipo físico. **D)** Adquirir los componentes y elementos necesarios para la actualización, vigencia de soporte y capacidad para atención a los usuarios en el equipo de cómputo físico. **E)** Llenar formato 25 y colocar nombre y firma de quien realizó la acción.
26	3	Hito	**Artículo 18. III. b) Definir el programa de mantenimiento preventivo.** **A)** De la lista de equipo de cómputo físico necesario para la operación del sistema de información, extraer las vigencias de mantenimiento. **B)** En caso de no estar en posibilidad de aplicar el mantenimiento preventivo por el personal del Área Universitaria, cotizar pólizas de mantenimiento de acuerdo con el tipo de componente, preferentemente una sola póliza para el conjunto del equipo físico. **C)** Adquirir las pólizas de mantenimiento preventivo y observar su vigencia. La vigencia no podrá ser menor de un año. **D)** Llenar formato 26 y colocar nombre y firma de quien realizó la acción.
27	3	Seis días hábiles	**Artículo 19. III. c) Aplicar el programa de mantenimiento preventivo a los equipos.** **A)** En caso de que el personal del Área Universitaria pueda realizar el mantenimiento preventivo, definir el calendario de inactividad del sistema de información, notificar a los usuarios y aplicar el plan en caso de mantenimiento o inactividad.

Núm. formato	Etapa	Duración estimada	Medidas de seguridad técnicas y proceso recomendado para su cumplimiento
			B) En caso de que sea a través de un proveedor que se proporcione el mantenimiento al equipo de cómputo, ejecutar el calendario de acciones preventivas en un período no superior a cada 3 meses hasta la conclusión del contrato o póliza respectivo. **C)** Llenar formato 27 y colocar nombre y firma de quien realizó la acción.
28	3	Hito	**Artículo 21. Solo se permitirá el uso de servicios de nube pública para el resguardo de archivos cifrados que contengan respaldos de la información.** **A)** Identificar los respaldos que se tengan resguardados en servicios de nube pública. **B)** Verificar el cifrado en cada uno de los respaldos que se almacenen en nube pública. El cifrado no deberá ser de menor capacidad al equivalente a AES de 128 bits. **C)** Llenar formato 28 y colocar nombre y firma de quien realizó la acción.

(Nombre del sistema A1)			Identificador único A1	
Formato	**1**	**Verificación anual**	**Acción concluida**	( )
Medida de seguridad técnica:	**Artículo 18. I. c) Utilizar datos no personales durante el desarrollo y pruebas de los sistemas.**			
Aplicable en:	I. Bases de datos y sistemas de tratamiento.			
Tiempo estimado:	Un día hábil.			
Importancia de la acción:	Evitar usar datos personales mientras se está desarrollando, actualizando o modificando el código fuente de un sistema de información.			
Proceso recomendado:	**A)** Realizar respaldo completo de la base de datos. **B)** Ejecutar consulta en el sistema de información, por medio de formato o comandos. **C)** Verificar que los datos usados en el desarrollo no correspondan a personas identificables. **D)** Si se usan datos de personas identificables, cambiar por datos genéricos o datos ficticios y regresar al punto B. **E)** Si no se usan datos de personas identificables, llenar formato con nombre y firma de quien realizó la acción, fecha de inicio y de conclusión.			
Mejores prácticas, referencias:	**1.-** Se recomienda al desarrollar un sistema de información no usar datos personales sino ficticios. **2.-** Se sugiere incluir en la documentación del desarrollo de un sistema de información el inventario de datos y el tipo de información de prueba.			
Conocimientos requeridos:	Administración de bases de datos. Consulta y actualización de tablas.			

Ejecución	**Fecha inicio**
Nombre y firma Programador, desarrollador o diseñador del sistema de información	**Fecha término**
Observaciones / anotaciones	

I. _____

(Nombre del sistema A1)			Identificador único A1	
Formato:	**2**	**Verificación anual**	**Acción concluida**	( )
Medidas de seguridad técnicas:	**Artículo 18. I. e) Asignar o revocar los privilegios de acceso para los usuarios teniendo como base el principio del menor privilegio.**			
Aplicable en:	I. Bases de datos y sistemas de tratamiento.			
Tiempo estimado:	Un día hábil.			
Importancia de la acción:	No se deben asignar privilegios de acceso a los usuarios en niveles que no estén relacionados con su responsabilidad en el tratamiento de datos.			
Proceso recomendado:	**A)** Realizar respaldo completo de la base de datos. **B)** Ejecutar consulta en el sistema de información de la lista de usuarios y sus niveles o privilegios de acceso. **C)** Validar que los niveles de acceso son acordes a la relación del usuario con el tratamiento de datos personales. **D)** Si hay usuarios con privilegios mayores a los que les son necesarios, cambiar al mínimo indispensable e informarlo al usuario. Regresar al punto B. **E)** Si los privilegios de acceso son correctos para los usuarios, llenar formato con nombre y firma de quien realizó la acción, fecha de inicio y de conclusión.			
Mejores prácticas, referencias:	**1.-** Definir niveles de acceso adecuados para cada perfil o tipo de usuario. **2.-** Tener un mínimo de administradores o usuarios con altos privilegios en el sistema.			
Conocimientos requeridos:	Administración de bases de datos. Consulta y actualización de usuarios.			
Ejecución			**Fecha inicio**	
Nombre y firma Administrador del sistema de información			**Fecha término**	
Observaciones / anotaciones				

(Nombre del sistema A1)			Identificador único A1	
Formato:	**3**	**Verificación anual**	**Acción concluida**	( )
Medidas de seguridad técnicas:		**Artículo 18. I. g) Instalar y mantener vigentes certificados de comunicación segura SSL en el caso de servicios basados en Web.**		
Aplicable en:		I. Bases de datos y sistemas de tratamiento.		
Tiempo estimado:		Tres días hábiles.		
Importancia de la acción:		El instalar un certificado SSL en servidores web incrementa la seguridad al encriptar la transferencia de datos y la unicidad del sitio para los usuarios.		
Proceso recomendado:		**A)** En caso de no tener un certificado SSL vigente, enviar correo electrónico al Departamento de Firma Electrónica de DGTIC a firma.tic@unam.mx solicitando la asignación. **B)** El Departamento de Firma Electrónica Avanzada envía procedimiento para obtención de CSR del servidor, formato de la solicitud y costos de recuperación en función del tipo de certificado requerido (organizacional, comodín o corporativo). **C)** Completar documentación, proceso y pago de costo de recuperación. Enviar comprobantes a firma.tic@unam.mx. **D)** Al recibir el certificado SSL, instalarlo en el servidor de acuerdo con las instrucciones recibidas junto con el certificado.		
Mejores prácticas, referencias:		**1.-** Los certificados SSL deben tener una vigencia de al menos un año. **2.-** En caso de tener varios sistemas de información bajo un mismo dominio, se recomienda obtener un certificado SSL del tipo comodín (*wildcard*). **3.-** Se debe realizar el proceso de renovación del certificado al menos 10 días hábiles antes de su vencimiento.		
Conocimientos requeridos:		Administración de sistema operativo. Administración de servicios Web.		
Ejecución			**Fecha inicio**	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término**	
Observaciones / anotaciones				

(Nombre del sistema A1)			Identificador único A1	
Formato:	**4**	**Verificación anual**	**Acción concluida**	( )
Medidas de seguridad técnicas:	**Artículo 18. I. h) Definir el plan de respaldos de la información, incluyendo periodicidad y alcance.**			
Aplicable en:	I. Bases de datos y sistemas de tratamiento.			
Tiempo estimado:	Dos días hábiles.			
Importancia de la acción:	En todo sistema de información es indispensable contar con un plan de respaldos periódicos, y especialmente en aquellos que contienen datos personales.			
Proceso recomendado:	**A)** Elaborar documento con la secuencia de respaldos al menos con el siguiente orden: - Diario – incremental. - Semanal – incremental. - Mensual – total. **B)** Establecer en el plan los medios para resguardo del respaldo y su forma de identificación: - En línea: mismo equipo donde se ejecuta el sistema. - Respaldo como servicio: otro equipo de almacenamiento. - Fuera de línea: medios magnéticos (cintas, discos) y/u ópticos. **C)** Incluir en el plan: - Responsables de cada tipo y medio de respaldo. - Rotación de respaldos y medios. - Áreas de resguardo. - Métodos de cifrado. - RTO: *Recovery Time Objective*. Tiempo objetivo de recuperación. - RPO: *Recovery Point Objective*: Punto objetivo de recuperación. **D)** Concluir este documento, adjuntarlo a SGPDP, llenar y firmar formato.			
Mejores prácticas, referencias:	**1.-** Se deben tener al menos 3 respaldos del sistema y sus bases de datos en distintos medios.			
Conocimientos requeridos:	Administración de sistema operativo. Gestión y programación de respaldos.			

Ejecución	**Fecha inicio**
Nombre y firma Administrador del sistema de información o servidor	**Fecha término**

Observaciones / anotaciones	

(Nombre del sistema A1)			Identificador único A1	
Formato:	**5**	**Verificación anual**	**Acción concluida**	( )
Medidas de seguridad técnicas:	**Artículo 18. I. i) Definir el procedimiento para el borrado seguro.**			
Aplicable en:	I. Bases de datos y sistemas de tratamiento.			
Tiempo estimado:	Un día hábil.			
Importancia de la acción:	Al igual que el procedimiento de respaldo, el borrado seguro de la información debe estar definido en cualquier sistema de información.			
Proceso recomendado:	**A)** Elaborar documento con el procedimiento y la herramienta para borrado seguro en función del tipo de base de datos para registros, tablas y base de datos. **B)** Incluir en el documento de borrado seguro el proceso de verificación de la no existencia del dato, generalmente por medio de consultas y de copias de respaldo. **C)** El borrado seguro debe incluirse en los respaldos incrementales y totales y en cualquiera de los medios de respaldo, así como máquinas virtuales o contenedores. **D)** Concluir este documento, adjuntarlo a SGPDP, llenar y firmar formato.			
Mejores prácticas, referencias:	**1.-** Para el caso de baja de equipo, se debe llenar el formato con la declaración de borrado seguro del Patronato Universitario, disponible en: http://www.patrimonio.unam.mx/patrimonio/descargas/formato_responsiva_borrado_datos.pdf **2.-** Se recomienda utilizar herramientas de borrado seguro por medio de sobre escritura aleatoria, llenado de ceros (0x00), llenado de unos o protocolos de borrado del estándar *DOD-5220.22-M*.			
Conocimientos requeridos:	Administración de sistema operativo. Comandos de borrado.			

Ejecución	**Fecha inicio**
Nombre y firma Administrador del sistema de información o servidor	**Fecha término**

Observaciones / anotaciones	

(Nombre del sistema A1)			Identificador único A1	
Formato:	**6**	**Verificación anual**	**Acción concluida**	( )
Medidas de seguridad técnicas:	**Artículo 18. II. a) Sincronizar la fecha y hora con el servidor NTP (Network Time Protocol) oficial de la UNAM**			
Aplicable en:	II. Sistemas operativos y servicios.			
Tiempo estimado:	Un día hábil.			
Importancia de la acción:	A fin de poseer información consistente, los sistemas de información deben estar sincronizados con una instancia central de tiempo, en este caso el servidor NTP de la UNAM.			
Proceso recomendado:	**A)** Realizar la verificación y configuración con privilegio de administrador del sistema operativo. **B)** En función del sistema operativo, acceder a la configuración de servidor de tiempo (NTP) en interfaz gráfica o por medio de línea de comandos. *Por ejemplo*, en el caso del sistema operativo Linux: - Verificar la existencia del archivo */etc/ntp.conf* - Editar el archivo *ntp.conf* incluyendo en la primera línea: *server ntpdgtic.redunam.unam.mx* ***ó*** *server 132.247.169.17* - Reiniciar el demonio del cliente NTP con el comando *sudo service ntp reload.* **C)** En caso de no tener el cliente NTP instalado, descargarlo del repositorio de aplicaciones del sistema operativo, instalarlo y regresar al punto B. **D)** Llenar y firmar formato.			
Mejores prácticas, referencias:	**1.-** Los servidores virtuales y contenedores hospedados en el Centro de Datos en DGTIC son configurados de origen con sincronización al servidor NTP de la UNAM. **2.-** No se deben usar otros servidores de NTP distintos al de UNAM.			
Conocimientos requeridos:	Administración de sistema operativo.			

Ejecución	**Fecha inicio**
Nombre y firma Administrador del sistema de información o servidor	**Fecha término**
Observaciones / anotaciones	

(Nombre del sistema A1)			Identificador único A1	
Formato:	**7**	**Verificación anual**	**Acción concluida**	( )
Medidas de seguridad técnicas:	**Artículo 18. II. b) Instalar y mantener actualizado el software antimalware.**			
Aplicable en:	II. Sistemas operativos y servicios.			
Tiempo estimado:	Dos días hábiles.			
Importancia de la acción:	El servidor que hospede el sistema de información debe tener protecciones instaladas para mitigar la inserción de *malware* (*rootkits, backdoors o* códigos maliciosos) que pueda alterar su operación o la integridad y seguridad de los datos.			
Proceso recomendado:	**A)** En función del sistema operativo, instalar uno o varios programas para la contención de malware. *Por ejemplo*, para el caso del sistema operativo Linux existen herramientas de código abierto y uso libre como *chkrootkit, rootkit hunter, bothunter, clamAV, avast*, entre otros, que se pueden instalar desde el repositorio correspondiente a la distribución de Linux en uso. **B)** Disponer de comandos para la localización de amenazas. *Por ejemplo*, para el caso de Linux, se recomienda usar el comando *grep* para la detección de cadenas regulares de texto en las invocaciones al *shell*. **C)** Una vez instalada la solución, verificar periódicamente su actualización **D)** Llenar y firmar formato.			
Mejores prácticas, referencias:	**1.-** UNAM-CERT puede asesorar en la selección de las herramientas *anti malware* más adecuadas para el servidor donde se aloje el sistema de información. Contactar al correo seguridad.tic@unam.mx.			
Conocimientos requeridos:	Administración de sistema operativo. Instalación de aplicaciones.			

Ejecución	**Fecha inicio**
Nombre y firma Administrador del sistema de información o servidor	**Fecha término**

Observaciones / anotaciones	

(Nombre del sistema A1)			Identificador único A1	
Formato:	**8**	**Verificación anual**	**Acción concluida**	( )
Medidas de seguridad técnicas:	**Artículo 18. II. c) Instalar las actualizaciones de seguridad más recientes disponibles.**			
Aplicable en:	II. Sistemas operativos y servicios.			
Tiempo estimado:	Cuatro días hábiles.			
Importancia de la acción:	El servidor que hospede el sistema de información debe tener vigentes todas las actualizaciones de seguridad proporcionadas por el fabricante o desarrollador del sistema operativo.			
Proceso recomendado:	**A)** En función del sistema operativo, se debe revisar la vigencia y actualización de las herramientas de seguridad de la información. *Por ejemplo*, en el sistema operativo Linux ejecutar *apt-get update* para obtener la lista de actualizaciones, especialmente en el repositorio *security* de la respectiva distribución. **B)** Realizar un respaldo del sistema para garantizar retorno a versión anterior en caso de incompatibilidad con alguna aplicación de las actualizaciones de seguridad. **C)** Instalar las actualizaciones en el sistema operativo. **D)** Llenar y firmar formato.			
Mejores prácticas, referencias:	**1.-** Debe verificarse la actualización de seguridad del sistema operativo al menos una vez a la semana y configurar la actualización o notificación inmediata en caso de complementos de seguridad urgentes.			
Conocimientos requeridos:	Administración de sistema operativo. Instalación de aplicaciones.			

Ejecución	**Fecha inicio**
Nombre y firma Administrador del sistema de información o servidor	**Fecha término**

Observaciones / anotaciones	

(Nombre del sistema A1)			Identificador único A1	
Formato:	**9**	**Verificación anual**	**Acción concluida**	( )
Medidas de seguridad técnicas:	**Artículo 19. I. a) Aplicar un mecanismo de autenticación para las personas autorizadas con base en el principio del menor privilegio.**			
Aplicable en:	I. Bases de datos y sistemas de tratamiento.			
Tiempo estimado:	Cuatro días hábiles.			
Importancia de la acción:	Partiendo de la asignación o niveles de acceso a la información con el principio del menor privilegio, debe haber en operación en el sistema al menos un mecanismo para la validación de los usuarios autorizados.			
Proceso recomendado:	**A)** Verificar el tipo de control de acceso al sistema, esto es: a través de contraseñas, claves, identificadores, nombres de usuario, nombres de dominio, entre otros. Según sea aplicable al sistema de información en lo particular. En caso de no tener un control de acceso establecer al menos uno como: usuarios de sistema operativo, cuenta y contraseña de sistema. **B)** Revisar que los privilegios de acceso sean los adecuados en función del rol del usuario. *Por ejemplo:* el usuario de conexión a la base de datos no debe estar asignado a alguna cuenta del personal que tiene acceso al sistema. **D)** Llenar y firmar formato.			
Mejores prácticas, referencias:	**1.-** Se recomienda usar un esquema estándar de acceso a sistemas que están vinculados, por ejemplo: por medio de Directorio Activo (*Active Directory*), *LDAP* u *OpenAIM.* **2.-** Las contraseñas deben ser de 12 caracteres o más con uso de signos, letras mayúsculas y minúsculas y números.			
Conocimientos requeridos:	Administración de bases de datos. Consulta y actualización de usuarios.			

Ejecución	**Fecha inicio**
Nombre y firma Administrador del sistema de información o servidor	**Fecha término**

Observaciones / anotaciones	

(Nombre del sistema A1)			Identificador único A1	
Formato:	**10**	**Verificación anual**	**Acción concluida**	( )
Medida de seguridad técnica:	**Artículo 19. II. b) Evitar la instalación de cualquier elemento de software que implique algún riesgo para el tratamiento de datos personales.**			
Aplicable en:	II. Sistemas operativos.			
Tiempo estimado:	Dos días hábiles.			
Importancia de la acción:	Por la relevancia de los sistemas de información con datos personales se debe minimizar o erradicar el riesgo de seguridad que implica instalar aplicaciones no verificadas.			
Proceso recomendado:	**A)** Dependiendo del sistema operativo, configurar las actualizaciones solamente para versiones maduras o revisiones certificadas de las aplicaciones. *Por ejemplo*: en sistemas Linux desactivar la instalación de versiones *beta, test, debug, non-official.* **B)** De la lista de software instalado, verificar el consumo de recursos de aplicaciones *TSR (Terminal and Stay Resident)*. Identificar demonios que ocupen excesiva RAM o tiempo de ejecución en el procesador. *Por ejemplo*: En sistemas Windows usar el Administrador de Tareas para identificar programas de alto consumo. **C)** Desinstalar toda aquella aplicación, librería, programa, paquetería o servicio que no sea estrictamente necesario para la operación del sistema. *Por ejemplo*, si el servidor Linux no proporcionará direcciones IP, el demonio o servicio *dchpd* no debe estar instalado. **D)** Llenar y firmar formato.			
Mejores prácticas, referencias:	**1.-** En ningún caso puede instalarse software de procedencia desconocida. Se debe impedir a los usuarios en sus privilegios de acceso instalar software o inyectar código a la aplicación del sistema de información. y se debe realizar un control estricto de los puertos de comunicación (USB, Red, etc) para evitar la extracción no autorizada de datos.			
Conocimientos requeridos:	Administración de sistema operativo. Instalación de aplicaciones.			

Ejecución	**Fecha inicio**
Nombre y firma Administrador del sistema de información o servidor	**Fecha término**
Observaciones / anotaciones	

(Nombre del sistema A1)			Identificador único A1	
Formato:	**11**	**Verificación anual**	**Acción concluida**	( )
Medidas de seguridad técnicas:	**Artículo 19. III. a) Establecer las medidas físicas de seguridad que controlen el acceso a los equipos.**			
Aplicable en:	III. Equipo de cómputo.			
Tiempo estimado:	Dos días hábiles.			
Importancia de la acción:	Además de las protecciones de tipo lógico, deben implementarse medidas de seguridad para reducir el riesgo al sistema de información por accesos físicos no autorizados.			
Proceso recomendado:	**A)** Identificar las medidas físicas que restrinjan el acceso físico a equipos, tales como chapas, puertas, biométricos. **B)** En función de la ubicación del equipo de cómputo, hacer una relación de las condiciones más adecuadas para su protección que aún sean necesarias implementar. **C)** Establecer y seguir un plan de mejoramiento de la protección física de equipos. *Por ejemplo*; cámaras de video vigilancia, bitácoras, vigilantes, cuartos cerrados, racks con puerta y chapa, candados en equipos, bloqueo o desconexión física de puertos USB, alarmas y sensores, según sea lo más conveniente como mínimo para la protección de los datos. **D)** Llenar y firmar formato.			
Mejores prácticas, referencias:	**1.-** Las medidas físicas de seguridad deben revisarse regularmente y formar parte de plan de continuidad de operaciones, así como ser del conocimiento de la Comisión local de seguridad.			
Conocimientos requeridos:	Administración de bases de datos. Consulta y actualización de usuarios.			

Ejecución	**Fecha inicio**
Nombre y firma Administrador del sistema de información o servidor	**Fecha término**
Observaciones / anotaciones	

(Nombre del sistema A1)			Identificador único A1	
Formato:	**12**	**Verificación anual**	**Acción concluida**	( )
Medidas de seguridad técnicas:	**Artículo 19. III. b) Restringir la salida de equipos de las instalaciones de cada área universitaria.**			
Aplicable en:	III. Equipo de cómputo.			
Tiempo estimado:	Un día hábil.			
Importancia de la acción:	Se debe tener un mecanismo de control para la entrada y salida de equipos de cómputo y eliminar extracciones no autorizadas.			
Proceso recomendado:	**A)** Diseñar una bitácora o formato para el registro de entrada y salida de equipos de cómputo y periféricos asociados como discos duros, cintas, unidades *flash*, discos ópticos, monitores, teclados, ratones y en lo general todo componente de un equipo. **B)** La bitácora de entrada y salida debe incluir el registro de número de serie e inventario UNAM. responsable de ingreso o egreso del componente y firma autorizada del responsable del área. **C)** Incluir en el procedimiento la revisión periódica (al menos una vez al mes) de la consistencia del inventario registrado contra la bitácora de entrada y salida. **D)** Llenar y firmar formato.			
Mejores prácticas, referencias:	**1.-** Se recomienda usar un formato estándar de control de entrada y salida de bienes proporcionado por las áreas administrativas de las entidades y dependencias y conservar una copia en el área responsable del equipo de cómputo. **2.-** En la bitácora se debe incluir la razón de la entrada o salida del equipo. En el caso de baja, se deberá firmar la declaración de borrado seguro de Patrimonio Universitario.			
Conocimientos requeridos:	Gestión de Tecnología de información, control de entrada y salida de equipo y materiales.			

Ejecución	**Fecha inicio**
Nombre y firma Administrador del sistema de información o servidor	**Fecha término**

Observaciones / anotaciones	

(Nombre del sistema A1)			Identificador único A1	
Formato:	**13**	**Verificación anual**	**Acción concluida**	( )
Medidas de seguridad técnicas:	**Artículo 19. IV. a) Realizar la transmisión de datos personales a través de un canal cifrado.**			
Aplicable en:	IV. Red de datos.			
Tiempo estimado:	Tres días hábiles.			
Importancia de la acción:	La comunicación del sistema de información con otros sistemas o servicios, así como el acceso de administración para ejecución de procesos por comandos, debe estar encriptada para evitar el envío o recepción de datos susceptibles de ser interceptados en tránsito.			
Proceso recomendado:	**A)** Identificar, mediante el administrador de aplicaciones que corresponda al sistema operativo, los protocolos y aplicaciones instalados para comunicación cifrada. *Por ejemplo*: *SFTP (Secure File Transfer Protocol), SSH (Secure Shell), SCP (Secure Copy*). **B)** Instalar con el administrador de aplicaciones o comando similar los protocolos de comunicación cifrada que sean necesarios para el tipo de transacciones y accesos del sistema. *Por ejemplo*, en el caso de requerir ejecutar comandos de forma remota en un servidor Linux, instalarlo con el comando *apt-get install openssh-server.* **C)** Activar los protocolos de comunicación encriptada en el servidor. *Por ejemplo*: en Linux con el comando *sudo systemctl enable ssh*. **D)** Llenar y firmar formato.			
Mejores prácticas, referencias:	**1.-** Se deben mantener actualizados los protocolos de comunicación por canal cifrado al igual que las utilerías de seguridad. 2.- El protocolo de comunicación cifrada requiere puertos específicos TCP, los cuales deberán estar permitidos en la configuración del equipo activo de red.			
Conocimientos requeridos:	Administración de sistema operativo. Instalación de aplicaciones. Administración de red.			

Ejecución	**Fecha inicio**
Nombre y firma Administrador del sistema de información o servidor	**Fecha término**

Observaciones / anotaciones	

(Nombre del sistema A1)			Identificador único A1	
Formato:	**14**	**Verificación anual**	**Acción concluida**	( )
Medidas de seguridad técnicas:	**Artículo 20. Aplicar el procedimiento de borrado seguro que impida la recuperación en las bases de datos y todos sus respaldos.**			
Aplicable en:	Bases de datos y sistemas de tratamiento.			
Tiempo estimado:	Tres días hábiles.			
Importancia de la acción:	Se debe verificar que el procedimiento de borrado seguro es funcional y que el dato no persiste en función del tipo de borrado (registro, tabla, base, sistema).			
Proceso recomendado:	**A)** Realizar una copia integral del sistema de información y colocarla en un servicio temporal. *Por ejemplo:* máquina virtual directorio temporal en el servidor. **B)** Ingresar a la copia del sistema de información y realizar el borrado de un registro. Verificar que el dato no persiste en la base de datos por medio de forma de consulta o comando. **C)** Realizar el mismo proceso del punto B para una tabla y finalmente para la base de datos completa. D) En caso de persistencia del dato, instalar y ejecutar herramientas para borrado seguro. *Por ejemplo*: en Linux se dispone *de shred, wipe, secure-delete, srm, sfill, sswap, sdmem,* que se pueden instalar desde el administrador de aplicaciones. **D)** Llenar y firmar este formato.			
Mejores prácticas, referencias:	**1.-** Se recomienda usar al menos un comando a nivel de sistema operativo para el borrado seguro de conformidad con el procedimiento establecido.			
Conocimientos requeridos:	Administración de sistema operativo. Instalación de aplicaciones. Gestión de archivos.			

Ejecución	**Fecha inicio**
Nombre y firma Administrador del sistema de información o servidor	**Fecha término**
Observaciones / anotaciones	

(Nombre del sistema A1)			Identificador único A1	
Formato:	**15**	**Verificación anual**	**Acción concluida**	( )
Medidas de seguridad técnicas	**Artículo 18. I. a) Utilizar los datos personales preexistentes que estén disponibles, de acuerdo con sus respectivas políticas de uso y acceso en bases de datos a cargo de otras áreas universitarias.**			
Aplicable en:	I. Bases de datos y sistemas de tratamiento.			
Tiempo estimado:	Hito.			
Importancia de la acción:	Optimizar y consolidar el uso y la protección de datos personales al hacer referencia a instancias universitarias que sean las principales responsables de su obtención, resguardo y protección.			
Proceso recomendado:	**A)** Disponer del inventario de datos del sistema de información, esto es: documento con la descripción de tablas, campos, tipo de datos, relaciones y consultas. **B)** Con la Área Universitaria que esté identificada como la instancia autoritativa en materia de datos personales, comparar el inventario de datos. *Por ejemplo*: La Dirección General de Administración Escolar es la dependencia autoritativa en materia de datos personales de estudiantes. **C)** Establecer el acuerdo por escrito para el uso de campos específicos de datos personales de la instancia autoritativa. **D)** Establecer el mecanismo de comunicación entre el sistema de información y el de la instancia autoritativa. *Por ejemplo*: *Webservices*, transferencia *SFTP.* **E)** Llenar y firmar formato.			
Mejores prácticas, referencias:	**1.-** El hacer referencia a instancias a cargo de la obtención de los datos personales y su protección se garantiza la homogeneidad de la información.			
Conocimientos requeridos:	Administración de sistema de información. Gestión de bases de datos.			

Ejecución	**Fecha inicio**
Nombre y firma Administrador del sistema de información o servidor	**Fecha término**

Observaciones / anotaciones	

(Nombre del sistema A1)			Identificador único A1	
Formato:	**16**	**Verificación anual**	**Acción concluida**	( )
Medidas de seguridad técnicas:	**Artículo 18. I. d) Permitir el acceso al código fuente de los sistemas exclusivamente a la administración del sistema y personal para el desarrollo.**			
Aplicable en:	I. Bases de datos y sistemas de tratamiento.			
Tiempo estimado:	Ocho días hábiles.			
Importancia de la acción:	Evitar el uso de códigos originales de los sistemas de información que posteriormente implique un riesgo a la seguridad de estos.			
Proceso recomendado:	**A)** Recopilar el código fuente y documentación del sistema de información en todas sus versiones disponibles. **B)** Depositar en un equipo central de desarrollo todas las versiones de código fuente y su documentación (inventario de datos, manual de administración, manual de programador). **C)** Establecer control de acceso por usuario y contraseña hacia el equipo central de desarrollo **D)** Activar bitácoras de acceso (*log*) hacia el equipo central de desarrollo. **E)** Proporcionar las credenciales de acceso al equipo central de desarrollo exclusivamente al personal a cargo de programación y mantenimiento de código y manuales. **F)** Llenar y firmar formato.			
Mejores prácticas, referencias:	**1.-** Se debe documentar todo el proceso de desarrollo y actualización de un sistema de información.			
Conocimientos requeridos:	Administración de sistema de información. Gestión de bases de datos.			

Ejecución	**Fecha inicio**
Nombre y firma Administrador del sistema de información o servidor	**Fecha término**

Observaciones / anotaciones	

(Nombre del sistema A1)			Identificador único A1	
Formato:	**17**	**Verificación anual**	**Acción concluida**	( )
Medidas de seguridad técnicas:	**Artículo 19. I. b) Establecer las medidas de seguridad en los periodos de inactividad o mantenimiento.**			
Aplicable en:	I. Bases de datos y sistemas de tratamiento.			
Tiempo estimado:	Cuatro días hábiles.			
Importancia de la acción:	Garantizar la continuidad de la operación y disponibilidad de los sistemas de información especialmente durante períodos vacacionales, contingencias o ciclos de mantenimiento.			
Proceso recomendado:	**A)** Elaborar documento con las medidas necesarias de seguridad para períodos vacacionales, contingencias y ventanas de mantenimiento, incluyendo: control de acceso físico y lógico a los equipos, ejecución de respaldos, sistemas de alta disponibilidad (redundancia). **B)** Incluir en el documento la descripción de los procedimientos en caso de contingencia por falla de servicio de red, falla de equipo de cómputo, falla lógica en sistema operativo. **C)** Incluir en el documento el directorio de responsables de cada uno de los puntos a atender: apagado seguro, apagado fortuito, apagado programado, verificación de integridad de información, activación de servicios locales o de respaldo. **D)** Llenar y firmar formato.			
Mejores prácticas, referencias:	**1.-** Las medidas de seguridad durante períodos de mantenimiento deben formar parte de un plan de continuidad de operaciones y de recuperación ante desastres (**DRP**).			
Conocimientos requeridos:	Administración de sistema de información. Administración de sistema operativo.			

Ejecución	**Fecha inicio**
Nombre y firma Administrador del sistema de información o servidor	**Fecha término**
Observaciones / anotaciones	

(Nombre del sistema A1)			Identificador único A1	
Formato:	**18**	**Verificación anual**	**Acción concluida**	( )
Medidas de seguridad técnica:	**Artículo 19. I. c) Generar respaldos y aplicar los mecanismos de control y protección para su resguardo.**			
Aplicable en:	I. Bases de datos y sistemas de tratamiento.			
Tiempo estimado:	Ocho días hábiles.			
Importancia de la acción:	Verificar que el plan de respaldos opera adecuadamente para su utilización en caso de contingencia.			
Proceso recomendado:	**A)** De acuerdo con el plan de respaldos establecido, ejecutar la secuencia de respaldos. **B)** Designar responsables de respaldos y responsables de verificación de respaldos. **C)** Completar bitácora de control de los respaldos, indicando fecha, hora, tipo de respaldo (integral, total, parcial de registros), ejecutor y revisor del respaldo, ubicación del respaldo, medio y etiqueta. **D)** Llenar y firmar formato.			
Mejores prácticas, referencias:	**1.-** La generación de respaldos, su control y protección deben formar parte de un plan de continuidad de operaciones y de recuperación ante desastres (**DRP**).			
Conocimientos requeridos:	Administración de sistema de información. Administración de sistema operativo.			

Ejecución	**Fecha inicio**
Nombre y firma Administrador del sistema de información o servidor	**Fecha término**

Observaciones / anotaciones	

(Nombre del sistema A1)			Identificador único A1	
Formato:	**19**	**Verificación anual**	**Acción concluida**	( )
Medidas de seguridad técnicas:	**Artículo 19. I. d) Impedir el uso de cuentas y servicios gestionados por personas físicas para el tratamiento de los datos personales.**			
Aplicable en:	I. Bases de datos y sistemas de tratamiento.			
Tiempo estimado:	Veinte días hábiles.			
Importancia de la acción:	Debe evitarse el riesgo que implica el depender de cuentas de control personal para acceder a servicios, fuentes de información o cualquier elemento del sistema de información que ponga en riesgo su estabilidad y confiabilidad.			
Proceso recomendado:	**A)** Realizar revisión integral del sistema de información en materia de accesos, cuentas y servicios. *Por ejemplo*: En caso de consultar vía un *Webservice* a un sistema autoritativo de datos personales en la DGAE, identificar la cuenta de acceso a ese sistema. **B)** Determinar si las cuentas de acceso a servicios locales o remotos están bajo el control de la administración del sistema. *Por ejemplo*: Si la cuenta de acceso a un *Webservice* – su usuario y contraseña – está bajo el control del administrador del sistema, o si un respaldo que se realiza en un equipo remoto es con una cuenta y contraseña controlada por el administrador del sistema. **C)** Si las cuentas de acceso a servicios locales o remotos pertenecen a personas del Área Universitaria, cambiarlas por cuentas institucionales dentro del control de la instancia universitaria. *Por ejemplo*: si la identificación para acceder a un respaldo remoto es del tipo xxx@google.com, deberá cambiarse por una cuenta del tipo xxxx@unam.mx **D)** Llenar y firmar formato.			
Mejores prácticas, referencias:	**1.-** Nunca deben usarse cuentas, servicios, suscripciones, licencias o cualquier otro elemento informático cuyo control dependa de una sola persona.			
Conocimientos requeridos:	Administración de sistema de información. Gestión de bases de datos.			

Ejecución	**Fecha inicio**
Nombre y firma Administrador del sistema de información o servidor	**Fecha término**
Observaciones / anotaciones	

(Nombre del sistema A1)			Identificador único A1	
Formato:	**20**	**Verificación anual**	**Acción concluida**	( )
Medidas de seguridad técnicas:	**Artículo 19. II. a) Proteger ante manipulaciones indebidas y accesos no autorizados las bitácoras y los dispositivos donde se almacenan.**			
Aplicable en:	II. Sistemas operativos.			
Tiempo estimado:	Cuatro días hábiles.			
Importancia de la acción:	Las bitácoras son un elemento esencial para determinar acciones que atentan contra la estabilidad del sistema de información y la protección de los datos personales.			
Proceso recomendado:	**A)** Elaborar una lista de las bitácoras relacionadas con el sistema de información, tanto en medio digital como físico. *Por ejemplo*: En el equipo de cómputo las bitácoras de acceso de usuarios al sistema operativo y al sistema de información (*logs*), de forma física las bitácoras de acceso al área donde está el equipo de cómputo. **B)** Junto a la lista elaborar el cronograma de revisión de integridad y respaldo de las bitácoras. *Por ejemplo*: diario, semanal, mensual. **C)** Establecer en el documento el procedimiento de resguardo de las bitácoras. *Por ejemplo*: respaldo y protección de *logs* en el caso de equipo de cómputo o zonas seguras de almacenamiento de bitácoras en papel, digitalización de registros. **D)** Llenar y firmar formato.			
Mejores prácticas, referencias:	**1.-** Las bitácoras digitales y en papel deben resguardarse preferentemente en una zona independiente de la ubicación del sistema de información.			
Conocimientos requeridos:	Administración de sistema de información. Administración de sistema operativo.			

Ejecución	**Fecha inicio**
Nombre y firma Administrador del sistema de información o servidor	**Fecha término**

Observaciones / anotaciones	

(Nombre del sistema A1)			Identificador único A1	
Formato:	**21**	**Verificación anual**	**Acción concluida**	( )
Norma Complementaria Técnica	**Artículo 19. IV. b) Supervisar los controles de seguridad en la red de datos donde opere el sistema para tratamiento de datos personales.**			
Aplicable en:	IV. Red de datos.			
Tiempo estimado:	Cuatro días hábiles.			
Importancia de la acción:	El control de seguridad de los equipos activos de red que suministran la conectividad al sistema de información es un elemento básico para la protección de los datos.			
Proceso recomendado:	**A)** Identificar los equipos activos de red que permiten la conexión del equipo de cómputo con el sistema de información, incluyendo marca, modelo, versión de software, vigencia de mantenimiento y capacidades de protección de las comunicaciones. **B)** Determinar las reglas de seguridad físicas (acceso restringido, cuartos de telecomunicaciones) y lógicas (cuentas de acceso, puertos activos, protocolos activos) para el equipo de red. **C)** Incluir en las acciones para aseguramiento de la red de datos aquellas que sean necesarias en función de los controles actuales. Definir un plan de regularización de la seguridad en caso de ser aplicable. **D)** Mantener actualizados los equipos activos de red y con un programa de mantenimiento. **E)** Identificar y en su caso programar la instalación de equipo para seguridad perimetral de la red de datos. **D)** Llenar y firmar formato.			
Mejores prácticas, referencias:	**1.-** Las ubicaciones físicas de los equipos activos de red deben estar protegidas con cerraduras y controles de acceso, cumplir las normas de operación y no emplearse para ningún otro equipo o uso.			
Conocimientos requeridos:	Administración de redes de datos.			
Ejecución			**Fecha inicio**	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término**	
Observaciones / anotaciones				

(Nombre del sistema A1)			Identificador único A1	
Formato:	**22**	**Verificación anual**	**Acción concluida**	( )
Medidas de seguridad técnicas:	**Artículo 19. IV. c) Proporcionar exclusivamente el acceso desde redes y servicios autorizados.**			
Aplicable en:	IV. Red de datos.			
Tiempo estimado:	Cuatro días hábiles.			
Importancia de la acción:	Es necesario reducir el mínimo necesario los puertos de comunicación para el funcionamiento del sistema de información.			
Proceso recomendado:	**A)** Revisar los puertos de comunicación (*TCP y UDP*) que requiera el sistema de información para su operación. *Por ejemplo*: para servicios *Web* los puertos 80 y 8080 son los convencionales. **B)** Activar en el sistema operativo la herramienta correspondiente para el control de puertos de comunicación. *Por ejemplo*, en Linux puede tratarse de un *firewall* a nivel de software o las herramientas que para tal efecto contenga la distribución correspondiente del sistema operativo. **C)** Dejar activos solamente los puertos necesarios para la operación del sistema. **D)** Activar el filtrado de la comunicación por direccionamiento IP en caso de ser posible para la operación del sistema. *Por ejemplo*: Permitir el acceso al puerto de *SSH* solamente a direcciones IP en una subred de la UNAM (132.248.x.y) o a un grupo de direcciones IP específicas. **E)** Llenar y firmar formato.			
Mejores prácticas, referencias:	**1.-** No se deben tener activos accesos que no son necesarios vía la red de datos.			
Conocimientos requeridos:	Administración de sistema de información. Administración de sistema operativo.			

Ejecución	**Fecha inicio**
Nombre y firma Administrador del sistema de información o servidor	**Fecha término**

Observaciones / anotaciones	

(Nombre del sistema A1)			Identificador único A1	
Formato:	**23**	**Verificación anual**	**Acción concluida**	( )
Medidas de seguridad técnicas:	**Artículo 18. I. b) Contar con entornos para desarrollo, pruebas y operación.**			
Aplicable en:	I. Bases de datos y sistemas de tratamiento.			
Tiempo estimado:	Veinte días hábiles.			
Importancia de la acción:	Para evitar riesgos innecesarios a la información, el desarrollo y actualización de los mismos deberá ser realizado siempre en una plataforma y ambientes por separado.			
Proceso recomendado:	**A)** Instalar y configurar equipos similares en características, preferentemente virtuales, a los equipos donde se instalará el sistema de información en su nueva o actualizada versión. **B)** Crear un repositorio en un equipo central de desarrollo para el resguardo de códigos, documentación, inventarios de datos y manuales de usuario, administrador y programador. **C)** Ejecutar las pruebas de nuevas versiones o actualizaciones del sistema de información en el equipo dispuesto para tal efecto. Nunca usar -equipos físicos o virtuales con el sistema actualmente en producción como las plataformas para evaluación de versiones en desarrollo. **D)** Llenar y firmar formato.			
Mejores prácticas, referencias:	**1.-** Se deben realizar respaldos de la información en los sistemas en desarrollo del mismo modo que como se realicen con el sistema en producción.			
Conocimientos requeridos:	Administración de sistema de información. Desarrollo de aplicaciones.			

Ejecución	**Fecha inicio**
Nombre y firma Administrador del sistema de información o servidor	**Fecha término**
Observaciones / anotaciones	

(Nombre del sistema A1)			Identificador único A1	
Formato:	**24**	**Verificación anual**	**Acción concluida**	( )
Medidas de seguridad técnicas:	**Artículo 18. I. f) Cumplir con las especificaciones de seguridad informática previo a la puesta en operación.**			
Aplicable en:	I. Bases de datos y sistemas de tratamiento.			
Tiempo estimado:	Veinte días hábiles.			
Importancia de la acción:	Solo los sistemas de información revisados integralmente en su seguridad y estabilidad pueden ser publicados bajo el dominio .unam.mx .			
Proceso recomendado:	**A)** Una vez concluido el desarrollo o actualización de un sistema de información, solicitar al área de seguridad del Área Universitaria la revisión de seguridad informática del sistema, lo que incluye: pruebas de penetración, pruebas de estabilidad, pruebas de carga y endurecimiento de la seguridad. En caso de no contar con esa área, requerirlo a UNAM CERT al correo seguridad.tic@unam.mx . **B)** Una vez recibido el reporte del área de seguridad, aplicar las medidas de corrección que incluya el reporte. Regresar al punto A. **C)** Habiendo resuelto los hallazgos y sugerencias de mejora de la seguridad señalados por el área especializada, realizar la instalación del sistema en la plataforma definitiva de cómputo, extrayéndolo del entorno de desarrollo. **D)** Llenar y firmar formato.			
Mejores prácticas, referencias:	**1.-** El equipo de UNAM CERT puede asesorar a las entidades y dependencias en la aplicación de las medidas de corrección y mitigación a partir de los resultados de la revisión de seguridad.			
Conocimientos requeridos:	Administración de aplicaciones. Administración de sistema operativo.			

Ejecución	**Fecha inicio**
Nombre y firma Administrador del sistema de información o servidor	**Fecha término**

Observaciones / anotaciones	

(Nombre del sistema A1)			Identificador único A1	
Formato:	**25**	**Verificación anual**	**Acción concluida**	( )
Medidas de seguridad técnicas:	**Artículo 18. III. a) Utilizar equipos con componentes actualizados, protegidos con garantías y soporte, y con la capacidad suficiente para atender la demanda del servicio y de los usuarios.**			
Aplicable en:	III. Equipos de cómputo.			
Tiempo estimado:	Hito.			
Importancia de la acción:	Mantener en adecuada condición de operación el equipo de cómputo incrementa la estabilidad y seguridad del sistema de información.			
Proceso recomendado:	**A)** Elaborar una lista del inventario de los equipos de cómputo, periféricos y de almacenamiento necesarios para la ejecución del sistema de información. **B)** Determinar la razón por la que el sistema de información requerirá estar localizado en un equipo físico y no en un servidor virtual. Con ello justificar una adquisición o actualización. Por ejemplo: por incompatibilidad con hipervisores, necesidades de comunicación exclusivamente locales en la entidad y dependencia o el no necesitar de un entorno de alta disponibilidad automática. **C)** Identificar en el inventario versiones, introducción en el mercado, vida útil, contratos de mantenimiento y soporte para todos y cada uno de los componentes, en el caso de emplear equipo físico. **D)** Adquirir los componentes y elementos necesarios para la actualización, vigencia de soporte y capacidad para atención a los usuarios en el equipo de cómputo físico. **E)** Llenar y firmar formato.			
Mejores prácticas, referencias:	**1.-** El mantenimiento preventivo debe contar con medidas de verificación.			
Conocimientos requeridos:	Administración de infraestructura.			

Ejecución	**Fecha inicio**
Nombre y firma Administrador del sistema de información o servidor	**Fecha término**

Observaciones / anotaciones	

(Nombre del sistema A1)			Identificador único A1	
Formato:	**26**	**Verificación anual**	**Acción concluida**	( )
Medidas de seguridad técnicas:	**Artículo 18. III. b) Definir el programa de mantenimiento preventivo.**			
Aplicable en:	III. Equipos de cómputo.			
Tiempo estimado:	Hito.			
Importancia de la acción:	Garantizar que el plan de mantenimiento de equipo se realiza en tiempo y forma.			
Proceso recomendado:	**A)** De la lista de equipo de cómputo físico necesario para la operación del sistema de información, extraer las vigencias de mantenimiento. **B)** En caso de no estar en posibilidad de aplicar el mantenimiento preventivo por el personal del Área Universitaria, cotizar pólizas de mantenimiento de acuerdo con el tipo de componente, preferentemente una sola póliza para el conjunto del equipo físico. **C)** Adquirir las pólizas de mantenimiento preventivo y observar su vigencia. La vigencia no podrá ser menor de un año. **D)** Llenar y firmar formato.			
Mejores prácticas, referencias:	**1.-** El programa de mantenimiento debe considerar los costos de contratos, refacciones, partes, actualizaciones y reemplazos.			
Conocimientos requeridos:	Administración de infraestructura.			

Ejecución	**Fecha inicio**
Nombre y firma Administrador del sistema de información o servidor	**Fecha término**

Observaciones / anotaciones	

(Nombre del sistema A1)			Identificador único A1	
Formato:	**27**	**Verificación anual**	**Acción concluida**	( )
Medidas de seguridad técnicas:	**Artículo 19. III. c) Aplicar el programa de mantenimiento preventivo a los equipos.**			
Aplicable en:	III. Equipos de cómputo.			
Tiempo estimado:	Seis días hábiles.			
Importancia de la acción:	Garantizar que el plan de mantenimiento de equipo se realiza en tiempo y forma.			
Proceso recomendado:	**A)** En caso de que el personal del Área Universitaria pueda realizar el mantenimiento preventivo, definir el calendario de inactividad del sistema de información, notificar a los usuarios y aplicar el plan en caso de mantenimiento o inactividad. **B)** En caso de que sea a través de un proveedor que se proporcione el mantenimiento al equipo de cómputo, ejecutar el calendario de acciones preventivas en un período no superior a cada 3 meses hasta la conclusión del contrato o póliza respectivo. **C)** Llenar y firmar formato.			
Mejores prácticas, referencias:	**1.-** Debe actualizarse el equipo de cómputo de manera suficiente para continuar la operación del sistema y considerar en el mantenimiento preventivo sistemas paralelos de manera temporal hasta la conclusión de los trabajos.			
Conocimientos requeridos:	Administración de infraestructura.			

Ejecución	**Fecha inicio**
Nombre y firma Administrador del sistema de información o servidor	**Fecha término**
Observaciones / anotaciones	

(Nombre del sistema A1)			Identificador único A1	
Formato:	**28**	**Verificación anual**	**Acción concluida**	( )
Medidas de seguridad técnicas:	**Artículo 21. Solo se permitirá el uso de servicios de nube pública para el resguardo de archivos cifrados que contengan respaldos de la información.**			
Aplicable en:	Servicios en la nube pública.			
Tiempo estimado:	Hito.			
Importancia de la acción:	No pueden conservarse o usarse datos personales que sean tratados por la UNAM en servicios de nube pública. Estos servicios sólo se permiten para el respaldo de archivos cifrados, no en producción.			
Proceso recomendado:	**A)** Identificar los respaldos que se tengan resguardados en servicios de nube pública. **B)** Verificar el cifrado en cada uno de los respaldos que se almacenen en nube pública. El cifrado no deberá ser de menor capacidad al equivalente a AES de 128 bits.			
Mejores prácticas, referencias:	**1.-** La DGTIC proporciona el servicio de respaldos en el Centro de Datos, por lo que se sugiere utilizarlo en lugar de respaldos en la nube pública.			
Conocimientos requeridos:	Administración de respaldos. Administración de sistema operativo.			

Ejecución	**Fecha inicio**
Nombre y firma Administrador del sistema de información o servidor	**Fecha término**

Observaciones / anotaciones	

UNAM-TUCSON

CENTRO DE ESTUDIOS MEXICANOS

1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES – A1 - UNAM-Tucson-SIyPCTAC

UNAM-TUCSON-628.13	
Identificador único*	**UNAM-Tucson-SIyPCTAC**
(Nombre del sistema A1) *	Sistemas de inscripción y pago a curso y talleres académicos y culturales.
Datos personales (sensibles o no) contenidos en el sistema*:	Nombre, teléfono celular o particular, situación académica actual, correo electrónico
Responsable*:	
Nombre*:	**Jesús Arnoldo Bautista Corral**
Cargo*:	**Coordinador de Relaciones y Gestión**
Funciones*:	• Definir el uso que se le dará a los datos personales de los alumnos. • Designar a los encargados del sistema que tendrán acceso a los datos personales. • Comunicar a los encargados del sistema las políticas de uso de los datos personales. • Generar los recibos de pago de los alumnos. • Redactar y enviar informes académicos y administrativos que contienen datos personales de los alumnos.
Obligaciones*:	• Asegurar la protección de datos personales contenidos en el sistema implementando medidas de seguridad. • Asegurar que no difundan los datos personales de los alumnos. • Asegurar que no se modifique la información almacenada en el servidor • Asegurar que no se realicen los respaldos de la información de datos personales.
	Encargados[1]:
(Nombre del Encargado 1*)	**Jesús Arnoldo Bautista Corral**
Cargo*:	**Coordinador de Relaciones y Gestión**
Funciones*:	• Diseñar y elaborar las bases de datos y formatos de registro de la información en la plataforma SMARTSHEETS de cada curso o taller para recabar la información de los alumnos registrados. • Apoyar en la publicación de los enlaces para acceder a los formatos de registro que llenan los alumnos interesados en los cursos.
Obligaciones*:	• Asegurar la protección de datos personales contenidos en el sistema implementando las medidas de seguridad. • Asegurar la no difusión de datos personales de los alumnos. • Asegurar que no se modifique la información almacenada en el servidor • Asegurar que no se realicen los respaldos en equipo

	personal de la información de datos personales.
(Nombre del Usuario 1*)	Judith Fuentes
Cargo*:	Asistente
Funciones*:	• Establecer comunicación con los alumnos durante el proceso de inscripción. • Validar y administrar las bases de datos que contienen los datos personales de los alumnos registrados. • Enviar los recibos de pago a los alumnos generados en la plataforma PayPal. El único dato que se utiliza para esta acción es el correo electrónico. • Recibir los comprobantes de pago de los alumnos. • Elaborar las listas de asistencia de los cursos. • Elaborar y enviar las constancias de los estudiantes de cada curso.
Obligaciones*:	• Asegurar la protección de datos personales contenidos en el sistema implementando las medidas de seguridad. • Asegurar la no difusión de datos personales de los alumnos. • Asegurar que no se modifique la información de las bases de datos almacenada en el servidor • Asegurar que no se realicen los respaldos en equipo personal de la información de datos personales.
(Nombre del Usuario 2*)	• Paola Suyette Mendieta Verdejo
Cargo*:	• Jefa del Departamento de Apoyo Académico a las sedes en el extranjero
Funciones*:	• Comprobar y la información vertida en el formato de Actividades Académicas y Culturales
Obligaciones*:	• Asegurar la protección de datos personales contenidos en el sistema implementando las medidas de seguridad. • Asegurar la no difusión de datos personales de los alumnos. • Asegurar que no se modifique la información de las bases de datos almacenada en el servidor • Asegurar que no se realicen los respaldos en equipo personal de la información de datos personales.

2. ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

UNAM-TUCSON-628.13	
Identificador único*	**UNAM-Tucson-SIyPCTAC**
(Nombre del sistema A1) *	Sistemas de inscripción y pago a curso y talleres académicos y culturales.
Tipo de soporte :*	Electrónico
Descripción*	Plataforma Digital de Administración de Base de datos (Smartsheets)
Características del lugar donde se resguardan los soportes*	• Lo soportes se resguardan en la nube privada de SmartSheets a la que solo pueden acceder usuarios autorizados por el responsable del sistema (Responsable 1). • El acceso a la Plataforma se realiza a través de equipo de cómputo de la Sede y de equipo de asistente con autorización del administrador de la plataforma SmartSheets (Responsable 1). • Las listas de asistencias y respaldo de bases de datos se manejan y respaldan en un Drive de la nube de Google Drive con acceso autorizado del Encargado1. A los instructores de cursos y/o talleres se les dé acceso a listas de asistencia que solo contienen el nombre de los alumnos y donde se coloca la información de asistencia y tareas.

3. ANÁLISIS DE RIESGOS

UNAM-TUCSON-628.13		
Identificador único*	**UNAM-Tucson-SIyPCTAC**	
(Nombre del sistema A1) *	Sistemas de inscripción y pago a curso y talleres académicos y culturales.	
Riesgo*	**Impacto***	**Mitigación***
• Acceso no autorizado a sistemas de SmartSheets o Google Drive	• Perdida de información. • Acceso y alteración de datos personales.	• Contraseñas robustas. • Mecanismos accesos. • Respaldar y borrar la información de la nube una vez concluido el curso.

4. ANÁLISIS DE BRECHA

UNAM-TUCSON-628.13		
Identificador único*	**UNAM-Tucson-SIyPCTAC**	
(Nombre del sistema A1) *	Sistemas de inscripción y pago a curso y talleres académicos y culturales.	
Medida de seguridad actual*	**Medida de seguridad necesaria***	**Acciones para remediación***
Las plataformas utilizadas para el manejo de las bases de datos (SmartSheets y Google Drive) requieren contraseñas y protocolos de seguridad robustos.	Definir contraseñas robustas y conservarlas en lugares seguros. Cambiar contraseñas con una frecuencia determinada y en forma sistemática.	Establecer un programa de capacitación a responsables, encargados y usuarios para incrementar las medidas de seguridad en el uso de las plataformas.

1. PLAN DE TRABAJO

UNAM-TUCSON-628.13			
Identificador único*	**UNAM-Tucson-SIyPCTAC**		
(Nombre del sistema A1) *	Sistemas de inscripción y pago a curso y talleres académicos y culturales.		
Actividad*	**Descripción***	**Duración***	**Cobertura***
1. Capacitación	Se realizará un proceso de capacitación sobre medidas de seguridad en el manejo de las bases de datos en las plataformas, protocolos y cuidado en el resguardos de claves de acceso.	Dos sesiones de 1 hora.	Parcial
2. Actualización de contraseñas del sistema	Se cambiarán periódicamente las contraseñas utilizadas por los responsables, encargados y usuarios del sistema.	Anual	Total
3. Eliminar información no requerida.	Eliminar información que ya no se requiere en las plataformas utilizadas.	Semestral	Total
4. Respaldar información que se requiera almacenar	Se respaldará la información que requiera almacenar en unidades de almacenamiento físico de la Sede y la información almacenada en las plataformas se eliminará de la misma.	Anual	Total

2. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

I. TRANSFERENCIAS DE DATOS PERSONALES

UNAM-TUCSON-628.13	
Identificador único*	**UNAM-Tucson-SIyPCTAC**
(Nombre del sistema A1) *	Sistemas de inscripción y pago a curso y talleres académicos y culturales.
TRANSFERENCIA DE DATOS PERSONALES	
Transferencia mediante el traslado de soportes físicos.	No aplica
Transferencias mediante el traslado de soportes electrónicos:	• Se comparte de manera digital y a través de Goole Drive la información parcial que contiene los datos personales de los alumnos con la Coordinación de Relaciones y Asuntos Internacionales como parte de la entrega de informes académicos y administrativos. • Se comparte de manera digital con los responsables de la Red Universitaria de Responsables de Internacionalización.
Transferencias mediante el traslado sobre redes electrónicas:	No aplica

II RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS

1. El sistema UNAM-Tucson-SIyPCTAC no realiza envíos de datos personales con soportes físicos, ya que se encuentran en soporte electrónico mediante el uso de plataformas de manejo de base de datos.
2. El sistema UNAM-Tucson-SIyPCTAC realiza respaldos de las bases de datos que se quieren conservar en discos duros que se conservan bajo llave por el responsable.

V. ACCESO A LAS INSTALACIONES

1. Seguridad perimetral exterior (las instalaciones del área universitaria):

La Sede de la UNAM Tucson se ubica en las instalaciones del campus de la Universidad de Arizona en la ciudad de Tucson, Arizona, las cuales no tiene ningún tipo de barreras. La seguridad perimetral exterior es gestionada por dicha institución.

2. Seguridad perimetral interior

Las oficinas de UNAM Tucson se encuentran abiertas única y exclusivamente cuando algún funcionario de la Sede o de la UA que trabaja en las instalaciones de la Sede se encuentra físicamente en las instalaciones. De lo contrario, se encuentran cerradas bajo llave y el público no tiene acceso a los espacios o mobiliario.

Para las personas que acceden a dichos espacios interiores:

1. Para acceder a las instalaciones tiene que tocar a la puerta. Al hacerlo se le pregunta a que persona quiere visitar y cuál es su asunto.
2. No se autentifica.
3. Se le autoriza el acceso a discreción de la persona que lo recibe.

VII. PERFILES DE USUARIO Y CONTRASEÑAS

En este rubro el área universitaria deberá describir el esquema de perfiles de usuario y contraseñas que tiene implementado para control de acceso mediante una red electrónica.

1. Modelo de control de acceso (alguno de los siguientes):

a) Es obligatorio (etiquetas para objetos y acreditación para sujetos). Se utiliza el sistema de Internet y de correos electrónico de la Universidad de Arizona o de la CRAI de la UNAM:

2. Perfiles de usuario y contraseñas en el sistema operativo de red:

a) ¿Cuenta con un sistema operativo de red instalado en sus equipos? Si

b) ¿Proporciona dicho sistema operativo un manejo riguroso de perfiles de usuario y contraseñas? Si

c) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena? Si

3. Perfiles de usuario y contraseñas manejados por el software aplicativo del sistema de tratamiento de datos personales:

a) ¿Ofrece dicho software un manejo riguroso de perfiles de usuario y contraseñas? Si
b) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena? Si

4. Administración de perfiles de usuario y contraseñas:

a) ¿Quién da de alta nuevos perfiles? La Universidad de Arizona
b) ¿Quién autoriza la creación de nuevos perfiles? La Universidad de Arizona
c) ¿Se lleva registro de la creación de nuevos perfiles? Si, La Universidad de Arizona.

5. Acceso remoto al sistema de tratamiento de datos personales:

a) ¿Requieren los usuarios acceso remoto al equipo de cómputo que por lo general utilizan para trabajar con el sistema? si
b) ¿Requiere el administrador acceso remoto al equipo donde reside el sistema para realizar tareas de mantenimiento? si
c) ¿Cómo se evita el acceso remoto no autorizado?A través de los protocolos de seguridad de la Universidad de Arizona

1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES – A2 – UNAM-Tucson-SPREA

UNAM-TUCSON-628.13	
Identificador único*	**UNAM-Tucson-SPREA**
(Nombre del sistema A2) *	Sistemas de preinscripción para examen de admisión
Datos personales (sensibles o no) contenidos en el sistema*:	Nombre, nacionalidad, correo electrónico, teléfono celular o particular, licenciatura, promedio bachillerato, CURP, comprobante de domicilio.
Responsable*:	
Nombre*:	**Jesús Arnoldo Bautista Corral**
Cargo*:	**Coordinador de Relaciones y Gestión**
Funciones*:	• Definir el uso que se le dará a los datos personales de los alumnos. • Designar a los encargados del sistema que tendrán acceso a los datos personales. • Comunicar a los encargados del sistema las políticas de uso de los datos personales. • Diseñar Formatos en la plataforma SmartSheets. • Redactar y enviar informes académicos y administrativos que contienen datos personales de los alumnos.
Obligaciones*:	• Asegurar la protección de datos personales contenidos en el sistema implementando medidas de seguridad. • Asegurar que no difundan los datos personales de los alumnos. • Asegurar que no se modifique la información almacenada en el servidor • Asegurar que no se realicen los respaldos de la información de datos personales.
	Encargados[2]:
(Nombre del Encargado 1*)	**Jesús Arnoldo Bautista Corral**
Cargo*:	**Coordinador de Relaciones y Gestión**
Funciones*:	• Diseñar y elaborar las bases de datos y formatos de registro de la información en la plataforma SMARTSHEETS de cada curso o taller para recabar la información de los alumnos registrados. • Apoyar en la publicación de los enlaces para acceder a los formatos de registro que llenan los alumnos interesados en los cursos.
Obligaciones*:	• Asegurar la protección de datos personales contenidos en el sistema implementando las medidas de seguridad. • Asegurar la no difusión de datos personales de los alumnos. • Asegurar que no se modifique la información almacenada en el servidor • Asegurar que no se realicen los respaldos en equipo personal de la información de datos personales.
(Nombre del Encargados/Usuarios 2,3,4,5*)	**Héctor Zavala, Eréndira Estrada, Alfredo Ávalos, Fernando, Jorge Zavala.**

Cargo*:	Encargados de apoyar los procesos de aplicación de exámenes de adminsión en cada sede.
Funciones*:	• Establecer comunicación con los alumnos durante el proceso de inscripción. • Validar y administrar las bases de datos que contienen los datos personales de los alumnos registrados. • Recibir los comprobantes de domicilio digitales y otra documentación correspondiente de los alumnos. • Elaborar las listas pre registro del examen de admisión • Proporcionar a DAGE listas e información recabada.
Obligaciones*:	• Asegurar la protección de datos personales contenidos en el sistema implementando las medidas de seguridad. • Asegurar la no difusión de datos personales de los alumnos. • Asegurar que no se modifique la información de las bases de datos almacenada en el servidor • Asegurar que no se realicen los respaldos en equipo personal de la información de datos personales.

2. ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

UNAM-TUCSON-628.13	
Identificador único*	**UNAM-Tucson-SPREA**
(Nombre del sistema A2) *	Sistemas de preinscripción para examen de admisión
Tipo de soporte :*	Electrónico
Descripción*	Plataforma Digital de Administración de Base de datos (Smartsheets)
Características del lugar donde se resguardan los soportes*	• Lo soportes se resguardan en la nube privada de SmartSheets a la que solo pueden acceder usuarios autorizados por el responsable del sistema (Responsable 1). • El acceso a la Plataforma se realiza a través de equipo de cómputo de los Encargados/Usuarios cada Sede. • Las listas de pre-registro para la aplicación de examen y respaldo de bases de datos se manejan y respaldan en un Drive de la nube de Google Drive con acceso autorizado del Encargado1. La información se proporcionará a personal autorizado de DEGE.

3. ANÁLISIS DE RIESGOS

UNAM-TUCSON-628.13		
Identificador único*	**UNAM-Tucson-SPREA**	
(Nombre del sistema A2) *	Sistemas de preinscripción para examen de admisión	
Riesgo*	**Impacto***	**Mitigación***
• Acceso no autorizado a sistemas de SmartSheets o Google Drive	• Perdida de información. • Acceso y alteración de datos personales.	• Contraseñas robustas. • Mecanismos accesos. • Respaldar y borrar la información de la nube una vez concluido el curso.

4. ANÁLISIS DE BRECHA

UNAM-TUCSON-628.13		
Identificador único*	**UNAM-Tucson-SPREA**	
(Nombre del sistema A2) *	Sistemas de preinscripción para examen de admisión	
Medida de seguridad actual*	**Medida de seguridad necesaria***	**Acciones para remediación***
Las plataformas utilizadas para el manejo de las bases de datos (SmartSheets y Google Drive) requieren contraseñas y protocolos de seguridad robustos.	Definir contraseñas robustas y conservarlas en lugares seguros. Cambiar contraseñas con una frecuencia determinada y en forma sistemática.	Establecer un programa de capacitación a responsables, encargados y usuarios para incrementar las medidas de seguridad en el uso de las plataformas.

3. PLAN DE TRABAJO

UNAM-TUCSON-628.13			
Identificador único*	**UNAM-Tucson-SPREA**		
(Nombre del sistema A2) *	Sistemas de preinscripción para examen de admisión		
Actividad*	**Descripción***	**Duración***	**Cobertura***
5. Capacitación	Se realizará un proceso de capacitación sobre medidas de seguridad en el manejo de las bases de datos en las plataformas, protocolos y cuidado en el resguardos de claves de acceso.	Dos sesiones de 1 hora.	Parcial
6. Actualización de contraseñas del sistema	Se cambiarán periódicamente las contraseñas utilizadas por los responsables, encargados y usuarios del sistema.	Anual	Total
7. Eliminar información no requerida.	Eliminar información que ya no se requiere en las	Semestral	Total

	plataformas utilizadas.		
8. Respaldar información que se requiera almacenar	Se respaldará la información que requiera almacenar en unidades de almacenamiento físico de la Sede y la información almacenada en las plataformas se eliminará de la misma.	Anual	Total

4. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

I. TRANSFERENCIAS DE DATOS PERSONALES

UNAM-TUCSON-628.13	
Identificador único*	**UNAM-Tucson-SPREA**
(Nombre del sistema A2) *	Sistemas de preinscripción para examen de admisión
TRANSFERENCIA DE DATOS PERSONALES	
Transferencia mediante el traslado de soportes físicos.	No aplica
Transferencias mediante el traslado de soportes electrónicos:	• Se comparte de manera digital y a través de Google Drive la información parcial que contiene los datos personales de los alumnos con la Coordinación de Relaciones y Asuntos Internacionales como parte de la entrega de informes académicos y administrativos. • Se comparte de manera digital con los responsables de la Red Universitaria de Responsables de Internacionalización.
Transferencias mediante el traslado sobre redes electrónicas:	No aplica

II RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS

3. El sistema **UNAM-Tucson-SPREA** no realiza envíos de datos personales con soportes físicos, ya que se encuentran en soporte electrónico mediante el uso de plataformas de manejo de base de datos.
4. El sistema **UNAM-Tucson-SPREA** realiza respaldos de las bases de datos que se quieren consrvar en discos duros que se conservan bajo llave por el responsable.

V.a. ACCESO A LAS INSTALACIONES (UNAM Tucson – UNAM Boston)

1. Seguridad perimetral exterior (las instalaciones del área universitaria):

   La Sede de la UNAM Tucson y UNAM Boston se ubica en las instalaciones del campus de la la Universidad de Massachusetts en la ciudad de Boston, Massachusetts y de Universidad de Arizona en la ciudad de Tucson, Arizona, las cuales no tiene ningún tipo de barreras. La seguridad perimetral exterior es gestionada por dicha institución.

3. Seguridad perimetral interior
   Las oficinas de UNAM Tucson y UNAM Boston se encuentran abiertas única y exclusivamente cuando algún funcionario de la Sede o de la UA que trabaja en las instalaciones de la Serde se encuentra físicamente en las instalaciones. De lo contrario, se encuentran cerradas bajo llave y el público no tiene acceso a los espacios o mobiliario.

   Para las personas que acceden a dichos espacios interiores:

   1. Para acceder a las instalaciones tiene que tocar a la puerta. Al hacerlo se le pregunta a que persona quiere visitar y cuál es su asunto.
   2. No se autentifica.
   3. Se le autoriza el acceso a discreción de la persona que lo recibe.

VII.a. PERFILES DE USUARIO Y CONTRASEÑAS (UNAM Tucson)

En este rubro el área universitaria deberá describir el esquema de perfiles de usuario y contraseñas que tiene implementado para control de acceso mediante una red electrónica.

1. Modelo de control de acceso (alguno de los siguientes):

   a) Es obligatorio (etiquetas para objetos y acreditación para sujetos). Se utliza el sistema de Internet y de correos electrónico de la Universidad de Arizona o de la CRAI de la UNAM:

2. Perfiles de usuario y contraseñas en el sistema operativo de red:

   a) ¿Cuenta con un sistema operativo de red instalado en sus equipos? Si

   b) ¿Proporciona dicho sistema operativo un manejo riguroso de perfiles de usuario y contraseñas? Si

   c) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena? Si

3. Perfiles de usuario y contraseñas manejados por el software aplicativo del sistema de tratamiento de datos personales:

   a) ¿Ofrece dicho software un manejo riguroso de perfiles de usuario y contraseñas? Si

   b) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena? Si

4. Administración de perfiles de usuario y contraseñas:

   a) ¿Quién da de alta nuevos perfiles? CRAI-UNAM

   b) ¿Quién autoriza la creación de nuevos perfiles? CRAI-UNAM

   c) ¿Se lleva registro de la creación de nuevos perfiles? Si, la CRAI UNAM

5. Acceso remoto al sistema de tratamiento de datos personales:

   a) ¿Requieren los usuarios acceso remoto al equipo de cómputo que por lo general utilizan para trabajar con el sistema? si

   b) ¿Requiere el administrador acceso remoto al equipo donde reside el sistema para realizar tareas de mantenimiento? si

   c) ¿Cómo se evita el acceso remoto no autorizado?A través de los protocolos de seguridad de la Universidad de Arizona.

1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES – A3 - UNAM-Tucson-SIEAC

UNAM-TUCSON-628.13	
Identificador único*	**UNAM-Tucson-SIEAC**
(Nombre del sistema A3) *	Sistemas de inscripción a eventos académicos y culturales
Datos personales (sensibles o no) contenidos en el sistema*:	Nombre, teléfono celular o particular, correo electrónico
Responsable*:	
Nombre*:	**Jesús Arnoldo Bautista Corral**
Cargo*:	**Coordinador de Relaciones y Gestión**
Funciones*:	• Definir el uso que se le dará a los datos personales de personas que se inscriban a participar en los eventos académico culturales. • Designar a los encargados del sistema que tendrán acceso a los datos personales. • Comunicar a los encargados del sistema las políticas de uso de los datos personales. • Redactar y enviar informes académicos y administrativos que contienen datos personales de las personas que asisten a eventos.
Obligaciones*:	• Asegurar la protección de datos personales contenidos en el sistema implementando medidas de seguridad. • Asegurar que no difundan los datos personales de las personas que asisten a eventos. • Asegurar que no se modifique la información almacenada en el servidor • Asegurar que no se realicen los respaldos de la información de datos personales.
	Encargados[3]:
(Nombre del Encargado 1*)	**Jesus Arnoldo Bautista Corral**
Cargo*:	**Coordinador de Relaciones y Gestión**
Funciones*:	• Diseñar y elaborar las bases de datos y formatos de registro de la información en la plataforma SMARTSHEETS de cada evento académico o cultural para recabar la información de los alumnos registrados. • Apoyar en la publicación de los enlaces para acceder a los formatos de registro que llenan las personas interesados en los eventos académicos o culturales.
Obligaciones*:	• Asegurar la protección de datos personales contenidos en el sistema implementando las medidas de seguridad. • Asegurar la no difusión de datos personales de las personas que asistan a los eventos. • Asegurar que no se modifique la información almacenada en el servidor • Asegurar que no se realicen los respaldos en equipo personal de la información de datos personales.
(Nombre del Usuario 1*)	Judith Fuentes

Cargo*:	Asistente
Funciones*:	• Validar y administrar las bases de datos que contienen los datos personales de los alumnos registrados. • Elaborar las listas de asistencia de los eventos si fuera necesario • Elaborar y enviar las constancias a las personas que asistieron si fuera necesario.
Obligaciones*:	• Asegurar la protección de datos personales contenidos en el sistema implementando las medidas de seguridad. • Asegurar la no difusión de datos personales de las personas que asistan a los eventos. • Asegurar que no se modifique la información de las bases de datos almacenada en el servidor • Asegurar que no se realicen los respaldos en equipo personal de la información de datos personales.

2. ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

UNAM-TUCSON-628.13	
Identificador único*	**UNAM-Tucson-SIyPCTAC**
(Nombre del sistema A1) *	Sistemas de inscripción y pago a curso y talleres académicos y culturales.
Tipo de soporte :*	Electrónico
Descripción*	Plataforma Digital de Administración de Base de datos (Smartsheet)
Características del lugar donde se resguardan los soportes*	• Lo soportes se resguardan en la nube privada de SmartSheets a la que solo pueden acceder usuarios autorizados por el responsable del sistema (Responsable 1). • El acceso a la Plataforma se realiza a través de equipo de cómputo de la Sede y de equipo de asistente con autorización del administrador de la plataforma SamrtSheets (Responsable 1). • Las listas de asistencias y respaldo de bases de datos se manejan y respaldan en un Drive de la nube de Google Drive con acceso autorizado del Encargado1. A los instructores de cursos y/o talleres se les dé acceso a listas de asistencia que solo contienen el nombre de los alumnos y donde se coloca la información de asistencia y tareas.

3. ANÁLISIS DE RIESGOS

UNAM-TUCSON-628.13		
Identificador único*	**UNAM-Tucson-SIEAC**	
(Nombre del sistema A3) *	Sistemas de inscripción a eventos académicos y culturales	
Riesgo*	**Impacto***	**Mitigación***
• Acceso no autorizado a sistemas de SmartSheets o Google Drive	• Perdida de información. • Acceso y alteración de datos personales.	• Contraseñas robustas. • Mecanismos accesos. • Respaldar y borrar la información de la nube una vez concluido el curso.

4. ANÁLISIS DE BRECHA

UNAM-TUCSON-628.13		
Identificador único*	**UNAM-Tucson-SIEAC**	
(Nombre del sistema A3) *	Sistemas de inscripción a eventos académicos y culturales	
Medida de seguridad actual*	**Medida de seguridad necesaria***	**Acciones para remediación***
Las plataformas utilizadas para el manejo de las bases de datos (SmartSheets y Google Drive) requieren contraseñas y protocolos de seguridad robustos.	Definir contraseñas robustas y conservarlas en lugares seguros. Cambiar contraseñas con una frecuencia determinada y en forma sistemática.	Establecer un programa de capacitación a responsables, encargados y usuarios para incrementar las medidas de seguridad en el uso de las plataformas.

5. PLAN DE TRABAJO

UNAM-TUCSON-628.13			
Identificador único*	**UNAM-Tucson-SIEAC**		
(Nombre del sistema A3) *	Sistemas de inscripción a eventos académicos y culturales		
Actividad*	**Descripción***	**Duración***	**Cobertura***
9. Capacitación	Se realizará un proceso de capacitación sobre medidas de seguridad en el manejo de las bases de datos en las plataformas, protocolos y cuidado en el resguardos de claves de acceso.	Dos sesiones de 1 hora.	Parcial
10. Actualización de contraseñas del sistema	Se cambiarán periódicamente las contraseñas utilizadas por los responsables, encargados y usuarios del sistema.	Anual	Total
11. Eliminar información no requerida.	Eliminar información que ya no se requiere en las plataformas utilizadas.	Semestral	Total
12. Respaldar información que se requiera almacenar	Se respaldará la información que requiera almacenar en unidades de almacenamiento físico de la Sede y la información almacenada en las plataformas se eliminará de la misma.	Anual	Total

6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

I. TRANSFERENCIAS DE DATOS PERSONALES

UNAM-TUCSON-628.13	
Identificador único*	**UNAM-Tucson-SIEAC**
(Nombre del sistema A3) *	Sistemas de inscripción a eventos académicos y culturales
TRANSFERENCIA DE DATOS PERSONALES	
Transferencia mediante el traslado de soportes físicos.	No aplica
Transferencias mediante el traslado de soportes electrónicos:	• Si fuera necesario se comparte de manera digital y a través de Google Drive la información parcial que contiene los datos personales de las personas con la Coordinación de Relaciones y Asuntos Internacionales como parte de la entrega de informes académicos y administrativos.
Transferencias mediante el traslado sobre redes electrónicas:	No aplica

II RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS

5. El sistema UNAM-Tucson-SIyPCTAC no realiza envíos de datos personales con soportes físicos, ya que se encuentran en soporte electrónico mediante el uso de plataformas de manejo de base de datos.
6. El sistema UNAM-Tucson-SIyPCTAC realiza respaldos de las bases de datos que se quieren conservar en discos duros que se conservan bajo llave por el responsable.

V. ACCESO A LAS INSTALACIONES

1. Seguridad perimetral exterior (las instalaciones del área universitaria):

La Sede de la UNAM Tucson se ubica en las instalaciones del campus de la Universidad de Arizona en la ciudad de Tucson, Arizona, las cuales no tiene ningún tipo de barreras. La seguridad perimetral exterior es gestionada por dicha institución.

4. Seguridad perimetral interior

Las oficinas de UNAM Tucson se encuentran abiertas única y exclusivamente cuando algún funcionario de la Sede o de la UA que trabaja en las instalaciones de la Sede se encuentra físicamente en las instalaciones. De lo contrario, se encuentran cerradas bajo llave y el público no tiene acceso a los espacios o mobiliario.

Para las personas que acceden a dichos espacios interiores:

1. Para acceder a las instalaciones tiene que tocar a la puerta. Al hacerlo se le pregunta a que persona quiere visitar y cuál es su asunto.
2. No se autentifica.
3. Se le autoriza el acceso a discreción de la persona que lo recibe.

VII. PERFILES DE USUARIO Y CONTRASEÑAS

En este rubro el área universitaria deberá describir el esquema de perfiles de usuario y contraseñas que tiene implementado para control de acceso mediante una red electrónica.

1. Modelo de control de acceso (alguno de los siguientes):

a) Es obligatorio (etiquetas para objetos y acreditación para sujetos). Se utiliza el sistema de Internet y de correos electrónico de la Universidad de Arizona o de la CRAI de la UNAM:

2. Perfiles de usuario y contraseñas en el sistema operativo de red:

a) ¿Cuenta con un sistema operativo de red instalado en sus equipos? Si

b) ¿Proporciona dicho sistema operativo un manejo riguroso de perfiles de usuario y contraseñas? Si

c) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena? Si

3. Perfiles de usuario y contraseñas manejados por el software aplicativo del sistema de tratamiento de datos personales:

   a) ¿Ofrece dicho software un manejo riguroso de perfiles de usuario y contraseñas? Si
   b) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena? Si

4. Administración de perfiles de usuario y contraseñas:

   a) ¿Quién da de alta nuevos perfiles? CRAI-UNAM
   b) ¿Quién autoriza la creación de nuevos perfiles? CRAI-UNAM
   c) ¿Se lleva registro de la creación de nuevos perfiles? Si, CRAI-UNAM

5. Acceso remoto al sistema de tratamiento de datos personales:

   a) ¿Requieren los usuarios acceso remoto al equipo de cómputo que por lo general utilizan para trabajar con el sistema? si
   b) ¿Requiere el administrador acceso remoto al equipo donde reside el sistema para realizar tareas de mantenimiento? si
   c) ¿Cómo se evita el acceso remoto no autorizado? A través de los protocolos de seguridad de la Universidad de Arizona.

1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES – A4 - UNAM-Tucson-SSIAAPM

UNAM-TUCSON-628.13	
Identificador único*	**UNAM-Tucson-SSIAAPM**
(Nombre del sistema A4) *	Sistemas de administración de información de académicos o alumnos de programas de movilidad.
Datos personales (sensibles o no) contenidos en el sistema*:	Nombre, número de cuenta de la UNAM, correo electrónico, dirección particular, historial académico, pasaporte, número telefónico, Estados de cuenta de bancos.
Responsable*:	
Nombre*:	**Jesús Arnoldo Bautista Corral**
Cargo*:	**Coordinador de Relaciones y Gestión**
Funciones*:	• Definir el uso que se le dará a los datos personales de los académicos y/o alumnos en programas de movilidad. • Designar a los encargados del sistema que tendrán acceso a los datos personales. • Comunicar a los encargados del sistema las políticas de uso de los datos personales. • Redactar y enviar informes académicos y administrativos que contienen datos personales de los académicos o alumnos.
Obligaciones*:	• Asegurar la protección de datos personales contenidos en el sistema implementando medidas de seguridad. • Asegurar que no difundan los datos personales de los académicos o los alumnos. • Asegurar que no se modifique la información almacenada en el servidor • Asegurar que no se realicen los respaldos de la información de datos personales.
	Encargados[4]:
(Nombre del Encargado 1*)	**Jesús Arnoldo Bautista Corral**
Cargo*:	**Coordinador de Relaciones y Gestión**
Funciones*:	• Diseñar y elaborar las bases de datos y formatos de registro de la información en la plataforma DROPBOX de cada expediente para recabar la información de los académicos o alumnos en los programas de movilidad. . • Apoyar en la publicación de los enlaces para acceder a los formatos de registro que llenan los académicos y/o alumnos participantes en los programas de movilidad.
Obligaciones*:	• Asegurar la protección de datos personales contenidos en el sistema implementando las medidas de seguridad. • Asegurar la no difusión de datos personales de los académicos y/o de los alumnos en los programas de movilidad. • Asegurar que no se modifique la información almacenada en el servidor • Asegurar que no se realicen los respaldos en equipo personal de la información de datos personales.

(Nombre del Usuario 1*)	Alma Fuentes
Cargo*:	Asistente
Funciones*:	• Establecer comunicación con los alumnos durante el proceso de integración del expediente. • Validar y administrar las bases de datos que contienen los datos personales de los académicos y/o alumnos en programas de movilidad. • Revisar expediente y ponerlos a punto para revisión de la Universidad de Arizona para generar formato DS2019 para trámite de visas F1 o J1
Obligaciones*:	• Asegurar la protección de datos personales contenidos en el sistema implementando las medidas de seguridad. • Asegurar la no difusión de datos personales de los alumnos. • Asegurar que no se modifique la información de las bases de datos almacenada en el servidor • Asegurar que no se realicen los respaldos en equipo personal de la información de datos personales.
(Nombre del Usuario 2*)	Brittney Robinson
Cargo*:	Coordinator, Special Programs Arizona International, University of Arizona.
Funciones*:	• Confirmar que el expediente esté completo para emitir el formato DS2019 para con él solicitar visas F1 o J1 ante la Embajada o Consulado correspondiente de EUA.
Obligaciones*:	• Asegurar la protección de datos personales contenidos en el sistema implementando las medidas de seguridad. • Asegurar la no difusión de datos personales de los alumnos. • Asegurar que no se modifique la información de las bases de datos almacenada en el servidor • Asegurar que no se realicen los respaldos en equipo personal de la información de datos personales.

2. ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

UNAM-TUCSON-628.13	
Identificador único*	**UNAM-Tucson-SSIAAPM**
(Nombre del sistema A4) *	Sistemas de administración de información de académicos o alumnos de programas de movilidad.
Tipo de soporte :*	Electrónico
Descripción*	Plataforma Digital de Almacenaje de Base de datos (DROPBOX)
Características del lugar donde se resguardan los soportes*	• Lo soportes se resguardan en la nube privada de DROPBOX a la que solo pueden acceder usuarios autorizados por el responsable del sistema (Responsable 1). • El acceso a la Plataforma se realiza a través de equipo de cómputo de la Sede y de equipo de asistente con autorización del administrador de la plataforma DROPBOX(Responsable 1).

3. ANÁLISIS DE RIESGOS

UNAM-TUCSON-628.13		
Identificador único*	**UNAM-Tucson-SSIAAPM**	
(Nombre del sistema A4) *	Sistemas de administración de información de académicos o alumnos de programas de movilidad.	
Riesgo*	**Impacto***	**Mitigación***
• Acceso no autorizado a sistemas de almacenaje de DROPBOX	• Perdida de información. • Acceso y alteración de datos personales.	• Contraseñas robustas. • Mecanismos accesos. • Respaldar y borrar la información de la nube una vez concluido el curso.

4. ANÁLISIS DE BRECHA

UNAM-TUCSON-628.13		
Identificador único*	**UNAM-Tucson-SSIAAPM**	
(Nombre del sistema A4) *	Sistemas de administración de información de académicos o alumnos de programas de movilidad.	
Medida de seguridad actual*	**Medida de seguridad necesaria***	**Acciones para remediación***
Las plataforma utilizada para el almacenaje de las bases de datos (DROPBOX) requieren contraseñas y protocolos de seguridad robustos.	Definir contraseñas robustas y conservarlas en lugares seguros. Cambiar contraseñas con una frecuencia determinada y en forma sistemática.	Establecer un programa de capacitación a responsables, encargados y usuarios para incrementar las medidas de seguridad en el uso de las plataformas.

7. PLAN DE TRABAJO

UNAM-TUCSON-628.13			
Identificador único*	**UNAM-Tucson-SSIAAPM**		
(Nombre del sistema A4) *	Sistemas de administración de información de académicos o alumnos de programas de movilidad.		
Actividad*	**Descripción***	**Duración***	**Cobertura***
13. Capacitación	Se realizará un proceso de capacitación sobre medidas de seguridad en el manejo de las bases de datos en las plataformas, protocolos y cuidado en el resguardos de claves de acceso.	Dos sesiones de 1 hora.	Parcial
14. Actualización de contraseñas del sistema	Se cambiarán periódicamente las contraseñas utilizadas por los responsables, encargados y usuarios del sistema.	Anual	Total
15. Eliminar información no requerida.	Eliminar información que ya no se requiere en las plataformas utilizadas.	Semestral	Total
16. Respaldar información que se requiera almacenar	Se respaldará la información que requiera almacenar en unidades de almacenamiento físico de la Sede y la información almacenada en las plataformas se eliminará de la misma.	Anual	Total

8. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

I. TRANSFERENCIAS DE DATOS PERSONALES

UNAM-TUCSON-628.13	
Identificador único*	**UNAM-Tucson-SSIAAPM**
(Nombre del sistema A4) *	Sistemas de administración de información de académicos o alumnos de programas de movilidad.
TRANSFERENCIA DE DATOS PERSONALES	
Transferencia mediante el traslado de soportes físicos.	No aplica
Transferencias mediante el traslado de soportes electrónicos:	• Se comparte de manera digital y a través de DROPBOX la información parcial que contiene los datos personales de los académicos y/o de los alumnos con la Universidad de Arizona
Transferencias mediante el traslado sobre redes electrónicas:	No aplica

II RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS

7. El sistema UNAM-Tucson-SIyPCTAC no realiza envíos de datos personales con soportes físicos, ya que se encuentran en soporte electrónico mediante el uso de plataformas de manejo de base de datos.
8. El sistema UNAM-Tucson-SIyPCTAC realiza respaldos de las bases de datos que se quieren conservar en discos duros que se conservan bajo llave por el responsable.

V. ACCESO A LAS INSTALACIONES

1. Seguridad perimetral exterior (las instalaciones del área universitaria):

La Sede de la UNAM Tucson se ubica en las instalaciones del campus de la Universidad de Arizona en la ciudad de Tucson, Arizona, las cuales no tiene ningún tipo de barreras. La seguridad perimetral exterior es gestionada por dicha institución.

5. Seguridad perimetral interior

Las oficinas de UNAM Tucson se encuentran abiertas única y exclusivamente cuando algún funcionario de la Sede o de la UA que trabaja en las instalaciones de la Sede se encuentra físicamente en las instalaciones. De lo contrario, se encuentran cerradas bajo llave y el público no tiene acceso a los espacios o mobiliario.

Para las personas que acceden a dichos espacios interiores:

1. Para acceder a las instalaciones tiene que tocar a la puerta. Al hacerlo se le pregunta a que persona quiere visitar y cuál es su asunto.
2. No se autentifica.
3. Se le autoriza el acceso a discreción de la persona que lo recibe.

VII. PERFILES DE USUARIO Y CONTRASEÑAS

En este rubro el área universitaria deberá describir el esquema de perfiles de usuario y contraseñas que tiene implementado para control de acceso mediante una red electrónica.

1. Modelo de control de acceso (alguno de los siguientes):

a) Es obligatorio (etiquetas para objetos y acreditación para sujetos). Se utliza el sistema de Internet y de correos electrónico de la Universidad de Arizona o de la CRAI de la UNAM:

2. Perfiles de usuario y contraseñas en el sistema operativo de red:

a) ¿Cuenta con un sistema operativo de red instalado en sus equipos? Si

b) ¿Proporciona dicho sistema operativo un manejo riguroso de perfiles de usuario y contraseñas? Si

c) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena? Si

3. Perfiles de usuario y contraseñas manejados por el software aplicativo del sistema de tratamiento de datos personales:

   a) ¿Ofrece dicho software un manejo riguroso de perfiles de usuario y contraseñas? Si

   b) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena? Si

4. Administración de perfiles de usuario y contraseñas:

   a) ¿Quién da de alta nuevos perfiles? La Universidad de Arizona

   b) ¿Quién autoriza la creación de nuevos perfiles? La Universidad de Arizona

   c) ¿Se lleva registro de la creación de nuevos perfiles? Si, La Universidad de Arizona.

5. Acceso remoto al sistema de tratamiento de datos personales:

   a) ¿Requieren los usuarios acceso remoto al equipo de cómputo que por lo general utilizan para trabajar con el sistema? si

   b) ¿Requiere el administrador acceso remoto al equipo donde reside el sistema para realizar tareas de mantenimiento? si

   c) ¿Cómo se evita el acceso remoto no autorizado? A través de los protocolos de seguridad de la Universidad de Arizona

7. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

7.1. Herramientas y recursos para monitoreo de la protección de datos personales

(Denominación del área específica del Área Universitaria A)*		
Identificador único*	**A1. UNAM-Tucson-SIyPCTAC** **A2. UNAM-Tucson-SPREA** **A3. UNAM-Tucson-SIEAC** **A4. UNAM-Tucson-SSIAAPM**	
(Nombre del sistema)*	**A1**. Sistemas de inscripción y pago a curso y talleres académicos y culturales. **A2.** Sistemas de preinscripción para examen de admisión. **A3.** Sistemas de inscripción a eventos académicos y culturales **A4.** Sistemas de administración de información de académicos o alumnos de programas de movilidad.	
Recurso*	**Descripción***	**Control***
Revisión y monitoreo de los contratos y condiciones de operación de plataformas.	Revisión y monitoreo de los contratos y condiciones de operación de las plataformas de trabajo (SmartSheets, Dropbox, Google Drive y PayPal) para revisar la parte de tratamiento de datos personales	Control digital y/o en bitácora.
Monitoreo de contraseñas	Renovación anual de contraseñas	Llevar un control de contraseñas (definir si es digital o manual en bitácora
Monitoreo de los respaldos en disco duro y archivos digitales.	Supervisión de las actividades de respaldo del disco duro y archivos duros	Control digital y/o en bitácora
Monitoreo de las instalaciones y equipo electrónico y de cómputo de trabajo.	Revisión del estatus y vigencia del equipo instalaciones y equipos de trabajo.	Control digital y/o bitácora.

7.2. Procedimiento para la revisión de las medidas de seguridad

(Denominación del área específica del Área Universitaria A)*		
Identificador único*	**A1. UNAM-Tucson-SIyPCTAC** **A2. UNAM-Tucson-SPREA** **A3. UNAM-Tucson-SIEAC** **A4. UNAM-Tucson-SSIAAPM**	
(Nombre del sistema)*	**A1**. Sistemas de inscripción y pago a curso y talleres académicos y culturales. **A2.** Sistemas de preinscripción para examen de admisión. **A3.** Sistemas de inscripción a eventos académicos y culturales **A4.** Sistemas de administración de información de académicos o alumnos de programas de movilidad.	
Medida de seguridad*	**Procedimiento***	**Responsable***
Revisión y monitoreo de los contratos y condiciones de operación de plataformas.	*Acceso a la plataforma y revisar los contratos o si no están disponibles pedir que los envíen. Registrar información concerniente a datos personales.*	Director de la Sede
Monitoreo de contraseñas	*Generar y realizar el procedimiento de cambio de contraseñas*	Coordinador de Relaciones y Gestión
Monitoreo de los respaldos en disco duro y archivos digitales.	*Revisar el procedimiento de respaldos en disco duro de la información de datos personales de cada plataforma*	Coordinador de Relaciones y Gestión
Monitoreo de las instalaciones y equipo electrónico y de cómputo de trabajo.	*Revisar físicamente y digitalmente la actualidad de infraestructura (p.e. red alámbrica y de Wifi y de equipo electrónico y de cómputo.*	Director de la Sede

7.3. Resultados de la evaluación y pruebas a las medidas de seguridad

(Denominación del área específica del Área Universitaria A)*		
Identificador único*	**A1. UNAM-Tucson-SIyPCTAC** **A2. UNAM-Tucson-SPREA** **A3. UNAM-Tucson-SIEAC** **A4. UNAM-Tucson-SSIAAPM**	
(Nombre del sistema)*	**A1**. Sistemas de inscripción y pago a curso y talleres académicos y culturales. **A2.** Sistemas de preinscripción para examen de admisión. **A3.** Sistemas de inscripción a eventos académicos y culturales **A4.** Sistemas de administración de información de académicos o alumnos de programas de movilidad.	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***
Revisión y monitoreo de los contratos y condiciones de operación de plataformas.	En proceso	a) Director de la Sede
Monitoreo de contraseñas	En proceso	Coordinador de Relaciones y Gestión
Monitoreo de los respaldos en disco duro y archivos digitales.	En proceso	Coordinador de Relaciones y Gestión
Monitoreo de las instalaciones y equipo electrónico y de cómputo de trabajo.	En proceso	Director de la Sede

7.4. Acciones para la corrección y actualización de las medidas de seguridad

(Denominación del área específica del Área Universitaria A)*		
Identificador único*	**A1. UNAM-Tucson-SIyPCTAC** **A2. UNAM-Tucson-SPREA** **A3. UNAM-Tucson-SIEAC** **A4. UNAM-Tucson-SSIAAPM**	
(Nombre del sistema)*	**A1**. Sistemas de inscripción y pago a curso y talleres académicos y culturales. **A2.** Sistemas de preinscripción para examen de admisión. **A3.** Sistemas de inscripción a eventos académicos y culturales **A4.** Sistemas de administración de información de académicos o alumnos de programas de movilidad.	
Medida de seguridad*	**Acciones***	**Responsable***
Revisión y monitoreo de los contratos y condiciones de operación de plataformas.	a) Acciones correctivas: En caso de persistir la falla u omisión cambiar de plataforma. b) Acciones preventivas. Si se encuentra una falla u omisión en los contratos y condiciones de operación en las plataformas comunicarlo a los propietarios de dichas plataformas. Realizar acciones complementarias a las que realiza la plataforma.	Director de la Sede
Monitoreo de contraseñas	a) Acciones correctivas: Cambio de plataforma. b) Acciones preventivas. Si ocurre un incidente o motivo de preocupación hacer cambio anticipado de contraseña	Coordinador de Relaciones y Gestión
Monitoreo de los respaldos en disco duro y archivos digitales.	a) Acciones correctivas: Cambio de disco. b) Acciones preventivas. Incrementar frecuencia de respaldos	Coordinador de Relaciones y Gestión

Monitoreo de las instalaciones y equipo electrónico y de cómputo de trabajo.	a) Acciones correctivas: Cambio de dispositivo. b) Acciones preventivas. Incrementar frecuencia de respaldos	Coordinador de Relaciones y Gestión

8. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

8.1. Programa de capacitación a los responsables de tratamiento de datos personales

(Denominación del área específica del Área Universitaria A)*			
Identificador único*	**A1. UNAM-Tucson-SIyPCTAC** **A2. UNAM-Tucson-SPREA** **A3. UNAM-Tucson-SIEAC** **A4. UNAM-Tucson-SSIAAPM**		
(Nombre del sistema)*	**A1**. Sistemas de inscripción y pago a curso y talleres académicos y culturales. **A2.** Sistemas de preinscripción para examen de admisión. **A3.** Sistemas de inscripción a eventos académicos y culturales **A4.** Sistemas de administración de información de académicos o alumnos de programas de movilidad.		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Evento de capacitación para revisar el material documental de: Normas complementarias sobre medidas de seguridad técnicas, administrativas y físicas para la protección de datos personales en posesión de la universidad.	El curso debe incluir los protocolos y medidas de las Normas, de las evaluaciones anteriores y actuales, con el fin de asegurar la integridad, confidencialidad y disponibilidad de la información personal que éstos contienen	4 horas por 3 días	A todo el personal que maneje datos personales.

8.2. Programa de difusión de la protección a los datos personales

(Denominación del área específica del Área Universitaria A)*	
Identificador único*	**A1. UNAM-Tucson-SIyPCTAC** **A2. UNAM-Tucson-SPREA** **A3. UNAM-Tucson-SIEAC** **A4. UNAM-Tucson-SSIAAPM**
(Nombre del sistema)*	**A1**. Sistemas de inscripción y pago a curso y talleres académicos y culturales. **A2.** Sistemas de preinscripción para examen de admisión. **A3.** Sistemas de inscripción a eventos académicos y culturales **A4.** Sistemas de administración de información de académicos o alumnos de programas de movilidad.

Actividad*	Descripción*	Duración*	Cobertura*
Evento de difusión del material documental de: Normas complementarias sobre medidas de seguridad técnicas, administrativas y físicas para la protección de datos personales en posesión de la universidad.	Difundir losprotocolos y medidas de las Normas, de las evaluaciones anteriores y actuales, con el fin de asegurar la integridad, confidencialidad y disponibilidad de la información personal que éstos contienen a través de correo electrónico y de boletines internos.	Trimestralmente	A todo el personal que maneje datos personales.

9. MEJORA CONTINUA

9.1. Actualización y mantenimiento de sistemas de información

(Denominación del área específica del Área Universitaria A)*	
Identificador único*	**A1. UNAM-Tucson-SIyPCTAC** **A2. UNAM-Tucson-SPREA** **A3. UNAM-Tucson-SIEAC** **A4. UNAM-Tucson-SSIAAPM**
(Nombre del sistema)*	**A1**. Sistemas de inscripción y pago a curso y talleres académicos y culturales. **A2.** Sistemas de preinscripción para examen de admisión. **A3.** Sistemas de inscripción a eventos académicos y culturales **A4.** Sistemas de administración de información de académicos o alumnos de programas de movilidad.

Actividad*	Descripción*	Duración*	Cobertura*
Verificar que los mecanismos de monitoreo y revisión de las medidas de seguridad se lleven a cabo .	Revisión interna de los sistemas de tratamiento y archivo de datos personales.	*Trimestralmente*	*Todos los sistemas.*

9.2. Actualización y mantenimiento de equipo de cómputo

(Denominación del área específica del Área Universitaria A)*			
Identificador único*	**A1. UNAM-Tucson-SIyPCTAC** **A2. UNAM-Tucson-SPREA** **A3. UNAM-Tucson-SIEAC** **A4. UNAM-Tucson-SSIAAPM**		
(Nombre del sistema)*	**A1**. Sistemas de inscripción y pago a curso y talleres académicos y culturales. **A2.** Sistemas de preinscripción para examen de admisión. **A3.** Sistemas de inscripción a eventos académicos y culturales **A4.** Sistemas de administración de información de académicos o alumnos de programas de movilidad.		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Revisión anual	Revisión de anomalías que se presenten en el equipo y actualización de los sistemas computacionales que se utilizan en la Sede.	Una semana al año	Sistemas operativos, programas y aplicaciones.

9.3. Procesos para la conservación, preservación y respaldos de información

(Denominación del área específica del Área Universitaria A)*		
Identificador único*	**A1. UNAM-Tucson-SIyPCTAC** **A2. UNAM-Tucson-SPREA** **A3. UNAM-Tucson-SIEAC** **A4. UNAM-Tucson-SSIAAPM**	
(Nombre del sistema)*	**A1**. Sistemas de inscripción y pago a curso y talleres académicos y culturales. **A2.** Sistemas de preinscripción para examen de admisión. **A3.** Sistemas de inscripción a eventos académicos y culturales **A4.** Sistemas de administración de información de académicos o alumnos de programas de movilidad.	
Proceso*	**Descripción***	**Responsable***
Supervisión interna de los sistemas de tratamiento y archivo de datos personales y del seguimiento de procedimientos y mitigaciones de riesgo por parte del Coordinador de Relaciones y Gestión	Crear contraseñas digitales robustas y controlar accesos a las bases de datos y sistemas de datos personales. Asignar contraseñas a los archivos electrónicos que contengan datos personales. Borrar la información de la nube (Google Drive) y almacenarla en archivos digitales en un disco duro físico seguro con respaldo bajo el manejado del personal autorizado. Agregar cláusula de cesión de derechos sobre datos	*Coordinador de Relaciones y Gestión*

	personales en todo sistema de recopilación de datos. Adquisición de un programa antivirus. Estrategias y protocolos para el uso de llaves y cerraduras de la oficina. Tener un disco duro en la oficina y otro en el domicilio de personal de confianza de la Sede.	

9.4. Procesos de borrado seguro y disposición final de equipos y componentes informáticos

(Denominación del área específica del Área Universitaria A)*		
Identificador único*		
(Nombre del sistema A1)*	**(Nombre del sistema A1)***	
Proceso*	**Descripción***	**Responsable***
Borrado electrónico definitivo y eliminación de rastros y copias de los datos.	Borrado permanente de los archivos originales y cualquier copia, rastro o respaldo que pueda quedar en la nube (Google Drive)	*Coordinador de Relaciones y Gestión*

10. PROCEDIMIENTO PARA LA CANCELACIÓN DE UN SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

(Informar y describir el procedimiento para la cancelación de un sistema de tratamiento de datos personales.)

A) DATOS DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES QUE SERÁ CANCELADO:

a) Denomination
b) Motivo de la cancelación

B) PLAZOS Y CONDICIONES PARA EL BLOQUEO DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES:

(Señalar el periodo de bloqueo, considerando los plazos de prescripción para el ejercicio de algún derecho por parte de los titulares de conformidad con la normatividad de cada área universitaria. Asimismo, se debe señalar las condiciones y el procedimiento que se seguirá para realizar el bloqueo)

C) MEDIDAS DE SEGURIDAD PARA EL BLOQUEO Y POSTERIOR SUPRESIÓN DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES:

(Describir las medidas de seguridad aplicables al periodo de bloqueo y la supresión del sistema, considerando el nivel de protección requerido en virtud del tipo de datos personales contenidos en el sistema)

D) PROCEDIMIENTO PARA LA SUPRESIÓN DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

(Describir el procedimiento para suprimir el sistema, una vez cumplido el plazo de bloqueo)

E) MECANISMOS PARA LA SUPRESIÓN DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

(Describir las técnicas para la eliminación física del sistema)

11. APROBACIÓN DEL DOCUMENTO DE SEGURIDAD

		Nombre y firma de quienes revisaron el presente documento:
Responsable del desarrollo:	Nombre: Raúl López Parra Cargo: Coordinador de Comunicación y Vinculación Tel: (+86) 8881 5379 Correo electrónico: rlparra@china.unam.mx	
Revisó:	Nombre: Edmundo Borja Navarro Cargo: Coordinador de Relaciones Institucionales y Gestión Tel: (+86) 8881 5379 Correo electrónico: eborja@china.unam.mx	
	Nombre: Pablo Mendoza Ruiz Cargo: Coordinador Académico y Cultural Tel: (+86) 8881 5379 Correo electrónico: pmendoza@china.unam.mx	
Autorizó:	Nombre: Adalberto Noyola Cargo: Director Tel: (+86) 8881 5379 Correo electrónico: noyola@china.unam.mx	
Fecha de aprobación:	30 de noviembre de 2022	
Fecha de actualización:	30 de noviembre de 2022	

ANEXO II. FORMATO UNIVERSITARIO DE "SOLICITUD DE EJERCICIO DE DERECHOS ARCO"

Formato de solicitud de ejercicio de derechos Acceso, Rectificación, Cancelación y Oposición (ARCO)

Con fundamento en el artículo 54 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, esta área universitaria le solicita llenar el presente formato para ejercer sus derechos de Acceso, Rectificación, Cancelación y Oposición.

1. Datos del Área Universitaria de la UNAM responsable de tratar los datos personales*:

2. Datos del Titular de los Datos Personales*:

Primer apellido:	Segundo apellido:	Nombre(s):
CURP (para evitar homónimos):		

3. Datos del solicitante:

Primer apellido:	Segundo apellido:	Nombre(s):
Indicar si los datos corresponden a:		
☐Titular		
☐Menor de edad		
☐Persona que se encuentren en estado de interdicción o incapacidad establecida por ley.		
☐Fallecida		
Datos de identidad y representación legal (opcional, solo si usted no es el titular de los datos personales)		
☐Persona física:		
☐Nombre completo del representante:		
☐Representación de un menor de edad:		
☐Representación de una persona que se encuentren en estado de interdicción o incapacidad establecida por ley.		
☐Persona moral:		
☐Nombre o razón social del representante:		
Registro Federal de Contribuyentes (RFC):		
Documento con el que acredita la representación:		
☐Poder notarial ☐Carta poder simple signada ante dos testigos (con copia de los documentos que acrediten la identidad de los testigos y titular) ☐Declaración en comparecencia del Titular (en las instalaciones del área universitaria).		

4. Documento oficial de identificación del titular o solicitante (sólo originales) *:

☐Credencial para votar (INE)	☐Pasaporte	☐Licencia de conducir
☐Cédula profesional	☐Cartilla del Servicio militar nacional	☐Documento migratorio
☐Acta de nacimiento	☐Acta de defunción	☐Otra identificación con fotografía (especifique):

5. Medio por el cual prefiere que le sea notificada la puesta a disposición de la respuesta*:

☐Acudir al área universitaria donde presentó este formato	☐Correo electrónico (especificar):

6. Modalidad en la cual prefiere le sean entregados los datos, en caso de ser procedente. *

☐Copia simple	☐Correo electrónico
☐Copia certificada	☐ Otro medio electrónico como USB/CD ROOM/ DVD *(previo depósito de ficha de pago):*
☐Consultas directas	☐Yo proporciono el medio magnético o electrónico para reproducir los datos personales.

7. Tipo de solicitud de ejercicio de Derechos Acceso, Rectificación, Cancelación y Oposición (ARCO) a datos personales*:

☐ACCESO
Describir la información datos personales que obran en posesión del área universitaria y a los que requiere tener acceso*: _____ _____ _____

Señalar el nombre y ubicación del archivo o registro de datos personales*: _____ _____ _____
☐RECTIFICACIÓN
☐Son inexactos.
☐Son incompletos.
☐Requieren ser actualizados
Justificación y documentación original que acompaña para motivar su petición*: _____ _____ _____
CANCELACIÓN (supresión o eliminación)
Causas que motivan la cancelación*:
OPOSICIÓN (cese del tratamiento)
Causas que motivan la oposición (daño o perjuicio que le causa la persistencia del tratamiento de sus datos)*:_____ _____
Señalar si es para una finalidad específica o para todos los sistemas de información que obren en el área universitaria*._____
Documentación original que acompaña para motivar su petición*: _____
Señalar la referencia o documento que facilite la localización de sus datos personales*
_____ _____

Leí el Aviso de privacidad del área universitaria a la que acudo y en este acto otorgo el consentimiento para que mis datos personales sean tratados conforme al mismo.

_____

Firma o huella dactilar*

Plazos y procedimiento para la atención de las solicitudes de ejercicio de derechos ARCO:
Una vez que se presentó la solicitud, esta área universitaria cuenta con:

- Un plazo de 20 días hábiles, contados a partir del día siguiente a la recepción de la solicitud, para informarle si procede o no el ejercicio del derecho solicitado.
- Un plazo de 15 días hábiles, contados a partir del día siguiente en el que le haya notificado la respuesta anterior, en caso de que haya procedido el ejercicio del derecho, deberá llevar a cabo las acciones necesarias para hacerlo efectivo.

El ejercicio de los derechos ARCO será sencillo y gratuito, siempre que no rebase las 20 hojas simples, por lo que las áreas universitarias realizarán el cobro del costo de reproducción de acuerdo con los Lineamientos para la determinación de los costos de reproducción y envío en el marco de solicitudes de acceso a Información y entrega de datos personales en la Universidad Nacional Autónoma de México.

ANEXO III. CARTA DE CONFIDENCIALIDAD

Carta compromiso de confidencialidad, no divulgación, reserva y resguardo de información y datos personales

(Este documento debe firmarse por todas aquellas personas que por su empleo, cargo o comisión en la Universidad reciban y traten información confidencial de otras personas)

CIUDAD DE _____, A (DD-MM-AAAA)

(Nombre completo), *(cargo)*, adscrita(o) *(dependencia/entidad de adscripción)* de la Universidad Nacional Autónoma de México (en adelante la UNAM) acepto los términos y condiciones, que se describen más adelante, de resguardo, reserva, custodia y protección de la seguridad y confidencialidad de la información, datos personales y de todo tipo de documentos propiedad de la UNAM de los que tenga conocimiento, con motivo de las funciones que desempeño en la Universidad.

El presente compromiso me responsabiliza respecto de la información que me sea proporcionada por la UNAM, ya sea de forma oral, escrita, impresa, sonora, visual, electrónica, informática u holográfica, contenida en cualquier tipo de documento, que puede consistir en: expedientes, reportes, estudios, actas, resoluciones, oficios, correspondencia, acuerdos, directivas, directrices, circulares, contratos, convenios, instructivos, notas, memorandos, estadísticas, o bien, cualquier otro registro en medio conocido o por conocer que documente el ejercicio de las facultades, funciones y competencias del área universitaria y de los servidores universitarios, sin importar su fuente o fecha de elaboración.

La información que me sea proporcionada podría ser considerada, según el caso, como reservada, privilegiada y confidencial, en los términos de las leyes aplicables, por lo que me obligo a protegerla, reservarla, resguardarla y no divulgarla, utilizándola única y exclusivamente para llevar a cabo y cumplir con las actividades y obligaciones que expresamente me sean conferidas por la Universidad.

Es mi responsabilidad no reproducir, hacer pública o divulgar a terceros la información objeto de la presente Carta, y de cumplir con las medidas de seguridad adecuadas al tipo de documento con el que se trabaje.

Mi obligación de confidencialidad no es aplicable en los siguientes casos:

a) Cuando la información se encuentre en el dominio público en el momento en que me sea suministrada o, una vez suministrada, ésta se haga pública.
b) Cuando la legislación vigente o un mandato judicial exija su divulgación.
c) Cuando la información se desarrolle o reciba legítimamente de terceros, de forma totalmente independiente a mi relación con la Universidad.

A t e n t a m e n t e

_____
Firma o huella dactilar

ANEXO IV. RUTA CRÍTICA PARA CUMPLIMIENTO DE LAS MEDIDAS DE SEGURIDAD TÉCNICAS (MST)

A continuación, se presentan los requisitos técnicos para sistemas de información, descritos en las MST del capítulo II de las Normas Complementarias, por orden de prioridad, esto es: de los mínimos indispensables para asegurar los datos personales hasta los necesarios para incrementar la protección de dichos datos.

Dada la complejidad de diversos sistemas en la UNAM, se ha dispuesto la ruta crítica para el cumplimiento de las MST en tres etapas para los sistemas de información que a la fecha de publicación de esta guía estén en producción o funcionamiento. Todo sistema de información deberá satisfacer a cabalidad el 100% de las MST en un tiempo máximo de un año contado a partir de la publicación de las MST para conservar su registro y publicación dentro del dominio institucional .***unam.mx***.

A) **Etapa 1. Corto plazo**. Requisitos de misión crítica y mínimos indispensables para la protección de datos personales y datos personales sensibles. Cumplimiento obligatorio en menos de treinta días hábiles.
B) **Etapa 2. Mediano plazo**. Requisitos importantes para garantizar la protección de datos personales y datos personales sensibles. Ejecución estimada entre un mes y seis meses.
C) **Etapa 3. Largo plazo**. Requisitos necesarios para reforzar la seguridad en la protección de datos personales y datos personales sensibles. Ejecución estimada entre seis y doce meses.

Instrucciones

- Para cada MST se ha diseñado un formato, el cual está numerado en correspondencia con la ruta crítica de cumplimiento.
- Se deberán completar todos los formatos aplicables por cada uno de los sistemas de información a cargo del Área Universitaria.
- Todos los formatos deberán integrar el anexo del documento de seguridad de datos personales.
- En el caso de los sistemas que estén en desarrollo al momento de la publicación de las Normas complementarias, deberán cumplir con el 100% de las MST, previo a su publicación como sistema en producción.
- Es requisito indispensable el cumplimiento de las MST para conservar el registro dominio institucional ***.unam.mx*** en el caso de servicios Web.

Núm. formato	Etapa	Duración estimada	Medidas de seguridad técnicas y proceso recomendado para su cumplimiento
ETAPA 1			
Anexo I, numerales 1 y 2	1	Un día hábil	**Generar el inventario de sistemas de tratamiento de datos personales y la Estructura de descripción de los sistemas de tratamiento de datos personales.**
			A) Integrar la información correspondiente a todos los sistemas que dan tratamiento de datos personales en el área universitaria. **B)** Llenar formatos y colocar nombre y firma de quien realizó la acción.
1	1	Un día hábil	**Artículo 18. I. c) Utilizar datos no personales durante el desarrollo y pruebas de los sistemas.**

Núm. formato	Etapa	Duración estimada	Medidas de seguridad técnicas y proceso recomendado para su cumplimiento
			A) Realizar respaldo completo de la base de datos. **B)** Ejecutar consulta en el sistema de información, por medio de formato o comandos. **C)** Verificar que los datos usados en el desarrollo no correspondan a personas identificables. **D)** Si se usan datos de personas identificables, cambiar por datos genéricos o datos ficticios y regresar al punto B. **E)** Si no se usan datos de personas identificables, llenar formato 1 con nombre y firma de quien realizó la acción, fecha de inicio y de conclusión.
2	1	Un día hábil	**Artículo 18. I. e) Asignar o revocar los privilegios de acceso para los usuarios teniendo como base el principio del menor privilegio.**
			A) Realizar respaldo completo de la base de datos. **B)** Ejecutar consulta en el sistema de información de la lista de usuarios y sus niveles o privilegios de acceso. **C)** Validar que los niveles de acceso son acordes a la relación del usuario con el tratamiento de datos personales. **D)** Si hay usuarios con privilegios mayores a los que les son necesarios, cambiar al mínimo indispensable e informarlo al usuario. Regresar al punto B. **E)** Si los privilegios de acceso son correctos para los usuarios, llenar formato 2 con nombre y firma de quien realizó la acción, fecha de inicio y de conclusión.
3	1	Tres días hábiles	**Artículo 18. I. g) Instalar y mantener vigentes certificados de comunicación segura SSL en el caso de servicios basados en Web.**
			A) En caso de no tener un certificado SSL vigente, enviar correo electrónico al Departamento de Firma Electrónica de DGTIC a firma.tic@unam.mx solicitando la asignación. **B)** El Departamento de Firma Electrónica Avanzada envía procedimiento para obtención de CSR del servidor, formato de la solicitud y costos de recuperación en función del tipo de certificado requerido (organizacional, comodín o corporativo). **C)** Completar documentación, proceso y pago de costo de recuperación. Enviar comprobantes a firma.tic@unam.mx. **D)** Al recibir el certificado SSL, instalarlo en el servidor de acuerdo con las instrucciones recibidas junto con el certificado. **E)** Llenar formato 3 y colocar nombre y firma de quien realizó la acción.
4	1	Dos días hábiles	**Artículo 18. I. h) Definir el plan de respaldos de la información, incluyendo periodicidad y alcance.**
			A) Elaborar documento con la secuencia de respaldos al menos con el siguiente orden: - Diario – incremental. - Semanal – incremental. - Mensual – total.

Núm. formato	Etapa	Duración estimada	Medidas de seguridad técnicas y proceso recomendado para su cumplimiento
			B) Establecer en el plan los medios para resguardo del respaldo y su forma de identificación: - En línea: mismo equipo donde se ejecuta el sistema. - Respaldo como servicio: otro equipo de almacenamiento. - Fuera de línea: medios magnéticos (cintas, discos) y/u ópticos. **C)** Incluir en el plan: - Responsables de cada tipo y medio de respaldo. - Rotación de respaldos y medios. - Áreas de resguardo. - Métodos de cifrado. - RTO: *Recovery Time Objective*. Tiempo objetivo de recuperación. - RPO: *Recovery Point Objective*: Punto objetivo de recuperación. **D)** Concluir este documento, adjuntarlo a SGPDP, llenar formato 4 y colocar nombre y firma de quien realizó la acción.
5	1	Un día hábil	**Artículo 18. I. i) Definir el procedimiento para el borrado seguro.** **A)** Elaborar documento con el procedimiento y la herramienta para borrado seguro en función del tipo de base de datos para registros, tablas y base de datos. **B)** Incluir en el documento de borrado seguro el proceso de verificación de la no existencia del dato, generalmente por medio de consultas y de copias de respaldo. **C)** El borrado seguro debe incluirse en los respaldos incrementales y totales y en cualquiera de los medios de respaldo, así como máquinas virtuales o contenedores. **D)** Concluir este documento, adjuntarlo a SGPDP llenar formato 5 y colocar nombre y firma de quien realizó la acción.
6	1	Un día hábil	**Artículo 18. II. a) Sincronizar la fecha y hora con el servidor NTP (Network Time Protocol) oficial de la UNAM** **A)** Realizar la verificación y configuración con privilegio de administrador del sistema operativo. **B)** En función del sistema operativo, acceder a la configuración de servidor de tiempo (NTP) en interfaz gráfica o por medio de línea de comandos. *Por ejemplo*, en el caso del sistema operativo Linux: - Verificar la existencia del archivo */etc/ntp.conf* - Editar el archivo *ntp.conf* incluyendo en la primera línea: *server ntpdgtic.redunam.unam.mx* ***ó*** *server 132.247.169.17* - Reiniciar el demonio del cliente NTP con el comando *sudo service ntp reload.* **C)** En caso de no tener el cliente NTP instalado, descargarlo del repositorio de aplicaciones del sistema operativo, instalarlo y regresar al punto B. **D)** Llenar formato 6 y colocar nombre y firma de quien realizó la acción.
7	1	Dos días hábiles	**Artículo 18. II. b) Instalar y mantener actualizado el software antimalware.**

Núm. formato	Etapa	Duración estimada	Medidas de seguridad técnicas y proceso recomendado para su cumplimiento
			A) En función del sistema operativo, instalar uno o varios programas para la contención de malware. *Por ejemplo*, para el caso del sistema operativo Linux existen herramientas de código abierto y uso libre como *chkrootkit, rootkit hunter, bothunter, clamAV, avast*, entre otros, que se pueden instalar desde el repositorio correspondiente a la distribución de Linux en uso. **B)** Disponer de comandos para la localización de amenazas. *Por ejemplo*, para el caso de Linux, se recomienda usar el comando *grep* para la detección de cadenas regulares de texto en las invocaciones al *shell*. **C)** Una vez instalada la solución, verificar periódicamente su actualización. **D)** Llenar formato 7 y colocar nombre y firma de quien realizó la acción.
8	1	Cuatro días hábiles	**Artículo 18. II. c) Instalar las actualizaciones de seguridad más recientes disponibles.**
			A) En función del sistema operativo, se debe revisar la vigencia y actualización de las herramientas de seguridad de la información. *Por ejemplo*, en el sistema operativo Linux ejecutar *apt-get update* para obtener la lista de actualizaciones, especialmente en el repositorio *security* de la respectiva distribución. **B)** Realizar un respaldo del sistema para garantizar retorno a versión anterior en caso de incompatibilidad con alguna aplicación de las actualizaciones de seguridad. **C)** Instalar las actualizaciones en el sistema operativo. **D)** Llenar formato 8 y colocar nombre y firma de quien realizó la acción.
9	1	Cuatro días hábiles	**Artículo 19. I. a) Aplicar un mecanismo de autenticación para las personas autorizadas con base en el principio del menor privilegio.**
			A) Verificar el tipo de control de acceso al sistema, esto es: a través de contraseñas, claves, identificadores, nombres de usuario, nombres de dominio, entre otros. Según sea aplicable al sistema de información en lo particular. En caso de no tener un control de acceso establecer al menos uno como: usuarios de sistema operativo, cuenta y contraseña de sistema. **B)** Revisar que los privilegios de acceso sean los adecuados en función del rol del usuario. *Por ejemplo:* el usuario de conexión a la base de datos no debe estar asignado a alguna cuenta del personal que tiene acceso al sistema. **D)** Llenar formato 9 y colocar nombre y firma de quien realizó la acción.
10	1	Dos días hábiles	**Artículo 19. II. b) Evitar la instalación de cualquier elemento de software que implique algún riesgo para el tratamiento de datos personales.**
			A) Dependiendo del sistema operativo, configurar las actualizaciones solamente para versiones maduras o revisiones certificadas de las aplicaciones. *Por ejemplo*: en sistemas Linux desactivar la instalación de versiones *beta, test, debug, non-official.*

Núm. formato	Etapa	Duración estimada	Medidas de seguridad técnicas y proceso recomendado para su cumplimiento
			B) De la lista de software instalado, verificar el consumo de recursos de aplicaciones *TSR (Terminal and Stay Resident)*. Identificar demonios que ocupen excesiva RAM o tiempo de ejecución en el procesador. *Por ejemplo*: En sistemas Windows usar el Administrador de Tareas para identificar programas de alto consumo. **C)** Desinstalar toda aquella aplicación, librería, programa, paquetería o servicio que no sea estrictamente necesario para la operación del sistema. *Por ejemplo*, si el servidor Linux no proporcionará direcciones IP, el demonio o servicio *dchpd* no debe estar instalado. **D)** Llenar formato 10 y colocar nombre y firma de quien realizó la acción.
11	1	Dos días hábiles	**Artículo 19. III. a) Establecer las medidas físicas de seguridad que controlen el acceso a los equipos.** **A)** Identificar las medidas físicas que restrinjan el acceso físico a equipos, tales como chapas, puertas, biométricos. **B)** En función de la ubicación del equipo de cómputo, hacer una relación de las condiciones más adecuadas para su protección que aún sean necesarias implementar. **C)** Establecer y seguir un plan de mejoramiento de la protección física de equipos. *Por ejemplo*; cámaras de video vigilancia, bitácoras, vigilantes, cuartos cerrados, racks con puerta y chapa, candados en equipos, bloqueo o desconexión física de puertos USB, alarmas y sensores, según sea lo más conveniente como mínimo para la protección de los datos. **D)** Llenar formato 11 y colocar nombre y firma de quien realizó la acción.
12	1	Un día hábil	**Artículo 19. III. b) Restringir la salida de equipos de las instalaciones de cada área universitaria.** **A)** Diseñar una bitácora o formato para el registro de entrada y salida de equipos de cómputo y periféricos asociados como discos duros, cintas, unidades flash, discos ópticos, monitores, teclados, ratones y en lo general todo componente de un equipo. **B)** La bitácora de entrada y salida debe incluir el registro de número de serie e inventario UNAM. responsable de ingreso o egreso del componente y firma autorizada del responsable del área. **C)** Incluir en el procedimiento la revisión periódica (al menos una vez al mes) de la consistencia del inventario registrado contra la bitácora de entrada y salida. **D)** Llenar 12 y colocar nombre y firma de quien realizó la acción.
13	1	Tres días hábiles	**Artículo 19. IV. a) Realizar la transmisión de datos personales a través de un canal cifrado.** **A)** Identificar, mediante el administrador de aplicaciones que corresponda al sistema operativo, los protocolos y aplicaciones instalados para comunicación cifrada. *Por ejemplo*: *SFTP (Secure File Transfer Protocol), SSH (Secure Shell), SCP (Secure Copy*). **B)** Instalar con el administrador de aplicaciones o comando similar los protocolos de comunicación cifrada que sean necesarios para el tipo de transacciones y accesos del sistema.

Núm. formato	Etapa	Duración estimada	Medidas de seguridad técnicas y proceso recomendado para su cumplimiento
			Por ejemplo, en el caso de requerir ejecutar comandos de forma remota en un servidor Linux, instalarlo con el comando *apt-get install openssh-server.* **C)** Activar los protocolos de comunicación encriptada en el servidor. *Por ejemplo*: en Linux con el comando *sudo systemctl enable ssh*. **D)** Llenar formato 13 y colocar nombre y firma de quien realizó la acción.
14	1	Tres días hábiles	**Artículo 20. Aplicar el procedimiento de borrado seguro que impida la recuperación en las bases de datos y todos sus respaldos.** **A)** Realizar una copia integral del sistema de información y colocarla en un servicio temporal. *Por ejemplo:* máquina virtual o directorio temporal en el servidor. **B)** Ingresar a la copia del sistema de información y realizar el borrado de un registro. Verificar que el dato no persiste en la base de datos por medio de forma de consulta o comando. **C)** Realizar el mismo proceso del punto B para una tabla y finalmente para la base de datos completa. D) En caso de persistencia del dato, instalar y ejecutar herramientas para borrado seguro. *Por ejemplo*: en Linux se dispone *de shred, wipe, secure-delete, srm, sfill, sswap, sdmem,* que se pueden instalar desde el administrador de aplicaciones. **D)** Llenar formato 14 y colocar nombre y firma de quien realizó la acción.
			ETAPA 2
15	2	Hito	**Artículo 18. I. a) Utilizar los datos personales preexistentes que estén disponibles, de acuerdo con sus respectivas políticas de uso y acceso, en bases de datos a cargo de otras áreas universitarias.** **A)** Disponer del inventario de datos del sistema de información, esto es: documento con la descripción de tablas, campos, tipo de datos, relaciones y consultas. **B)** Con el Área Universitaria que esté identificada como la instancia autoritativa en materia de datos personales, comparar el inventario de datos. *Por ejemplo*: La Dirección General de Administración Escolar es la dependencia autoritativa en materia de datos personales de estudiantes. **C)** Establecer el acuerdo por escrito para el uso de campos específicos de datos personales de la instancia autoritativa. **D)** Establecer el mecanismo de comunicación entre el sistema de información y el de la instancia autoritativa. *Por ejemplo*: *Webservices*, transferencia *SFTP.* **E)** Llenar 15 y colocar nombre y firma de quien realizó la acción.
16	2	Ocho días hábiles	**Artículo 18. I. d) Permitir el acceso al código fuente de los sistemas exclusivamente a la administración del sistema y personal para el desarrollo.** **A)** Recopilar el código fuente y documentación del sistema de información en todas sus versiones disponibles. **B)** Depositar en un equipo central de desarrollo todas las versiones de código fuente y su documentación (inventario de datos, manual de administración, manual de programador).

Núm. formato	Etapa	Duración estimada	Medidas de seguridad técnicas y proceso recomendado para su cumplimiento
			C) Establecer control de acceso por usuario y contraseña hacia el equipo central de desarrollo. **D)** Activar bitácoras de acceso (*log*) hacia el equipo central de desarrollo. **E)** Proporcionar las credenciales de acceso al equipo central de desarrollo exclusivamente al personal a cargo de programación y mantenimiento de código y manuales. **F)** Llenar formato 16 y colocar nombre y firma de quien realizó la acción.
17	2	Cuatro días hábiles	**Artículo 19. I. b) Establecer las medidas de seguridad en los periodos de inactividad o mantenimiento.** **A)** Elaborar documento con las medidas necesarias de seguridad para períodos vacacionales, contingencias y ventanas de mantenimiento, incluyendo: control de acceso físico y lógico a los equipos, ejecución de respaldos, sistemas de alta disponibilidad (redundancia). **B)** Incluir en el documento la descripción de los procedimientos en caso de contingencia por falla de servicio de red, falla de equipo de cómputo, falla lógica en sistema operativo. **C)** Incluir en el documento el directorio de responsables de cada uno de los puntos a atender: apagado seguro, apagado fortuito, apagado programado, verificación de integridad de información, activación de servicios locales o de respaldo. **D)** Llenar formato 17 y colocar nombre y firma de quien realizó la acción.
18	2	Ocho días hábiles	**Artículo 19. I. c) Generar respaldos y aplicar los mecanismos de control y protección para su resguardo.** **A)** De acuerdo con el plan de respaldos establecido, ejecutar la secuencia de respaldos. **B)** Designar responsables de respaldos y responsables de verificación de respaldos. **C)** Completar bitácora de control de los respaldos, indicando fecha, hora, tipo de respaldo (integral, total, parcial de registros), ejecutor y revisor del respaldo, ubicación del respaldo, medio y etiqueta. **D)** Llenar formato 18 y colocar nombre y firma de quien realizó la acción.
19	2	Veinte días hábiles	**Artículo 19. I. d) Impedir el uso de cuentas y servicios gestionados por personas físicas para el tratamiento de los datos personales.** **A)** Realizar revisión integral del sistema de información en materia de accesos, cuentas y servicios. *Por ejemplo*: En caso de consultar vía un *Webservice* a un sistema autoritativo de datos personales en la DGAE, identificar la cuenta de acceso a ese sistema. **B)** Determinar si las cuentas de acceso a servicios locales o remotos están bajo el control de la administración del sistema. *Por ejemplo*: Si la cuenta de acceso a un *Webservice* – su usuario y contraseña – está bajo el control del administrador del sistema, o si un respaldo que se realiza en un equipo remoto es con una cuenta y contraseña controlada por el administrador del sistema.

Núm. formato	Etapa	Duración estimada	Medidas de seguridad técnicas y proceso recomendado para su cumplimiento
			C) Si las cuentas de acceso a servicios locales o remotos pertenecen a personas del Área Universitaria, cambiarlas por cuentas institucionales dentro del control de la instancia universitaria. *Por ejemplo*: si la identificación para acceder a un respaldo remoto es del tipo xxx@google.com, deberá cambiarse por una cuenta del tipo xxxx@unam.mx. **D)** Llenar formato 19 y colocar nombre y firma de quien realizó la acción.
20	2	Cuatro días hábiles	**Artículo 19. II. a) Proteger ante manipulaciones indebidas y accesos no autorizados las bitácoras y los dispositivos donde se almacenan.**
			A) Elaborar una lista de las bitácoras relacionadas con el sistema de información, tanto en medio digital como físico. *Por ejemplo*: En el equipo de cómputo las bitácoras de acceso de usuarios al sistema operativo y al sistema de información (*logs*), de forma física las bitácoras de acceso al área donde está el equipo de cómputo. **B)** Junto a la lista elaborar el cronograma de revisión de integridad y respaldo de las bitácoras. *Por ejemplo*: diario, semanal, mensual. **C)** Establecer en el documento el procedimiento de resguardo de las bitácoras. *Por ejemplo*: respaldo y protección de *logs* en el caso de equipo de cómputo o zonas seguras de almacenamiento de bitácoras en papel, digitalización de registros. **D)** Llenar formato 20 y colocar nombre y firma de quien realizó la acción.
21	2	Cuatro días hábiles	**Artículo 19. IV. b) Supervisar los controles de seguridad en la red de datos donde opere el sistema para tratamiento de datos personales.**
			A) Identificar los equipos activos de red que permiten la conexión del equipo de cómputo con el sistema de información, incluyendo marca, modelo, versión de software, vigencia de mantenimiento y capacidades de protección de las comunicaciones. **B)** Determinar las reglas de seguridad físicas (acceso restringido, cuartos de telecomunicaciones) y lógicas (cuentas de acceso, puertos activos, protocolos activos) para el equipo de red. **C)** Incluir en las acciones para aseguramiento de la red de datos aquellas que sean necesarias en función de los controles actuales. Definir un plan de regularización de la seguridad en caso de ser aplicable. **D)** Mantener actualizados los equipos activos de red y con un programa de mantenimiento. **E)** Identificar y en su caso programar la instalación de equipo para seguridad perimetral de la red de datos. **D)** Llenar formato 21 y colocar nombre y firma de quien realizó la acción.
22	2	Cuatro días hábiles	**Artículo 19. IV. c) Proporcionar el acceso exclusivamente desde redes y servicios autorizados.**
			A) Revisar los puertos de comunicación (*TCP y UDP*) que requiera el sistema de información para su operación. *Por*

Núm. formato	Etapa	Duración estimada	Medidas de seguridad técnicas y proceso recomendado para su cumplimiento
			ejemplo: para servicios *Web* los puertos 80 y 8080 son los convencionales. **B)** Activar en el sistema operativo la herramienta correspondiente para el control de puertos de comunicación. *Por ejemplo*, en Linux puede tratarse de un *firewall* a nivel de software o las herramientas que para tal efecto contenga la distribución correspondiente del sistema operativo. **C)** Dejar activos solamente los puertos necesarios para la operación del sistema. **D)** Activar el filtrado de la comunicación por direccionamiento IP en caso de ser posible para la operación del sistema. *Por ejemplo*: Permitir el acceso al puerto de *SSH* solamente a direcciones IP en una subred de la UNAM (132.248.x.y) o a un grupo de direcciones IP específicas. **E)** Llenar formato 22 y colocar nombre y firma de quien realizó la acción.
ETAPA 3			
23	3	Veinte días hábiles	**Artículo 18. I. b) Contar con entornos para desarrollo, pruebas y operación.** **A)** Instalar y configurar equipos similares en características, preferentemente virtuales, a los equipos donde se instalará el sistema de información en su nueva o actualizada versión. **B)** Crear un repositorio en un equipo central de desarrollo para el resguardo de códigos, documentación, inventarios de datos y manuales de usuario, administrador y programador. **C)** Ejecutar las pruebas de nuevas versiones o actualizaciones del sistema de información en el equipo dispuesto para tal efecto. Nunca usar -equipos físicos o virtuales con el sistema actualmente en producción como las plataformas para evaluación de versiones en desarrollo. **D)** Llenar formato 23 y colocar nombre y firma de quien realizó la acción.
24	3	Veinte días hábiles	**Artículo 18. I. f) Cumplir con las especificaciones de seguridad informática previo a la puesta en operación.** **A)** Una vez concluido el desarrollo o actualización de un sistema de información, solicitar al área de seguridad del Área Universitaria la revisión de seguridad informática del sistema, lo que incluye: pruebas de penetración, pruebas de estabilidad, pruebas de carga y endurecimiento de la seguridad. En caso de no contar con esa área, requerirlo a UNAM CERT al correo seguridad.tic@unam.mx . **B)** Una vez recibido el reporte del área de seguridad, aplicar las medidas de corrección que incluya el reporte. Regresar al punto A. **C)** Habiendo resuelto los hallazgos y sugerencias de mejora de la seguridad señalados por el área especializada, realizar la instalación del sistema en la plataforma definitiva de cómputo, extrayéndolo del entorno de desarrollo. **D)** Llenar formato 24 y colocar nombre y firma de quien realizó la acción.
25	3	Hito	**Artículo 18. III. a) Utilizar equipos con componentes actualizados, protegidos con garantías y soporte, y con la**

Núm. formato	Etapa	Duración estimada	Medidas de seguridad técnicas y proceso recomendado para su cumplimiento
			capacidad suficiente para atender la demanda del servicio y de los usuarios.
			A) Elaborar una lista del inventario de los equipos de cómputo, periféricos y de almacenamiento necesarios para la ejecución del sistema de información. **B)** Determinar la razón por la que el sistema de información requerirá estar localizado en un equipo físico y no en un servidor virtual. Con ello justificar una adquisición o actualización. Por ejemplo: por incompatibilidad con hipervisores, necesidades de comunicación exclusivamente locales en la entidad y dependencia o el no necesitar de un entorno de alta disponibilidad automática. **C)** Identificar en el inventario versiones, introducción en el mercado, vida útil, contratos de mantenimiento y soporte para todos y cada uno de los componentes, en el caso de emplear equipo físico. **D)** Adquirir los componentes y elementos necesarios para la actualización, vigencia de soporte y capacidad para atención a los usuarios en el equipo de cómputo físico. **E)** Llenar formato 25 y colocar nombre y firma de quien realizó la acción.
26	3	Hito	**Artículo 18. III. b) Definir el programa de mantenimiento preventivo.**
			A) De la lista de equipo de cómputo físico necesario para la operación del sistema de información, extraer las vigencias de mantenimiento. **B)** En caso de no estar en posibilidad de aplicar el mantenimiento preventivo por el personal del Área Universitaria, cotizar pólizas de mantenimiento de acuerdo con el tipo de componente, preferentemente una sola póliza para el conjunto del equipo físico. **C)** Adquirir las pólizas de mantenimiento preventivo y observar su vigencia. La vigencia no podrá ser menor de un año. **D)** Llenar formato 26 y colocar nombre y firma de quien realizó la acción.
27	3	Seis días hábiles	**Artículo 19. III. c) Aplicar el programa de mantenimiento preventivo a los equipos.**
			A) En caso de que el personal del Área Universitaria pueda realizar el mantenimiento preventivo, definir el calendario de inactividad del sistema de información, notificar a los usuarios y aplicar el plan en caso de mantenimiento o inactividad. **B)** En caso de que sea a través de un proveedor que se proporcione el mantenimiento al equipo de cómputo, ejecutar el calendario de acciones preventivas en un período no superior a cada 3 meses hasta la conclusión del contrato o póliza respectivo. **C)** Llenar formato 27 y colocar nombre y firma de quien realizó la acción.
28	3	Hito	**Artículo 21. Solo se permitirá el uso de servicios de nube pública para el resguardo de archivos cifrados que contengan respaldos de la información.**

Núm. formato	Etapa	Duración estimada	Medidas de seguridad técnicas y proceso recomendado para su cumplimiento
			A) Identificar los respaldos que se tengan resguardados en servicios de nube pública. **B)** Verificar el cifrado en cada uno de los respaldos que se almacenen en nube pública. El cifrado no deberá ser de menor capacidad al equivalente a AES de 128 bits. **C)** Llenar formato 28 y colocar nombre y firma de quien realizó la acción.

(Nombre del sistema A1)			Identificador único A1	
Formato	**1**	**Verificación anual**	**Acción concluida**	( )
Medida de seguridad técnica:		**Artículo 18. I. c) Utilizar datos no personales durante el desarrollo y pruebas de los sistemas.**		
Aplicable en:		I. Bases de datos y sistemas de tratamiento.		
Tiempo estimado:		Un día hábil.		
Importancia de la acción:		Evitar usar datos personales mientras se está desarrollando, actualizando o modificando el código fuente de un sistema de información.		
Proceso recomendado:		**A)** Realizar respaldo completo de la base de datos. **B)** Ejecutar consulta en el sistema de información, por medio de formato o comandos. **C)** Verificar que los datos usados en el desarrollo no correspondan a personas identificables. **D)** Si se usan datos de personas identificables, cambiar por datos genéricos o datos ficticios y regresar al punto B. **E)** Si no se usan datos de personas identificables, llenar formato con nombre y firma de quien realizó la acción, fecha de inicio y de conclusión.		
Mejores prácticas, referencias:		**1.-** Se recomienda al desarrollar un sistema de información no usar datos personales sino ficticios. **2.-** Se sugiere incluir en la documentación del desarrollo de un sistema de información el inventario de datos y el tipo de información de prueba.		
Conocimientos requeridos:		Administración de bases de datos. Consulta y actualización de tablas.		
Ejecución			**Fecha inicio**	
Nombre y firma Programador, desarrollador o diseñador del sistema de información			**Fecha término**	
Observaciones / anotaciones				

I. _____

(Nombre del sistema A1)			Identificador único A1	
Formato:	**2**	**Verificación anual**	**Acción concluida**	( )
Medidas de seguridad técnicas:	**Artículo 18. I. e) Asignar o revocar los privilegios de acceso para los usuarios teniendo como base el principio del menor privilegio.**			
Aplicable en:	I. Bases de datos y sistemas de tratamiento.			
Tiempo estimado:	Un día hábil.			
Importancia de la acción:	No se deben asignar privilegios de acceso a los usuarios en niveles que no estén relacionados con su responsabilidad en el tratamiento de datos.			
Proceso recomendado:	**A)** Realizar respaldo completo de la base de datos. **B)** Ejecutar consulta en el sistema de información de la lista de usuarios y sus niveles o privilegios de acceso. **C)** Validar que los niveles de acceso son acordes a la relación del usuario con el tratamiento de datos personales. **D)** Si hay usuarios con privilegios mayores a los que les son necesarios, cambiar al mínimo indispensable e informarlo al usuario. Regresar al punto B. **E)** Si los privilegios de acceso son correctos para los usuarios, llenar formato con nombre y firma de quien realizó la acción, fecha de inicio y de conclusión.			
Mejores prácticas, referencias:	**1.-** Definir niveles de acceso adecuados para cada perfil o tipo de usuario. **2.-** Tener un mínimo de administradores o usuarios con altos privilegios en el sistema.			
Conocimientos requeridos:	Administración de bases de datos. Consulta y actualización de usuarios.			
Ejecución			**Fecha inicio**	
Nombre y firma Administrador del sistema de información			**Fecha término**	
Observaciones / anotaciones				

(Nombre del sistema A1)			Identificador único A1	
Formato:	**3**	**Verificación anual**	**Acción concluida**	( )
Medidas de seguridad técnicas:	**Artículo 18. I. g) Instalar y mantener vigentes certificados de comunicación segura SSL en el caso de servicios basados en Web.**			
Aplicable en:	I. Bases de datos y sistemas de tratamiento.			
Tiempo estimado:	Tres días hábiles.			
Importancia de la acción:	El instalar un certificado SSL en servidores web incrementa la seguridad al encriptar la transferencia de datos y la unicidad del sitio para los usuarios.			
Proceso recomendado:	**A)** En caso de no tener un certificado SSL vigente, enviar correo electrónico al Departamento de Firma Electrónica de DGTIC a firma.tic@unam.mx solicitando la asignación. **B)** El Departamento de Firma Electrónica Avanzada envía procedimiento para obtención de CSR del servidor, formato de la solicitud y costos de recuperación en función del tipo de certificado requerido (organizacional, comodín o corporativo). **C)** Completar documentación, proceso y pago de costo de recuperación. Enviar comprobantes a firma.tic@unam.mx. **D)** Al recibir el certificado SSL, instalarlo en el servidor de acuerdo con las instrucciones recibidas junto con el certificado.			
Mejores prácticas, referencias:	**1.-** Los certificados SSL deben tener una vigencia de al menos un año. **2.-** En caso de tener varios sistemas de información bajo un mismo dominio, se recomienda obtener un certificado SSL del tipo comodín (*wildcard*). **3.-** Se debe realizar el proceso de renovación del certificado al menos 10 días hábiles antes de su vencimiento.			
Conocimientos requeridos:	Administración de sistema operativo. Administración de servicios Web.			
Ejecución			**Fecha inicio**	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término**	
Observaciones / anotaciones				

(Nombre del sistema A1)			Identificador único A1	
Formato:	**4**	**Verificación anual**	**Acción concluida**	( )
Medidas de seguridad técnicas:	**Artículo 18. I. h) Definir el plan de respaldos de la información, incluyendo periodicidad y alcance.**			
Aplicable en:	I. Bases de datos y sistemas de tratamiento.			
Tiempo estimado:	Dos días hábiles.			
Importancia de la acción:	En todo sistema de información es indispensable contar con un plan de respaldos periódicos, y especialmente en aquellos que contienen datos personales.			
Proceso recomendado:	**A)** Elaborar documento con la secuencia de respaldos al menos con el siguiente orden: - Diario – incremental. - Semanal – incremental. - Mensual – total. **B)** Establecer en el plan los medios para resguardo del respaldo y su forma de identificación: - En línea: mismo equipo donde se ejecuta el sistema. - Respaldo como servicio: otro equipo de almacenamiento. - Fuera de línea: medios magnéticos (cintas, discos) y/u ópticos. **C)** Incluir en el plan: - Responsables de cada tipo y medio de respaldo. - Rotación de respaldos y medios. - Áreas de resguardo. - Métodos de cifrado. - RTO: *Recovery Time Objective*. Tiempo objetivo de recuperación. - RPO: *Recovery Point Objective*: Punto objetivo de recuperación. **D)** Concluir este documento, adjuntarlo a SGPDP, llenar y firmar formato.			
Mejores prácticas, referencias:	**1.-** Se deben tener al menos 3 respaldos del sistema y sus bases de datos en distintos medios.			
Conocimientos requeridos:	Administración de sistema operativo. Gestión y programación de respaldos.			

Ejecución	Fecha inicio
Nombre y firma Administrador del sistema de información o servidor	**Fecha término**

Observaciones / anotaciones	

(Nombre del sistema A1)	Identificador único A1

Formato:	5	Verificación anual	Acción concluida	( )
Medidas de seguridad técnicas:		**Artículo 18. I. i) Definir el procedimiento para el borrado seguro.**		
Aplicable en:		I. Bases de datos y sistemas de tratamiento.		
Tiempo estimado:		Un día hábil.		
Importancia de la acción:		Al igual que el procedimiento de respaldo, el borrado seguro de la información debe estar definido en cualquier sistema de información.		
Proceso recomendado:		**A)** Elaborar documento con el procedimiento y la herramienta para borrado seguro en función del tipo de base de datos para registros, tablas y base de datos. **B)** Incluir en el documento de borrado seguro el proceso de verificación de la no existencia del dato, generalmente por medio de consultas y de copias de respaldo. **C)** El borrado seguro debe incluirse en los respaldos incrementales y totales y en cualquiera de los medios de respaldo, así como máquinas virtuales o contenedores. **D)** Concluir este documento, adjuntarlo a SGPDP, llenar y firmar formato.		
Mejores prácticas, referencias:		**1.-** Para el caso de baja de equipo, se debe llenar el formato con la declaración de borrado seguro del Patronato Universitario, disponible en: http://www.patrimonio.unam.mx/patrimonio/descargas/formato_responsiva_borrado_datos.pdf **2.-** Se recomienda utilizar herramientas de borrado seguro por medio de sobre escritura aleatoria, llenado de ceros (0x00), llenado de unos o protocolos de borrado del estándar *DOD-5220.22-M*.		
Conocimientos requeridos:		Administración de sistema operativo. Comandos de borrado.		
Ejecución			**Fecha inicio**	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término**	
Observaciones / anotaciones				

(Nombre del sistema A1)			Identificador único A1	
Formato:	**6**	**Verificación anual**	**Acción concluida**	( )

Medidas de seguridad técnicas:	**Artículo 18. II. a) Sincronizar la fecha y hora con el servidor NTP (Network Time Protocol) oficial de la UNAM**
Aplicable en:	II. Sistemas operativos y servicios.
Tiempo estimado:	Un día hábil.
Importancia de la acción:	A fin de poseer información consistente, los sistemas de información deben estar sincronizados con una instancia central de tiempo, en este caso el servidor NTP de la UNAM.
Proceso recomendado:	**A)** Realizar la verificación y configuración con privilegio de administrador del sistema operativo. **B)** En función del sistema operativo, acceder a la configuración de servidor de tiempo (NTP) en interfaz gráfica o por medio de línea de comandos. *Por ejemplo*, en el caso del sistema operativo Linux: - Verificar la existencia del archivo */etc/ntp.conf* - Editar el archivo *ntp.conf* incluyendo en la primera línea: *server ntpdgtic.redunam.unam.mx* ***ó*** *server 132.247.169.17* - Reiniciar el demonio del cliente NTP con el comando *sudo service ntp reload.* **C)** En caso de no tener el cliente NTP instalado, descargarlo del repositorio de aplicaciones del sistema operativo, instalarlo y regresar al punto B. **D)** Llenar y firmar formato.
Mejores prácticas, referencias:	**1.-** Los servidores virtuales y contenedores hospedados en el Centro de Datos en DGTIC son configurados de origen con sincronización al servidor NTP de la UNAM. **2.-** No se deben usar otros servidores de NTP distintos al de UNAM.
Conocimientos requeridos:	Administración de sistema operativo.

Ejecución	**Fecha inicio**
Nombre y firma Administrador del sistema de información o servidor	**Fecha término**

Observaciones / anotaciones	

(Nombre del sistema A1)			Identificador único A1	
Formato:	**7**	**Verificación anual**	**Acción concluida**	( )
Medidas de seguridad técnicas:	**Artículo 18. II. b) Instalar y mantener actualizado el software antimalware.**			
Aplicable en:	II. Sistemas operativos y servicios.			
Tiempo estimado:	Dos días hábiles.			
Importancia de la acción:	El servidor que hospede el sistema de información debe tener protecciones instaladas para mitigar la inserción de *malware* (*rootkits, backdoors o* códigos maliciosos) que pueda alterar su operación o la integridad y seguridad de los datos.			
Proceso recomendado:	**A)** En función del sistema operativo, instalar uno o varios programas para la contención de malware. *Por ejemplo*, para el caso del sistema operativo Linux existen herramientas de código abierto y uso libre como *chkrootkit, rootkit hunter, bothunter, clamAV, avast*, entre otros, que se pueden instalar desde el repositorio correspondiente a la distribución de Linux en uso. **B)** Disponer de comandos para la localización de amenazas. *Por ejemplo*, para el caso de Linux, se recomienda usar el comando *grep* para la detección de cadenas regulares de texto en las invocaciones al *shell*. **C)** Una vez instalada la solución, verificar periódicamente su actualización **D)** Llenar y firmar formato.			
Mejores prácticas, referencias:	**1.-** UNAM-CERT puede asesorar en la selección de las herramientas *anti malware* más adecuadas para el servidor donde se aloje el sistema de información. Contactar al correo seguridad.tic@unam.mx.			
Conocimientos requeridos:	Administración de sistema operativo. Instalación de aplicaciones.			
Ejecución			**Fecha inicio**	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término**	
Observaciones / anotaciones				

(Nombre del sistema A1)			Identificador único A1	
Formato:	**8**	**Verificación anual**	**Acción concluida**	( )
Medidas de seguridad técnicas:	**Artículo 18. II. c) Instalar las actualizaciones de seguridad más recientes disponibles.**			
Aplicable en:	II. Sistemas operativos y servicios.			
Tiempo estimado:	Cuatro días hábiles.			
Importancia de la acción:	El servidor que hospede el sistema de información debe tener vigentes todas las actualizaciones de seguridad proporcionadas por el fabricante o desarrollador del sistema operativo.			
Proceso recomendado:	**A)** En función del sistema operativo, se debe revisar la vigencia y actualización de las herramientas de seguridad de la información. *Por ejemplo*, en el sistema operativo Linux ejecutar *apt-get update* para obtener la lista de actualizaciones, especialmente en el repositorio *security* de la respectiva distribución. **B)** Realizar un respaldo del sistema para garantizar retorno a versión anterior en caso de incompatibilidad con alguna aplicación de las actualizaciones de seguridad. **C)** Instalar las actualizaciones en el sistema operativo. **D)** Llenar y firmar formato.			
Mejores prácticas, referencias:	**1.-** Debe verificarse la actualización de seguridad del sistema operativo al menos una vez a la semana y configurar la actualización o notificación inmediata en caso de complementos de seguridad urgentes.			
Conocimientos requeridos:	Administración de sistema operativo. Instalación de aplicaciones.			
Ejecución			**Fecha inicio**	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término**	
Observaciones / anotaciones				

(Nombre del sistema A1)			Identificador único A	
Formato:	**9**	**Verificación anual**	**Acción concluida**	( )
Medidas de seguridad técnicas:		**Artículo 19. I. a) Aplicar un mecanismo de autenticación para las personas autorizadas con base en el principio del menor privilegio.**		
Aplicable en:		I. Bases de datos y sistemas de tratamiento.		
Tiempo estimado:		Cuatro días hábiles.		
Importancia de la acción:		Partiendo de la asignación o niveles de acceso a la información con el principio del menor privilegio, debe haber en operación en el sistema al menos un mecanismo para la validación de los usuarios autorizados.		
Proceso recomendado:		**A)** Verificar el tipo de control de acceso al sistema, esto es: a través de contraseñas, claves, identificadores, nombres de usuario, nombres de dominio, entre otros. Según sea aplicable al sistema de información en lo particular. En caso de no tener un control de acceso establecer al menos uno como: usuarios de sistema operativo, cuenta y contraseña de sistema. **B)** Revisar que los privilegios de acceso sean los adecuados en función del rol del usuario. *Por ejemplo:* el usuario de conexión a la base de datos no debe estar asignado a alguna cuenta del personal que tiene acceso al sistema. **D)** Llenar y firmar formato.		
Mejores prácticas, referencias:		**1.-** Se recomienda usar un esquema estándar de acceso a sistemas que están vinculados, por ejemplo: por medio de Directorio Activo (*Active Directory*), *LDAP* u *OpenAIM.* **2.-** Las contraseñas deben ser de 12 caracteres o más con uso de signos, letras mayúsculas y minúsculas y números.		
Conocimientos requeridos:		Administración de bases de datos. Consulta y actualización de usuarios.		
Ejecución			**Fecha inicio**	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término**	
Observaciones / anotaciones				

(Nombre del sistema A1)			Identificador único A1	
Formato:	**10**	**Verificación anual**	**Acción concluida**	( )
Medida de seguridad técnica:	**Artículo 19. II. b) Evitar la instalación de cualquier elemento de software que implique algún riesgo para el tratamiento de datos personales.**			
Aplicable en:	II. Sistemas operativos.			
Tiempo estimado:	Dos días hábiles.			
Importancia de la acción:	Por la relevancia de los sistemas de información con datos personales se debe minimizar o erradicar el riesgo de seguridad que implica instalar aplicaciones no verificadas.			
Proceso recomendado:	**A)** Dependiendo del sistema operativo, configurar las actualizaciones solamente para versiones maduras o revisiones certificadas de las aplicaciones. *Por ejemplo*: en sistemas Linux desactivar la instalación de versiones *beta, test, debug, non-official.* **B)** De la lista de software instalado, verificar el consumo de recursos de aplicaciones *TSR (Terminal and Stay Resident)*. Identificar demonios que ocupen excesiva RAM o tiempo de ejecución en el procesador. *Por ejemplo*: En sistemas Windows usar el Administrador de Tareas para identificar programas de alto consumo. **C)** Desinstalar toda aquella aplicación, librería, programa, paquetería o servicio que no sea estrictamente necesario para la operación del sistema. *Por ejemplo*, si el servidor Linux no proporcionará direcciones IP, el demonio o servicio *dchpd* no debe estar instalado. **D)** Llenar y firmar formato.			
Mejores prácticas, referencias:	**1.-** En ningún caso puede instalarse software de procedencia desconocida. Se debe impedir a los usuarios en sus privilegios de acceso instalar software o inyectar código a la aplicación del sistema de información. y se debe realizar un control estricto de los puertos de comunicación (USB, Red, etc) para evitar la extracción no autorizada de datos.			
Conocimientos requeridos:	Administración de sistema operativo. Instalación de aplicaciones.			
Ejecución			**Fecha inicio**	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término**	
Observaciones / anotaciones				

(Nombre del sistema A1)			Identificador único A1	
Formato:	**11**	**Verificación anual**	**Acción concluida**	( )
Medidas de seguridad técnicas:	**Artículo 19. III. a) Establecer las medidas físicas de seguridad que controlen el acceso a los equipos.**			
Aplicable en:	III. Equipo de cómputo.			
Tiempo estimado:	Dos días hábiles.			
Importancia de la acción:	Además de las protecciones de tipo lógico, deben implementarse medidas de seguridad para reducir el riesgo al sistema de información por accesos físicos no autorizados.			
Proceso recomendado:	**A)** Identificar las medidas físicas que restrinjan el acceso físico a equipos, tales como chapas, puertas, biométricos. **B)** En función de la ubicación del equipo de cómputo, hacer una relación de las condiciones más adecuadas para su protección que aún sean necesarias implementar. **C)** Establecer y seguir un plan de mejoramiento de la protección física de equipos. *Por ejemplo*; cámaras de videovigilancia, bitácoras, vigilantes, cuartos cerrados, racks con puerta y chapa, candados en equipos, bloqueo o desconexión física de puertos USB, alarmas y sensores, según sea lo más conveniente como mínimo para la protección de los datos. **D)** Llenar y firmar formato.			
Mejores prácticas, referencias:	**1.-** Las medidas físicas de seguridad deben revisarse regularmente y formar parte de plan de continuidad de operaciones, así como ser del conocimiento de la Comisión local de seguridad.			
Conocimientos requeridos:	Administración de bases de datos. Consulta y actualización de usuarios.			
Ejecución			**Fecha inicio**	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término**	
Observaciones / anotaciones				

(Nombre del sistema A1)			Identificador único A1	
Formato:	**12**	**Verificación anual**	**Acción concluida**	( )
Medidas de seguridad técnicas:	**Artículo 19. III. b) Restringir la salida de equipos de las instalaciones de cada área universitaria.**			
Aplicable en:	III. Equipo de cómputo.			
Tiempo estimado:	Un día hábil.			
Importancia de la acción:	Se debe tener un mecanismo de control para la entrada y salida de equipos de cómputo y eliminar extracciones no autorizadas.			
Proceso recomendado:	**A)** Diseñar una bitácora o formato para el registro de entrada y salida de equipos de cómputo y periféricos asociados como discos duros, cintas, unidades *flash*, discos ópticos, monitores, teclados, ratones y en lo general todo componente de un equipo. **B)** La bitácora de entrada y salida debe incluir el registro de número de serie e inventario UNAM. responsable de ingreso o egreso del componente y firma autorizada del responsable del área. **C)** Incluir en el procedimiento la revisión periódica (al menos una vez al mes) de la consistencia del inventario registrado contra la bitácora de entrada y salida. **D)** Llenar y firmar formato.			
Mejores prácticas, referencias:	**1.-** Se recomienda usar un formato estándar de control de entrada y salida de bienes proporcionado por las áreas administrativas de las entidades y dependencias y conservar una copia en el área responsable del equipo de cómputo. **2.-** En la bitácora se debe incluir la razón de la entrada o salida del equipo. En el caso de baja, se deberá firmar la declaración de borrado seguro de Patrimonio Universitario.			
Conocimientos requeridos:	Gestión de Tecnología de información, control de entrada y salida de equipo y materiales.			
Ejecución			**Fecha inicio**	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término**	
Observaciones / anotaciones				

(Nombre del sistema A1)			Identificador único A1	
Formato:	**13**	**Verificación anual**	**Acción concluida**	( )
Medidas de seguridad técnicas:	**Artículo 19. IV. a) Realizar la transmisión de datos personales a través de un canal cifrado.**			
Aplicable en:	IV. Red de datos.			
Tiempo estimado:	Tres días hábiles.			
Importancia de la acción:	La comunicación del sistema de información con otros sistemas o servicios, así como el acceso de administración para ejecución de procesos por comandos, debe estar encriptada para evitar el envío o recepción de datos susceptibles de ser interceptados en tránsito.			
Proceso recomendado:	**A)** Identificar, mediante el administrador de aplicaciones que corresponda al sistema operativo, los protocolos y aplicaciones instalados para comunicación cifrada. *Por ejemplo*: *SFTP (Secure File Transfer Protocol), SSH (Secure Shell), SCP (Secure Copy*). **B)** Instalar con el administrador de aplicaciones o comando similar los protocolos de comunicación cifrada que sean necesarios para el tipo de transacciones y accesos del sistema. *Por ejemplo*, en el caso de requerir ejecutar comandos de forma remota en un servidor Linux, instalarlo con el comando *apt-get install openssh-server.* **C)** Activar los protocolos de comunicación encriptada en el servidor. *Por ejemplo*: en Linux con el comando *sudo systemctl enable ssh*. **D)** Llenar y firmar formato.			
Mejores prácticas, referencias:	**1.-** Se deben mantener actualizados los protocolos de comunicación por canal cifrado al igual que las utilerías de seguridad. 2.- El protocolo de comunicación cifrada requiere puertos específicos TCP, los cuales deberán estar permitidos en la configuración del equipo activo de red.			
Conocimientos requeridos:	Administración de sistema operativo. Instalación de aplicaciones. Administración de red.			
Ejecución			**Fecha inicio**	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término**	
Observaciones / anotaciones				

(Nombre del sistema A1)			Identificador único A1	
Formato:	**14**	**Verificación anual**	**Acción concluida**	( )
Medidas de seguridad técnicas:	**Artículo 20. Aplicar el procedimiento de borrado seguro que impida la recuperación en las bases de datos y todos sus respaldos.**			
Aplicable en:	Bases de datos y sistemas de tratamiento.			
Tiempo estimado:	Tres días hábiles.			
Importancia de la acción:	Se debe verificar que el procedimiento de borrado seguro es funcional y que el dato no persiste en función del tipo de borrado (registro, tabla, base, sistema).			
Proceso recomendado:	**A)** Realizar una copia integral del sistema de información y colocarla en un servicio temporal. *Por ejemplo:* máquina virtual directorio temporal en el servidor. **B)** Ingresar a la copia del sistema de información y realizar el borrado de un registro. Verificar que el dato no persiste en la base de datos por medio de forma de consulta o comando. **C)** Realizar el mismo proceso del punto B para una tabla y finalmente para la base de datos completa. D) En caso de persistencia del dato, instalar y ejecutar herramientas para borrado seguro. *Por ejemplo*: en Linux se dispone *de shred, wipe, secure-delete, srm, sfill, sswap, sdmem,* que se pueden instalar desde el administrador de aplicaciones. **D)** Llenar y firmar este formato.			
Mejores prácticas, referencias:	**1.-** Se recomienda usar al menos un comando a nivel de sistema operativo para el borrado seguro de conformidad con el procedimiento establecido.			
Conocimientos requeridos:	Administración de sistema operativo. Instalación de aplicaciones. Gestión de archivos.			
Ejecución			**Fecha inicio**	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término**	
Observaciones / anotaciones				

(Nombre del sistema A1)			Identificador único A1	
Formato:	**15**	**Verificación anual**	**Acción concluida**	( )
Medidas de seguridad técnicas		**Artículo 18. I. a) Utilizar los datos personales preexistentes que estén disponibles, de acuerdo con sus respectivas políticas de uso y acceso en bases de datos a cargo de otras áreas universitarias.**		
Aplicable en:		I. Bases de datos y sistemas de tratamiento.		
Tiempo estimado:		Hito.		
Importancia de la acción:		Optimizar y consolidar el uso y la protección de datos personales al hacer referencia a instancias universitarias que sean las principales responsables de su obtención, resguardo y protección.		
Proceso recomendado:		**A)** Disponer del inventario de datos del sistema de información, esto es: documento con la descripción de tablas, campos, tipo de datos, relaciones y consultas. **B)** Con la Área Universitaria que esté identificada como la instancia autoritativa en materia de datos personales, comparar el inventario de datos. *Por ejemplo*: La Dirección General de Administración Escolar es la dependencia autoritativa en materia de datos personales de estudiantes. **C)** Establecer el acuerdo por escrito para el uso de campos específicos de datos personales de la instancia autoritativa. **D)** Establecer el mecanismo de comunicación entre el sistema de información y el de la instancia autoritativa. *Por ejemplo*: *Webservices*, transferencia *SFTP.* **E)** Llenar y firmar formato.		
Mejores prácticas, referencias:		**1.-** El hacer referencia a instancias a cargo de la obtención de los datos personales y su protección se garantiza la homogeneidad de la información.		
Conocimientos requeridos:		Administración de sistema de información. Gestión de bases de datos.		
Ejecución			**Fecha inicio**	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término**	
Observaciones / anotaciones				

(Nombre del sistema A1)			Identificador único A1	
Formato:	**16**	**Verificación anual**	**Acción concluida**	( )
Medidas de seguridad técnicas:	**Artículo 18. I. d) Permitir el acceso al código fuente de los sistemas exclusivamente a la administración del sistema y personal para el desarrollo.**			
Aplicable en:	I. Bases de datos y sistemas de tratamiento.			
Tiempo estimado:	Ocho días hábiles.			
Importancia de la acción:	Evitar el uso de códigos originales de los sistemas de información que posteriormente implique un riesgo a la seguridad de estos.			
Proceso recomendado:	**A)** Recopilar el código fuente y documentación del sistema de información en todas sus versiones disponibles. **B)** Depositar en un equipo central de desarrollo todas las versiones de código fuente y su documentación (inventario de datos, manual de administración, manual de programador). **C)** Establecer control de acceso por usuario y contraseña hacia el equipo central de desarrollo **D)** Activar bitácoras de acceso (*log*) hacia el equipo central de desarrollo. **E)** Proporcionar las credenciales de acceso al equipo central de desarrollo exclusivamente al personal a cargo de programación y mantenimiento de código y manuales. **F)** Llenar y firmar formato.			
Mejores prácticas, referencias:	**1.-** Se debe documentar todo el proceso de desarrollo y actualización de un sistema de información.			
Conocimientos requeridos:	Administración de sistema de información. Gestión de bases de datos.			
Ejecución			**Fecha inicio**	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término**	
Observaciones / anotaciones				

(Nombre del sistema A1)			Identificador único A1	
Formato:	**17**	**Verificación anual**	**Acción concluida**	( )
Medidas de seguridad técnicas:		**Artículo 19. I. b) Establecer las medidas de seguridad en los periodos de inactividad o mantenimiento.**		
Aplicable en:		I. Bases de datos y sistemas de tratamiento.		
Tiempo estimado:		Cuatro días hábiles.		
Importancia de la acción:		Garantizar la continuidad de la operación y disponibilidad de los sistemas de información especialmente durante períodos vacacionales, contingencias o ciclos de mantenimiento.		
Proceso recomendado:		**A)** Elaborar documento con las medidas necesarias de seguridad para períodos vacacionales, contingencias y ventanas de mantenimiento, incluyendo: control de acceso físico y lógico a los equipos, ejecución de respaldos, sistemas de alta disponibilidad (redundancia). **B)** Incluir en el documento la descripción de los procedimientos en caso de contingencia por falla de servicio de red, falla de equipo de cómputo, falla lógica en sistema operativo. **C)** Incluir en el documento el directorio de responsables de cada uno de los puntos a atender: apagado seguro, apagado fortuito, apagado programado, verificación de integridad de información, activación de servicios locales o de respaldo. **D)** Llenar y firmar formato.		
Mejores prácticas, referencias:		**1.-** Las medidas de seguridad durante períodos de mantenimiento deben formar parte de un plan de continuidad de operaciones y de recuperación ante desastres (**DRP**).		
Conocimientos requeridos:		Administración de sistema de información. Administración de sistema operativo.		
Ejecución			**Fecha inicio**	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término**	
Observaciones / anotaciones				

(Nombre del sistema A1)			Identificador único A1	
Formato:	**18**	**Verificación anual**	**Acción concluida**	( )
Medidas de seguridad técnica:		**Artículo 19. I. c) Generar respaldos y aplicar los mecanismos de control y protección para su resguardo.**		
Aplicable en:		I. Bases de datos y sistemas de tratamiento.		
Tiempo estimado:		Ocho días hábiles.		
Importancia de la acción:		Verificar que el plan de respaldos opera adecuadamente para su utilización en caso de contingencia.		
Proceso recomendado:		**A)** De acuerdo con el plan de respaldos establecido, ejecutar la secuencia de respaldos. **B)** Designar responsables de respaldos y responsables de verificación de respaldos. **C)** Completar bitácora de control de los respaldos, indicando fecha, hora, tipo de respaldo (integral, total, parcial de registros), ejecutor y revisor del respaldo, ubicación del respaldo, medio y etiqueta. **D)** Llenar y firmar formato.		
Mejores prácticas, referencias:		**1.-** La generación de respaldos, su control y protección deben formar parte de un plan de continuidad de operaciones y de recuperación ante desastres (**DRP**).		
Conocimientos requeridos:		Administración de sistema de información. Administración de sistema operativo.		
Ejecución			**Fecha inicio**	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término**	
Observaciones / anotaciones				

(Nombre del sistema A1)			Identificador único A1	
Formato:	**19**	**Verificación anual**	**Acción concluida**	( )
Medidas de seguridad técnicas:	**Artículo 19. I. d) Impedir el uso de cuentas y servicios gestionados por personas físicas para el tratamiento de los datos personales.**			
Aplicable en:	I. Bases de datos y sistemas de tratamiento.			
Tiempo estimado:	Veinte días hábiles.			
Importancia de la acción:	Debe evitarse el riesgo que implica el depender de cuentas de control personal para acceder a servicios, fuentes de información o cualquier elemento del sistema de información que ponga en riesgo su estabilidad y confiabilidad.			
Proceso recomendado:	**A)** Realizar revisión integral del sistema de información en materia de accesos, cuentas y servicios. *Por ejemplo*: En caso de consultar vía un *Webservice* a un sistema autoritativo de datos personales en la DGAE, identificar la cuenta de acceso a ese sistema. **B)** Determinar si las cuentas de acceso a servicios locales o remotos están bajo el control de la administración del sistema. *Por ejemplo*: Si la cuenta de acceso a un *Webservice* – su usuario y contraseña – está bajo el control del administrador del sistema, o si un respaldo que se realiza en un equipo remoto es con una cuenta y contraseña controlada por el administrador del sistema. **C)** Si las cuentas de acceso a servicios locales o remotos pertenecen a personas del Área Universitaria, cambiarlas por cuentas institucionales dentro del control de la instancia universitaria. *Por ejemplo*: si la identificación para acceder a un respaldo remoto es del tipo xxx@google.com, deberá cambiarse por una cuenta del tipo xxxx@unam.mx **D)** Llenar y firmar formato.			
Mejores prácticas, referencias:	**1.-** Nunca deben usarse cuentas, servicios, suscripciones, licencias o cualquier otro elemento informático cuyo control dependa de una sola persona.			
Conocimientos requeridos:	Administración de sistema de información. Gestión de bases de datos.			

Ejecución	**Fecha inicio**
Nombre y firma Administrador del sistema de información o servidor	**Fecha término**

Observaciones / anotaciones	

(Nombre del sistema A1)			Identificador único A1	
Formato:	**20**	**Verificación anual**	**Acción concluida**	( )
Medidas de seguridad técnicas:	**Artículo 19. II. a) Proteger ante manipulaciones indebidas y accesos no autorizados las bitácoras y los dispositivos donde se almacenan.**			
Aplicable en:	II. Sistemas operativos.			
Tiempo estimado:	Cuatro días hábiles.			
Importancia de la acción:	Las bitácoras son un elemento esencial para determinar acciones que atentan contra la estabilidad del sistema de información y la protección de los datos personales.			
Proceso recomendado:	**A)** Elaborar una lista de las bitácoras relacionadas con el sistema de información, tanto en medio digital como físico. *Por ejemplo*: En el equipo de cómputo las bitácoras de acceso de usuarios al sistema operativo y al sistema de información (*logs*), de forma física las bitácoras de acceso al área donde está el equipo de cómputo. **B)** Junto a la lista elaborar el cronograma de revisión de integridad y respaldo de las bitácoras. *Por ejemplo*: diario, semanal, mensual. **C)** Establecer en el documento el procedimiento de resguardo de las bitácoras. *Por ejemplo*: respaldo y protección de *logs* en el caso de equipo de cómputo o zonas seguras de almacenamiento de bitácoras en papel, digitalización de registros. **D)** Llenar y firmar formato.			
Mejores prácticas, referencias:	**1.-** Las bitácoras digitales y en papel deben resguardarse preferentemente en una zona independiente de la ubicación del sistema de información.			
Conocimientos requeridos:	Administración de sistema de información. Administración de sistema operativo.			
Ejecución			**Fecha inicio**	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término**	
Observaciones / anotaciones				

(Nombre del sistema A1)			Identificador único A1	
Formato:	**21**	**Verificación anual**	**Acción concluida**	( )
Norma Complementaria Técnica		**Artículo 19. IV. b) Supervisar los controles de seguridad en la red de datos donde opere el sistema para tratamiento de datos personales.**		
Aplicable en:		IV. Red de datos.		
Tiempo estimado:		Cuatro días hábiles.		
Importancia de la acción:		El control de seguridad de los equipos activos de red que suministran la conectividad al sistema de información es un elemento básico para la protección de los datos.		
Proceso recomendado:		**A)** Identificar los equipos activos de red que permiten la conexión del equipo de cómputo con el sistema de información, incluyendo marca, modelo, versión de software, vigencia de mantenimiento y capacidades de protección de las comunicaciones. **B)** Determinar las reglas de seguridad físicas (acceso restringido, cuartos de telecomunicaciones) y lógicas (cuentas de acceso, puertos activos, protocolos activos) para el equipo de red. **C)** Incluir en las acciones para aseguramiento de la red de datos aquellas que sean necesarias en función de los controles actuales. Definir un plan de regularización de la seguridad en caso de ser aplicable. **D)** Mantener actualizados los equipos activos de red y con un programa de mantenimiento. **E)** Identificar y en su caso programar la instalación de equipo para seguridad perimetral de la red de datos. **D)** Llenar y firmar formato.		
Mejores prácticas, referencias:		**1.-** Las ubicaciones físicas de los equipos activos de red deben estar protegidas con cerraduras y controles de acceso, cumplir las normas de operación y no emplearse para ningún otro equipo o uso.		
Conocimientos requeridos:		Administración de redes de datos.		
Ejecución			**Fecha inicio**	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término**	
Observaciones / anotaciones				

(Nombre del sistema A1)			Identificador único A1	
Formato:	**22**	**Verificación anual**	**Acción concluida**	( )
Medidas de seguridad técnicas:		**Artículo 19. IV. c) Proporcionar exclusivamente el acceso desde redes y servicios autorizados.**		
Aplicable en:		IV. Red de datos.		
Tiempo estimado:		Cuatro días hábiles.		
Importancia de la acción:		Es necesario reducir el mínimo necesario los puertos de comunicación para el funcionamiento del sistema de información.		
Proceso recomendado:		**A)** Revisar los puertos de comunicación (*TCP y UDP*) que requiera el sistema de información para su operación. *Por ejemplo*: para servicios *Web* los puertos 80 y 8080 son los convencionales. **B)** Activar en el sistema operativo la herramienta correspondiente para el control de puertos de comunicación. *Por ejemplo*, en Linux puede tratarse de un *firewall* a nivel de software o las herramientas que para tal efecto contenga la distribución correspondiente del sistema operativo. **C)** Dejar activos solamente los puertos necesarios para la operación del sistema. **D)** Activar el filtrado de la comunicación por direccionamiento IP en caso de ser posible para la operación del sistema. *Por ejemplo*: Permitir el acceso al puerto de *SSH* solamente a direcciones IP en una subred de la UNAM (132.248.x.y) o a un grupo de direcciones IP específicas. **E)** Llenar y firmar formato.		
Mejores prácticas, referencias:		**1.-** No se deben tener activos accesos que no son necesarios vía la red de datos.		
Conocimientos requeridos:		Administración de sistema de información. Administración de sistema operativo.		
Ejecución			**Fecha inicio**	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término**	
Observaciones / anotaciones				

(Nombre del sistema A1)			Identificador único A1	
Formato:	**23**	**Verificación anual**	**Acción concluida**	( )
Medidas de seguridad técnicas:	**Artículo 18. I. b) Contar con entornos para desarrollo, pruebas y operación.**			
Aplicable en:	I. Bases de datos y sistemas de tratamiento.			
Tiempo estimado:	Veinte días hábiles.			
Importancia de la acción:	Para evitar riesgos innecesarios a la información, el desarrollo y actualización de los mismos deberá ser realizado siempre en una plataforma y ambientes por separado.			
Proceso recomendado:	**A)** Instalar y configurar equipos similares en características, preferentemente virtuales, a los equipos donde se instalará el sistema de información en su nueva o actualizada versión. **B)** Crear un repositorio en un equipo central de desarrollo para el resguardo de códigos, documentación, inventarios de datos y manuales de usuario, administrador y programador. **C)** Ejecutar las pruebas de nuevas versiones o actualizaciones del sistema de información en el equipo dispuesto para tal efecto. Nunca usar -equipos físicos o virtuales con el sistema actualmente en producción como las plataformas para evaluación de versiones en desarrollo. **D)** Llenar y firmar formato.			
Mejores prácticas, referencias:	**1.-** Se deben realizar respaldos de la información en los sistemas en desarrollo del mismo modo que como se realicen con el sistema en producción.			
Conocimientos requeridos:	Administración de sistema de información. Desarrollo de aplicaciones.			
Ejecución			**Fecha inicio**	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término**	
Observaciones / anotaciones				

(Nombre del sistema A1)			Identificador único A1	
Formato:	**24**	**Verificación anual**	**Acción concluida**	( )
Medidas de seguridad técnicas:	**Artículo 18. I. f) Cumplir con las especificaciones de seguridad informática previo a la puesta en operación.**			
Aplicable en:	I. Bases de datos y sistemas de tratamiento.			
Tiempo estimado:	Veinte días hábiles.			
Importancia de la acción:	Solo los sistemas de información revisados integralmente en su seguridad y estabilidad pueden ser publicados bajo el dominio .unam.mx .			
Proceso recomendado:	**A)** Una vez concluido el desarrollo o actualización de un sistema de información, solicitar al área de seguridad del Área Universitaria la revisión de seguridad informática del sistema, lo que incluye: pruebas de penetración, pruebas de estabilidad, pruebas de carga y endurecimiento de la seguridad. En caso de no contar con esa área, requerirlo a UNAM CERT al correo seguridad.tic@unam.mx . **B)** Una vez recibido el reporte del área de seguridad, aplicar las medidas de corrección que incluya el reporte. Regresar al punto A. **C)** Habiendo resuelto los hallazgos y sugerencias de mejora de la seguridad señalados por el área especializada, realizar la instalación del sistema en la plataforma definitiva de cómputo, extrayéndolo del entorno de desarrollo. **D)** Llenar y firmar formato.			
Mejores prácticas, referencias:	**1.-** El equipo de UNAM CERT puede asesorar a las entidades y dependencias en la aplicación de las medidas de corrección y mitigación a partir de los resultados de la revisión de seguridad.			
Conocimientos requeridos:	Administración de aplicaciones. Administración de sistema operativo.			
Ejecución			**Fecha inicio**	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término**	
Observaciones / anotaciones				

(Nombre del sistema A1)			Identificador único A1	
Formato:	**25**	**Verificación anual**	**Acción concluida**	( )
Medidas de seguridad técnicas:	**Artículo 18. III. a) Utilizar equipos con componentes actualizados, protegidos con garantías y soporte, y con la capacidad suficiente para atender la demanda del servicio y de los usuarios.**			
Aplicable en:	III. Equipos de cómputo.			
Tiempo estimado:	Hito.			
Importancia de la acción:	Mantener en adecuada condición de operación el equipo de cómputo incrementa la estabilidad y seguridad del sistema de información.			
Proceso recomendado:	**A)** Elaborar una lista del inventario de los equipos de cómputo, periféricos y de almacenamiento necesarios para la ejecución del sistema de información. **B)** Determinar la razón por la que el sistema de información requerirá estar localizado en un equipo físico y no en un servidor virtual. Con ello justificar una adquisición o actualización. Por ejemplo: por incompatibilidad con hipervisores, necesidades de comunicación exclusivamente locales en la entidad y dependencia o el no necesitar de un entorno de alta disponibilidad automática. **C)** Identificar en el inventario versiones, introducción en el mercado, vida útil, contratos de mantenimiento y soporte para todos y cada uno de los componentes, en el caso de emplear equipo físico. **D)** Adquirir los componentes y elementos necesarios para la actualización, vigencia de soporte y capacidad para atención a los usuarios en el equipo de cómputo físico. **E)** Llenar y firmar formato.			
Mejores prácticas, referencias:	**1.-** El mantenimiento preventivo debe contar con medidas de verificación.			
Conocimientos requeridos:	Administración de infraestructura.			
Ejecución			**Fecha inicio**	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término**	
Observaciones / anotaciones				

(Nombre del sistema A1)			Identificador único A1	
Formato:	**26**	**Verificación anual**	**Acción concluida**	( )
Medidas de seguridad técnicas:	**Artículo 18. III. b) Definir el programa de mantenimiento preventivo.**			
Aplicable en:	III. Equipos de cómputo.			
Tiempo estimado:	Hito.			
Importancia de la acción:	Garantizar que el plan de mantenimiento de equipo se realiza en tiempo y forma.			
Proceso recomendado:	**A)** De la lista de equipo de cómputo físico necesario para la operación del sistema de información, extraer las vigencias de mantenimiento. **B)** En caso de no estar en posibilidad de aplicar el mantenimiento preventivo por el personal del Área Universitaria, cotizar pólizas de mantenimiento de acuerdo con el tipo de componente, preferentemente una sola póliza para el conjunto del equipo físico. **C)** Adquirir las pólizas de mantenimiento preventivo y observar su vigencia. La vigencia no podrá ser menor de un año. **D)** Llenar y firmar formato.			
Mejores prácticas, referencias:	**1.-** El programa de mantenimiento debe considerar los costos de contratos, refacciones, partes, actualizaciones y reemplazos.			
Conocimientos requeridos:	Administración de infraestructura.			
Ejecución			**Fecha inicio**	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término**	
Observaciones / anotaciones				

(Nombre del sistema A1)			Identificador único A1	
Formato:	**27**	**Verificación anual**	**Acción concluida**	( )
Medidas de seguridad técnicas:		**Artículo 19. III. c) Aplicar el programa de mantenimiento preventivo a los equipos.**		
Aplicable en:		III. Equipos de cómputo.		
Tiempo estimado:		Seis días hábiles.		
Importancia de la acción:		Garantizar que el plan de mantenimiento de equipo se realiza en tiempo y forma.		
Proceso recomendado:		**A)** En caso de que el personal del Área Universitaria pueda realizar el mantenimiento preventivo, definir el calendario de inactividad del sistema de información, notificar a los usuarios y aplicar el plan en caso de mantenimiento o inactividad. **B)** En caso de que sea a través de un proveedor que se proporcione el mantenimiento al equipo de cómputo, ejecutar el calendario de acciones preventivas en un período no superior a cada 3 meses hasta la conclusión del contrato o póliza respectivo. **C)** Llenar y firmar formato.		
Mejores prácticas, referencias:		**1.-** Debe actualizarse el equipo de cómputo de manera suficiente para continuar la operación del sistema y considerar en el mantenimiento preventivo sistemas paralelos de manera temporal hasta la conclusión de los trabajos.		
Conocimientos requeridos:		Administración de infraestructura.		
Ejecución			**Fecha inicio**	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término**	
Observaciones / anotaciones				

(Nombre del sistema A1)			Identificador único A1	
Formato:	**28**	**Verificación anual**	**Acción concluida**	( )
Medidas de seguridad técnicas:		**Artículo 21. Solo se permitirá el uso de servicios de nube pública para el resguardo de archivos cifrados que contengan respaldos de la información.**		
Aplicable en:		Servicios en la nube pública.		
Tiempo estimado:		Hito.		
Importancia de la acción:		No pueden conservarse o usarse datos personales que sean tratados por la UNAM en servicios de nube pública. Estos servicios sólo se permiten para el respaldo de archivos cifrados, no en producción.		
Proceso recomendado:		**A)** Identificar los respaldos que se tengan resguardados en servicios de nube pública. **B)** Verificar el cifrado en cada uno de los respaldos que se almacenen en nube pública. El cifrado no deberá ser de menor capacidad al equivalente a AES de 128 bits.		
Mejores prácticas, referencias:		**1.-** La DGTIC proporciona el servicio de respaldos en el Centro de Datos, por lo que se sugiere utilizarlo en lugar de respaldos en la nube pública.		
Conocimientos requeridos:		Administración de respaldos. Administración de sistema operativo.		
Ejecución			**Fecha inicio**	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término**	
Observaciones / anotaciones				

UNAM-BOSTON

CENTRO DE ESTUDIOS MEXICANOS

1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

UNAM-BOSTON	
Identificador único*	**BOS-IC**
(Nombre del sistema A1) *	**UNAM Boston Inscripciones a cursos**
Datos personales (sensibles o no) contenidos en el sistema*:	Nombre, teléfono celular o particular, correo electrónico, nacionalidad, titulo, cedula profesional, credencial (UNAM), visa, pasaporte, seguro médico, certificación de vacunación COVID-19.
Responsable*	
Nombre*:	Héctor Zavala Guzmán
Cargo*:	Coordinación de Relaciones y Gestión
Funciones*:	Definir el uso que se le dará a los datos personales de los alumnos. Designar a los encargados del sistema que tendrán acceso a los datos personales. Comunicar a los encargados del sistema las políticas de uso de los datos personales. Generar los recibos de pago de los alumnos.
Obligaciones*:	Mantener la protección de datos personales contenidos en el sistema implementando medidas de seguridad. No difundir datos personales de los alumnos. No modificar la información almacenada en el servidor No hacer respaldos en equipo personal de la información de datos personales. Redactar y enviar informes académicos y administrativos que contienen datos personales de los alumnos.
	Encargados:
(Nombre del Encargado 1*)	**Renata Gatica**
Cargo*:	**Planeación**
Funciones*:	Realizar el formulario de cada curso para recabar la información de los alumnos registrados. Enviar el formulario a los alumnos interesados en los cursos. Establecer comunicación con los alumnos durante el proceso de inscripción. Validar y archivar los documentos que contienen los datos personales de los alumnos registrados. Enviar los recibos de pago a los alumnos.
Obligaciones*:	Mantener la protección de datos personales contenidos en el sistema implementando las medidas de seguridad. No difundir datos personales de los alumnos. No modificar la información almacenada en el servidor

	No hacer respaldos en equipo personal de la información de datos personales.
(Nombre del Encargado 2*)	**Paulina Morales Valle**
Cargo*:	**Diseño**
Funciones*:	Elaborar las constancias de los estudiantes de cada curso.
Obligaciones*:	Mantener la protección de datos personales contenidos en el sistema implementando las medidas de seguridad. No difundir datos personales de los alumnos. No modificar la información almacenada en el servidor No hacer respaldos en equipo personal de la información de datos personales.

2. ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

UNAM-BOSTON	
Identificador único¨*	**BOS-IC**
(Nombre del sistema A1*)	**UNAM Boston Inscripciones a cursos**
Tipo de soporte:*	Electrónico
Descripción:*	Base de datos
Características del lugar donde se resguardan los soportes:*	Nube privada en Google Drive a la que solo pueden acceder usuarios autorizados por el responsable del sistema. Equipo de cómputo de la Sede. Disco duro externo de la Sede.

3. ANÁLISIS DE RIESGOS

UNAM-BOSTON		
Identificador único*	**BOS-IC**	
(Nombre del sistema A1) *	**UNAM Boston Inscripciones a cursos**	
Riesgo*	**Impacto***	**Mitigación***
Hackeo de los correos electrónicos de los usuarios del sistema.	Perdida de documentación. Acceso y alteración de datos personales.	Contraseñas robustas. Controlar accesos. Respaldar y borrar la información de la nube una vez concluido el curso.
Robo de soporte electrónico de almacenamiento (computadoras, discos duros, USBs, etc.)	Acceso a la información contenido en el dispositivo de almacenamiento y posible difusión y revelación de la información.	Asignar contraseñas a los archivos electrónicos que contengan datos personales.
Almacenamiento de datos personales en la nube.	Filtraciones y acceso a la información.	Borrar información de la nube y almacenarlo en un disco duro físico, bajo el manejado del personal autorizado.
Vulnerabilidad jurídica al no solicitar permiso de uso y almacenamiento de datos al titular.	Caer en responsabilidad jurídica por usar datos sin consentimiento.	Agregar cláusula de cesión de derechos sobre datos personales.
Infección del equipo de cómputo de la Sede por virus y malware.	Pérdida y filtración de información.	Evitar el uso de cómputo de la sede para navegar sitios web no relacionados a las actividades de la sede. Adquisición de un programa antivirus.
Robo del equipo de cómputo.	Pérdida y filtración de información.	Estrategias y protocolos para el uso de llaves y cerraduras de la oficina. Tener un disco duro en la oficina y otro en el domicilio de personal de confianza de la Sede.

4. ANÁLISIS DE BRECHA

UNAM-BOSTON		
Identificador único*	**BOS-IC**	
(Nombre del sistema A1) *	**UNAM Boston Inscripciones a cursos**	
Medida de seguridad actual*	**Medida de seguridad necesaria***	**Acciones para remediación***
Designar usuarios autorizados para el monitoreo de datos personales.	Definir contraseñas robustas para los documentos digitales.	Tener un protocolo de contraseñas seguras y actualizarlas cada semestre.
No se cuentan con expedientes físicos en los que aparezcan datos personales de los alumnos para evitar su extravío y mal uso de la información.	Correcto	No es necesario
Almacenamiento de datos en la nube.	Respaldo digital en almacenamiento de disco duro físico	Adquirir disco duro, bajar y eliminar información de la nube.

5. PLAN DE TRABAJO

UNAM-Boston			
Identificador único*	**BOS-IC**		
(Nombre del sistema A1) *	**UNAM Boston Inscripciones a cursos**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Indique actividad. Agregar un renglón por cada elemento	Describa el tipo de actividad, sus objetivos e impacto en la protección de datos personales	Indique duración en la ejecución de la actividad en horas, días, meses, su fecha de inicio y de término	Mencione los aspectos de la protección a datos personales que son resueltos, total o parcialmente, por la actividad.

6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

I. TRANSFERENCIAS DE DATOS PERSONALES

UNAM-BOSTON	
Identificador único*	**BOS-IC**
(Nombre del sistema A1)*	**UNAM Boston Inscripciones a cursos**
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	No aplica.
Transferencias mediante el traslado de soportes electrónicos:	Se comparte de manera digital la información que contiene los datos personales de los alumnos con la Coordinación de Relaciones y Asuntos Internacionales como parte de la entrega de informes académicos y administrativos. Se comparte de manera digital información con los responsables de la Red Universitaria de responsables de Internacionalización.
Transferencias mediante el traslado sobre redes electrónicas:	No aplica

II. RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS

El sistema UNAM-Boston inscripciones a cursos no realiza tratamientos de datos personales son soportes físicos, ya que se encuentran en soporte electrónico mediante el uso de una base de datos.

1. Señalar las medidas de seguridad que ha implementado el área universitaria para el resguardo de los soportes físicos del sistema de manera que evite la alteración, pérdida o acceso no autorizado a los mismos.
No aplica.
2. Señalar en un listado las personas (nombre, cargo, funciones y obligaciones) que tienen acceso a los soportes físicos del sistema.
No aplica.

III. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

No se llevan bitácoras

1. Los datos que se registran en las bitácoras:

a) Quién accede a los datos personales, fecha y hora en la que se realiza el acceso o se intenta el mismo, propósito del acceso, así como fecha y hora de salida;

b) Para soportes físicos: Número o clave del expediente utilizado, y

c) Para soportes electrónicos: Operaciones o acciones llevadas a cabo y registros utilizados de la base de datos.

2. Si las bitácoras están en soporte físico o en soporte electrónico;
3. Lugar dónde almacena las bitácoras y por cuánto tiempo;
4. La manera en que asegura la integridad de las bitácoras

5. Respecto del análisis de las bitácoras:

a) Quién es el responsable de analizarlas (si es el área universitaria o si es un tercero) y cada cuándo las analiza, y

b) Para el caso de que las bitácoras estén en soporte electrónico: las herramientas de análisis utilizadas.

IV. REGISTRO DE INCIDENTES:

No se cuenta con un procedimiento de atención de incidentes

V. ACCESO A LAS INSTALACIONES

1. Seguridad perimetral exterior (las instalaciones del área universitaria):

¿Qué medidas ha implementado para controlar el acceso de personas a sus instalaciones? Por ejemplo, se espera que describa si cuenta con uno o más puntos de control de acceso y quienes los operan, si tiene vigilancia las 24 horas, si ha levantado bardas o cercas, si existe un sistema de tratamiento de datos personales de video vigilancia, entre otras posibles medidas.

La Sede de la UNAM en Boston se ubica en las instalaciones del campus de la Universidad de Massachusetts en esa ciudad. Por lo tanto, la seguridad perimetral exterior es gestionada por dicha institución.

Para las personas que acceden a sus instalaciones:

a) ¿Cómo las identifica?

No se cuenta con mecanismos de identificación.

b) ¿Cómo las autentifica?

No se cuenta con mecanismos de autentificación.

c) ¿Cómo les autoriza el acceso?

No se cuenta con mecanismos de control de accesos.

2. Seguridad perimetral interior (oficina, almacén o bodega para soportes físicos, centro de datos para soportes electrónicos):

¿Qué medidas de seguridad ha implementado para controlar el acceso a los espacios donde almacena los soportes físicos o electrónicos del sistema? Por ejemplo, se espera que precise el tipo de puertas y cerraduras instaladas, si tiene instalados controles biométricos, si administra la asignación de llaves y/o claves de acceso para abrir puertas y/o estantería, si cuenta con vigilancia las 24 horas, si hay un sistema de tratamiento de datos personales de video vigilancia, entre otras medidas.

Las oficinas de UNAM Boston se encuentran abiertas única y exclusivamente cuando algún funcionario de la Sede se encuentra físicamente en las instalaciones. De lo contrario, se encuentran cerradas bajo llave y ninguna persona ajena tiene acceso a los espacios.

Para las personas que acceden a dichos espacios interiores:

a) ¿Cómo las identifica?

El personal de UNAM-Boston dará acceso únicamente a personas citadas previamente o que se identifiquen como miembros de la comunidad de la Universidad de Massachusetts.

b) ¿Cómo las autentifica?

Correo electrónico institucional @umb.edu, credencial oficial de la universidad.

c) ¿Cómo les autoriza el acceso?

A través de un sistema citas.

VI. ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

En este apartado se deberá establecer un mecanismo o procedimiento institucional para la actualización de la información personal contenida en el sistema, en donde se establezca la frecuencia con la que se efectúa y la forma en que se está solicitando al titular acreditar de manera idónea sus requerimientos de rectificación de datos inexactos.

La información contenida en el sistema se actualiza única y exclusivamente por solicitud por escrito de los interesados. Por ejemplo, si al recibir sus recibos de pago o sus constancias de participación identifican alguna inconsistencia en sus datos personales.

Las medidas de seguridad previstas a continuación en los incisos VII al IX, sólo aplican para soportes electrónicos

VII. PERFILES DE USUARIO Y CONTRASEÑAS

En este rubro el área universitaria deberá describir el esquema de perfiles de usuario y contraseñas que tiene implementado para control de acceso mediante una red electrónica.

1. Modelo de control de acceso (alguno de los siguientes):

Está basado en roles.

3. Perfiles de usuario y contraseñas en el sistema operativo de red:

a) ¿Cuenta con un sistema operativo de red instalado en sus equipos?
No
b)
c) ¿Proporciona dicho sistema operativo un manejo riguroso de perfiles de usuario y contraseñas?
No
d) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?
No

3. Perfiles de usuario y contraseñas manejados por el software aplicativo del sistema de tratamiento de datos personales:

a) ¿Ofrece dicho software un manejo riguroso de perfiles de usuario y contraseñas?
Si
b) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?
No

4. Administración de perfiles de usuario y contraseñas:

a) ¿Quién da de alta nuevos perfiles?
El responsable del sistema.
b) ¿Quién autoriza la creación de nuevos perfiles?
El responsable del sistema.
c) ¿Se lleva registro de la creación de nuevos perfiles?
Desde el sistema es posible visualizar la creación de perfiles.

5. Acceso remoto al sistema de tratamiento de datos personales:

a) ¿Requieren los usuarios acceso remoto al equipo de cómputo que por lo general utilizan para trabajar con el sistema?
No, cada usuario puede acceder al sistema desde cualquier equipo con conexión a internet.
b) ¿Requiereeladministradoraccesoremotoalequipodonderesideelsistemapararealizartareasdemantenimiento?
No
c) ¿Cómo se evita el acceso remoto no autorizado?
Se cuenta con controles de acceso basados en roles y privilegios, a través de la autorización de un teléfono o correo administrado por el Coordinador de Relaciones y gestión.

7. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

Herramientas y recursos para monitoreo de la protección de datos personales

(Denominación del área específica del Área Universitaria A)*		
Identificador único*	**BOS-IC**	
(Nombre del sistema A1)*	**UNAM Boston Inscripciones a cursos**	
Recurso*	**Descripción***	**Control***
Monitoreo de la nube (Google Drive)	Supervisión de la nube de parte de la Asistente de Planeación de UNAM Boston.	Revisión digital.
Monitoreo de las contraseñas.	Supervisión de las contraseñas digitales de parte de la Asistente de Planeación de UNAM Boston.	Revisión digital, supervisión y comunicación con el personal que tenga uso de las contraseñas.
Monitoreo del disco duro y archivos digitales.	Supervisión del respaldo del disco duro de parte de Coordinación de Relaciones y Gestión de UNAM Boston.	Revisión digital.
Monitoreo de las instalaciones y del equipo electrónico y de cómputo de trabajo.	Supervisión del disco duro físico y las instalaciones de la sede.	Vigilancia física del recinto y de las herramientas electrónicas de trabajo.
Monitoreo general del tratamiento y archivo de datos personales.	Solicitud anual del Comité de Transparencia de la UNAM, para que se evalúé la adaptación, adecuación y eficacia de los controles, medidas y mecanismos de tratamiento de datos personales.	Solicitud administrativa, posterior a la evaluación del Comité de Transparencia de la UNAM y aplicación de medidas correctivas o de refuerzo para la protección de datos personales.

7.1. Procedimiento para la revisión de las medidas de seguridad

(Denominación del área específica del Área Universitaria A)*		
Identificador único*	**BOS-IC**	
(Nombre del sistema A1)*	**UNAM Boston Inscripciones a cursos**	
Medida de seguridad*	**Procedimiento***	**Responsable***
Supervisión de la nube	La persona Asistente de Planeación revisará que los formularios y demás sistemas se bajen y borren de la nube de Drive.	Asistente de Planeación 1 día
Supervisión de contraseñas	La persona Asistente de Planeación revisará la seguridad de contraseñas robustas para el acceso a la información del disco duro.	Asistente de Planeación 5 días
Supervisión del disco duro y archivos digitales	La persona de Coordinación de Relaciones y Gestión revisará que los datos se guarden en orden y se sigan los protocolos establecidos para la seguridad de los datos personales recogidos por la sede.	Coordinador de Relaciones y Gestión 3 día
Supervisión de las instalaciones y equipo electrónico y de computo	La persona de Coordinación de Relaciones y Gestión vigilará las instalaciones y se asegurará que el disco duro físico esté siempre en buen estado y seguro.	Coordinador de Relaciones y Gestión 1 día
Evaluación anual del Comité de Transparencia de la UNAM.	Se le solicitará una evaluación al Comité de Transparencia de la UNAM de los sistemas y mecanismos de tratamiento de datos personales para seguir con la protección y mejoramiento de éstos.	Comité de Transparencia de la UNAM.

7.2. Resultados de la evaluación y pruebas a las medidas de seguridad

(Denominación del área específica del Área Universitaria A)*		
Identificador único*	**BOS-IC**	
(Nombre del sistema A1)*	**UNAM Boston Inscripciones a cursos**	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***
Evaluación anual de la Unidad de Transparencia de la UNAM.	En proceso.	Representante del Comité de Transparencia de la UNAM.

7.3. Acciones para la corrección y actualización de las medidas de seguridad

(Denominación del área específica del Área Universitaria A)*		
Identificador único*	**BOS-IC**	
(Nombre del sistema A1)*	**UNAM Boston Inscripciones a cursos**	
Medida de seguridad*	**Acciones***	**Responsable***
Evaluación anual del Comité de Transparencia de la UNAM	En proceso	Representante del Comité de Transparencia de la UNAM

8. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

8.1. Programa de capacitación a los responsables de tratamiento de datos personales

(Denominación del área específica del Área Universitaria A)*			
Identificador único*	**BOS-IC**		
(Nombre del sistema A1)*	**UNAM Boston Inscripciones a cursos**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Seguimiento del material documental de: *Normas complementarias sobre medidas de seguridad técnicas, administrativas y físicas para la protección de datos personales en posesión de la universidad.*	Revisión de los protocolos y medidas de las Normas, de las evaluaciones anteriores y actuales, con el fin de asegurar la integridad, confidencialidad y disponibilidad de la información personal que éstos contienen.	1 semana cada mes de Agosto	Todo el equipo de trabajo de la sede

8.2. Programa de difusión de la protección a los datos personales

(Denominación del área específica del Área Universitaria A)*			
Identificador único*	**BOS-IC**		
(Nombre del sistema A1)*	**UNAM Boston Inscripciones a cursos**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Jornada Anual para el mantenimiento y supervisión de tratamiento y archivo de datos personales al equipo de trabajo de la sede	Asesoramiento del Comité de Transparencia de la UNAM y del Coordinador de la sede para evaluar y reforzar el trabajo del equipo en tratamiento de datos personales	1 día	Todo el equipo de trabajo de la sede

9. MEJORA CONTINUA

9.1. Actualización y mantenimiento de sistemas de información

(Denominación del área específica del Área Universitaria A)*			
Identificador único*	**BOS-IC**		
(Nombre del sistema A1)*	**UNAM Boston Inscripciones a cursos**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Supervisión interna de los sistemas de tratamiento y archivo de datos personales.	El Coordinador de la sede realizará jornadas trimestrales o semestrales para supervisar que la nube, las contraseñas, el disco duro, archivos digitales, las instalaciones y el equipo electrónico de trabajo estén dentro de los protocolos establecidos y medidas de seguridad implementadas.	3 días en marzo, 3 días en junio y 3 días en septiembre.	La nube (Google Drive), las contraseñas, el disco duro, archivos digitales, las instalaciones y el equipo electrónico de trabajo.

9.2. Actualización y mantenimiento de equipo de cómputo

(Denominación del área específica del Área Universitaria A)*			
Identificador único*	**BOS-IC**		
(Nombre del sistema A1)*	**UNAM Boston Inscripciones a cursos**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Apoyo del jefe de departamento de Tecnologías de la Información y Comunicación.	Revisión de anomalías que se presenten en el equipo y actualización de los sistemas computacionales que se utilizan en la Sede.	1 día por año	Sistema operativo software utilizado por la Sede.

9.3. Procesos para la conservación, preservación y respaldos de información

(Denominación del área específica del Área Universitaria A)*		
Identificador único*	**BOS-IC**	
(Nombre del sistema A1)*	**UNAM Boston Inscripciones a cursos**	
Proceso*	**Descripción***	**Responsable***
Supervisión interna de los sistemas de tratamiento y archivo de datos personales y del seguimiento de procedimientos y mitigaciones de riesgo por parte del Coordinador de Relaciones y Gestión	Crear contraseñas digitales robustas y controlar accesos a las bases de datos y sistemas de datos personales. Asignar contraseñas a los archivos electrónicos que contengan datos personales. Borrar la información de la nube (Google Drive) y almacenarla en archivos digitales en un disco duro físico seguro con respaldo bajo el manejado del personal autorizado. Agregar cláusula de cesión de derechos sobre datos personales en todo sistema de recopilación de datos. Adquisición de un programa antivirus. Estrategias y protocolos para el uso de llaves y cerraduras de la oficina. Tener un disco duro en la oficina y otro en el domicilio de personal de confianza de la Sede.	**a)** *Coordinador de Relaciones y Gestión, y Asistente de Planeación* **b)** *5 días*

9.4. Procesos de borrado seguro y disposición final de equipos y componentes informáticos

(Denominación del área específica del Área Universitaria A)*		
Identificador único*	**BOS-IC**	
(Nombre del sistema A1)*	**UNAM Boston Inscripciones a cursos**	
Proceso*	**Descripción***	**Responsable***
Borrado electrónico definitivo y eliminación de rastros y copias de los datos.	Borrado permanente de los archivos originales y cualquier copia, rastro o respaldo que pueda quedar en la nube (Google Drive)	**a)** Asistente de Planeación **b)** 5 días

10. PROCEDIMIENTOPARALACANCELACIÓNDEUNSISTEMADE TRATAMIENTO DE DATOS PERSONALES

(Informar y describir el procedimiento para la cancelación de un sistema de tratamiento de datos personales.)

A) DATOSDELSISTEMADE TRATAMIENTO DE DATOS PERSONALES QUESERÁCANCELADO:

a) Denominación
b) Motivo de la cancelación

B) PLAZOS Y CONDICIONES PARA EL BLOQUEO DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES:

(Señalar el periodo de bloqueo, considerando los plazos de prescripción para el ejercicio de algún derecho por parte de los titulares de conformidad con la normatividad de cada área universitaria. Asimismo, se debe señalar las condiciones y el procedimiento que se seguirá para realizar el bloqueo)

C) MEDIDASDESEGURIDADPARAELBLOQUEOYPOSTERIORSUPRESIÓNDELSISTEMA DE TRATAMIENTO DE DATOS PERSONALES:

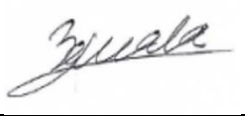
(Describir las medidas de seguridad aplicables al periodo de bloqueo y la supresión del sistema, considerando el nivel de protección requerido en virtud del tipo de datos personales contenidos en el sistema)

D) PROCEDIMIENTO PARA LA SUPRESIÓN DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

(Describir el procedimiento para suprimir el sistema, una vez cumplido el plazo de bloqueo)

E) MECANISMOS PARA LA SUPRESIÓN DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES
(Describir las técnicas para la eliminación física del sistema)

11. APROBACIÓN DEL DOCUMENTO DE SEGURIDAD

		Nombre y firma de quienes revisaron el presente documento:
Responsable del desarrollo:	**Lic. Renata Gatica** Asistente de Planeación planeación@boston.unam.mx 55 1045 4864	Renata Gatica 
Revisó	**Mtro. Héctor Zavala** Coordinador de Relaciones y Gestión Hector.zavala@boston.unam.mx +1(857)333-7591	Héctor Zavala 
Autorizó:	**Mtro. Javier Laguna** Director UNAM-Boston laguna@boston.unam.mx +1 (312) 391-7731	Javier Laguna 
Fecha de aprobación:	(Incluir la fecha de liberación dl documento)	
Fecha de actualización:	(Incluir la primera versión e ir agregando las subsiguientes del documento)	

Inventario de sistemas de tratamiento de datos personales:

UNAM-BOSTON BECARIOS

BOS-BE

1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

UNAM-BOSTON	
Identificador único*	**BOS-BE**
(Nombre del sistema A1) *	**UNAM-BOSTON_BECARIOS**
Datos personales (sensibles o no)contenidos en el sistema*:	Nombre, nacionalidad, correo electrónico, celular, licenciatura, promedio, CURP, comprobante de domicilio.
Responsable*:	
Nombre*:	**Héctor Zavala Guzmán**
Cargo*:	**Coordinación de Relaciones y Gestión**
Funciones*:	Definir el uso que se le dará a los datos personales de los alumnos. Designar a los encargados del sistema que tendrán acceso a los datos personales. Comunicar con los encargados del sistema las políticas de uso de los datos personales.
Obligaciones*:	• Mantener la protección de datos personales contenidos en el sistema implementando las medidas de seguridad. • No difundir datos personales de los alumnos. • No modificar la información almacenada en el servidor No hacer respaldos en equipo personal de la información de datos personales.
	Encargados:
(Nombre del Encargado 1*)	**Renata Gatica**
Cargo*:	**Planeación**
Funciones*:	• Establecer comunicación con los alumnos durante el proceso de selección. • Validar y archivar los documentos que contienen los datos personales de los alumnos registrados.
Obligaciones*:	• Mantener la protección de datos personales contenidos en el sistema implementando las medidas de seguridad. • No difundir datos personales de los alumnos. • No modificar la información almacenada en el servidor No hacer respaldos en equipo personal de la información de datos personales.

2. ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

UNAM-BOSTON	
Identificador único¨*	**BOS-BE**
(Nombre del sistema A1*)	**UNAM-BOSTON_BECARIOS**
Tipo de soporte:*	Electrónico
Descripción:*	Base de datos
Características del lugar donde se resguardan los soportes:*	Alojamiento en la nube privada en Google Drive a la que solo pueden acceder usuarios autorizados por el responsable del sistema.

3. ANÁLISIS DE RIESGOS

UNAM-BOSTON		
Identificador único*	**BOS-BE**	
(Nombre del sistema A1) *	**UNAM-BOSTON BECARIOS**	
Riesgo*	**Impacto***	**Mitigación***
Hackeo de los correos electrónicos de los usuarios del sistema.	Perdida de documentación. Acceso y alteración de datos personales.	Contraseñas fuertes. Controlar accesos. Respaldar y borrar la información de la nube una vez concluido el curso.
Almacenamiento de datos personales en la nube.	Filtraciones y acceso a la información.	Borrar información de la nube y almacenarlo en un disco duro físico, bajo el manejado del personal autorizado.
Vulnerabilidad jurídica al no solicitar permiso de uso y almacenamiento de datos al titular.	Caer en responsabilidad jurídica por usar datos sin consentimiento.	Agregar cláusula de cesión de derechos sobre datos personales.
Infección del equipo de cómputo de la Sede por virus y malware.	Pérdida y filtración de información.	Evitar el uso de cómputo de la sede para navegar sitios web no relacionados a las actividades de la sede. Adquisición de un programa antivirus.
Robo del equipo de cómputo.	Pérdida y filtración de información.	Estrategias y protocolos para el uso de llaves y cerraduras de la oficina. Tener un disco duro en la oficina y otro en el domicilio de personal de confianza de la Sede.

4. ANÁLISIS DE BRECHA

UNAM-BOSTON		
Identificador único*	**BOS-BE**	
(Nombre del sistema A1) *	**UNAM-BOSTON_BECARIOS**	
Medida de seguridad actual*	**Medida de seguridad necesaria***	**Acciones para remediación***
Designar usuarios autorizados para el monitoreo de datos personales.	Definir contraseñas robustas para los usuarios del sistema	Tener un protocolo de contraseñas seguras y actualizar cada semestre.
No se cuentan con expedientes físicos en los que aparezcan datos personales de los alumnos para evitar su extravió y mal uso de la información	Correcto	No es necesario
Almacenamiento de datos en la nube.	Respaldo digital en almacenamiento de disco duro físico	Adquirir disco duro, bajar y eliminar información de la nube.

5. PLAN DE TRABAJO

UNAM-BOSTON			
Identificador único*	**BOS-BE**		
(Nombre del sistema A1) *	**UNAM-BOSTON_BECARIOS**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Indique actividad. Agregar un renglón por cada elemento	Describa el tipo de actividad, sus objetivos e impacto en la protección de datos personales	Indique duración en la ejecución de la actividad en horas, días, meses, su fecha de inicio y de término	Mencione los aspectos de la protección a datos personales que son resueltos, total o parcialmente, por la actividad.

6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

I. TRANSFERENCIAS DE DATOS PERSONALES

UNAM-BOSTON	
Identificador único*	**BOS-BE**
(Nombre del sistema A1)*	**UNAM-BOSTON BECARIOS**
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	No aplica
Transferencias mediante el traslado de soportes electrónicos:	• Se comparte de manera digital la información que contiene los datos personales de los alumnos con la Coordinación de Relaciones y Asuntos Internacionales como parte de la entrega de informes académicos y administrativos. • Se comparte de manera digital información con los responsables de la Red Universitaria de responsables de Internacionalización.
Transferencias mediante el traslado sobre redes electrónicas:	No aplica

II. RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS

El sistema UNAM-Boston Becarios no realiza tratamientos de datos personales son soportes físicos, ya que se encuentran en soporte electrónico mediante el uso de una base de datos.

i. Señalar las medidas de seguridad que ha implementado el área universitaria para el resguardo de los soportes físicos del sistema de manera que evite la alteración, pérdida o acceso no autorizado a los mismos.

ii. Señalar en un listado las personas (nombre, cargo, funciones y obligaciones) que tienen acceso a los soportes físicos del sistema.

III. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

1. Los datos que se registran en las bitácoras:

c) Quién accede a los Datos personales, fecha y hora en la que se realiza el acceso o se intenta el mismo, propósito del acceso, así como fecha y hora de salida;

d) Para soportes físicos: Número o clave del expediente utilizado

e) Para soportes electrónicos: Operaciones o acciones llevadas a cabo y registros utilizados de la base de datos.

2. Si las bitácoras están en soporte físico o en soporte electrónico;

3. Lugar dónde almacena las bitácoras y por cuánto tiempo;

4. La manera en que asegura la integridad de las bitácoras, y

5. Respecto del análisis de las bitácoras:

a) Quién es el responsable de analizarlas (si es el área universitaria o si es un tercero) y cada cuándo las analiza

b) Para el caso de que las bitácoras estén en soporte electrónico: las herramientas de análisis utilizadas.

IV. REGISTRO DE INCIDENTES:

No se cuenta con un procedimiento de atención de incidentes

V. ACCESO A LAS INSTALACIONES

1. Seguridad perimetral exterior (las instalaciones del área universitaria):

¿Qué medidas ha implementado para controlar el acceso de personas a sus instalaciones? Por ejemplo, se espera que describa si cuenta con uno o más puntos de control de acceso y quienes los operan, si tiene vigilancia las 24 horas, si ha levantado bardas o cercas, si existe un sistema de tratamiento de datos personales de video vigilancia, entre otras posibles medidas.

La Sede de la UNAM en Boston se ubica en las instalaciones del campus de la Universidad de Massachusetts en esa ciudad. Por lo tanto, la seguridad perimetral exterior es gestionada por dicha institución.

Para las personas que acceden a sus instalaciones:

a) ¿Cómo las identifica?
No se cuenta con mecanismos de identificación
b) ¿Cómo las autentifica?
No se cuenta con los mecanismos de autentificación
c) ¿Cómo los autoriza?
No se cuenta con mecanismos de control de accesos

2. Seguridad perimetral interior (oficina, almacén o bodega para soportes físicos, centro de datos para soportes electrónicos):

¿Qué medidas de seguridad ha implementado para controlar el acceso a los espacios donde almacena los soportes físicos o electrónicos del sistema? Por ejemplo, se espera que precise el tipo de puertas y cerraduras instaladas, si tiene instalados controles biométricos, si administra la asignación de llaves y/o claves de acceso para abrir puertas y/o estantería, si cuenta con vigilancia las 24 horas, si hay un sistema de tratamiento de datos personales de video vigilancia, entre otras medidas.

Las oficinas de UNAM Boston se encuentran abiertas única y exclusivamente cuando algún funcionario de la Sede se encuentra físicamente en las instalaciones. De lo contrario, se encuentran cerradas bajo llave y ninguna persona ajena tiene acceso a los espacios.

Para las personas que acceden a dichos espacios interiores:

a) ¿Cómo las identifica?
El personal de UNAM-Boston dará acceso únicamente a personas citadas previamente o que se identifiquen como miembros de la comunidad de la Universidad de Massachusetts.
b) ¿Cómo las autentifica?
Correo electrónico institucional @umb.edu, credencial oficial de la universidad.
c) ¿Cómo los autoriza?
A través de un sistema citas.

VI. ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

En este apartado se deberá establecer un mecanismo o procedimiento institucional para la actualización de la información personal contenida en el sistema, en donde se establezca la frecuencia con la que se efectúa y la forma en que se está solicitando al titular acreditar de manera idónea sus requerimientos de rectificación de datos inexactos.

Las medidas de seguridad previstas a continuación en los incisos VII a XI, sólo aplican para soportes electrónicos

VII. PERFILES DE USUARIO Y CONTRASEÑAS

En este rubro el área universitaria deberá describir el esquema de perfiles de usuario y contraseñas que tiene implementado para control de acceso mediante una red electrónica.

1. Modelo de control de acceso (alguno de los siguientes):

Está basado en roles

2. Perfiles de usuario y contraseñas en el sistema operativo de red:

a) ¿Cuenta con un sistema operativo de red instalado en sus equipos?
No
c) ¿Proporciona dicho sistema operativo un manejo riguroso de perfiles de usuario y contraseñas?
No
d) ¿Cifraelmencionadosoftwarelosnombresdeusuarioylascontraseñascuandolosalmacena?
No

3. Perfiles de usuario y contraseñas manejados por el software aplicativo del sistema de tratamiento de datos personales:

a) ¿Ofrece dicho software un manejo riguroso de perfiles de usuario y contraseñas?
Si
b) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?
Si

4. Administración de perfiles de usuario y contraseñas:

a) ¿Quién da de alta nuevos perfiles?
Los usuarios sin privilegios administrativos pueden darse de alta en el sistema por sí mismos, con el fin de registrarse a eventos académicos o culturales.
b) ¿Quién autoriza la creación de nuevos perfiles?
El responsable del sistema.
c) ¿Se lleva registro de la creación de nuevos perfiles?
Desde el sistema es posible visualizar la creación de perfiles.

5. Acceso remoto al sistema de tratamiento de datos personales:

a) ¿Requieren los usuarios acceso remoto al equipo de cómputo que por lo general utilizan para trabajar con el sistema?
No, cada usuario puede acceder al sistema desde cualquier equipo con conexión a internet.
b) ¿Requiere el administrador acceso remoto al equipo donde reside el sistema para realizar tareas de mantenimiento?
No
c) ¿Cómo se evita el acceso remoto no autorizado?
Se cuenta con controles de acceso basados en roles y privilegios, a través de la autorización de un teléfono o correo administrado por el Coordinador de Relaciones y gestión

7. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

7.1 Herramientas y recursos para monitoreo de la protección de datos personales

(Denominación del área específica del Área Universitaria A)*		
Identificador único*	**BOS-BE**	
(Nombre del sistema A1)*	**UNAM-BOSTON BECARIOS**	
Recurso*		
Monitoreo de la nube (Google Drive)	Supervisión de la nube de parte de la Asistente de Planeación de UNAM Boston.	Revisión digital.
Monitoreo de las contraseñas	Supervisión de las contraseñas digitales de parte de la Asistente de Planeación de UNAM Boston.	Revisión digital, supervisión y comunicación con el personal que tenga uso de las contraseñas.
Monitoreo del disco duro y archivos digitales	Supervisión del respaldo del disco duro de parte de Coordinación de Relaciones y Gestión de UNAM Boston.	Revisión digital.
Monitoreo de las instalaciones y del equipo electrónico y de cómputo de trabajo	Supervisión del disco duro físico y las instalaciones de la sede.	Vigilancia física del recinto y de las herramientas electrónicas de trabajo.
Monitoreo general del tratamiento y archivo de datos personales.	Solicitud anual del Comité de Transparencia de la UNAM, para que se evalúa la adaptación, adecuación y eficacia de los controles, medidas y mecanismos de tratamiento de datos personales.	Solicitud administrativa, posterior a la evaluación del Comité de Transparencia de la UNAM y aplicación de medidas correctivas o de refuerzo para la protección de datos personales.

7.2 Procedimiento para la revisión de las medidas de seguridad

(Denominación del área específica del Área Universitaria A)*		
Identificador único*	**BOS-BE**	
(Nombre del sistema A1)*	**UNAM-BOSTON BECARIOS**	
Medida de seguridad*	**Procedimiento***	**Responsable***
Supervisión de la nube	La persona Asistente de Planeación revisará que los formularios y demás sistemas se bajen y borren de la nube de Drive.	Asistente de Planeación 1 día
Supervisión de contraseñas	La persona Asistente de Planeación revisará la seguridad de contraseñas robustas para el acceso a la información del disco duro.	Asistente de Planeación 5 días
Supervisión del disco duro y archivos digitales	La persona de Coordinación de Relaciones y Gestión revisará que los datos se guarden en orden y se sigan los protocolos establecidos para la seguridad de los datos personales recogidos por la sede.	Coordinador de Relaciones y Gestión 3 día
Supervisión de las instalaciones y equipo electrónico y de computo	La persona de Coordinación de Relaciones y Gestión vigilará las instalaciones y se asegurará que el disco duro físico esté siempre en buen estado y seguro.	Coordinador de Relaciones y Gestión 1 día
Evaluación anual del Comité de Transparencia de la UNAM	Se le solicitará una evaluación al Comité de Transparencia de la UNAM de los sistemas y mecanismos de tratamiento de datos personales para seguir con la protección y mejoramiento de éstos.	Comité de Transparencia de la UNAM

7.3 Resultados de la evaluación y pruebas a las medidas de seguridad

(Denominación del área específica del Área Universitaria A)*		
Identificador único*	**BOS-BE**	
(Nombre del sistema A1)*	**UNAM-BOSTON BECARIOS**	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***
Evaluación anual de la Unidad de Transparencia de la UNAM.	En proceso.	Representante del Comité de Transparencia de la UNAM.

7.4 Acciones para la corrección y actualización de las medidas de seguridad

(Denominación del área específica del Área Universitaria A)*		
Identificador único*	**BOS-BE**	
(Nombre del sistema A1)*	**UNAM-BOSTON BECARIOS**	
Medida de seguridad*	**Acciones***	**Responsable***
Evaluación anual del Comité de Transparencia de la UNAM.	En proceso	Representante del Comité de Transparencia de la UNAM.

8 PROGRAMA ESPECÍFICO DE CAPACITACIÓN

8.1 Programa de capacitación a los responsables de tratamiento de datos personales

(Denominación del área específica del Área Universitaria A)*			
Identificador único*	**BOS-BE**		
(Nombre del sistema A1)*	**UNAM-BOSTON BECARIOS**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Seguimiento del material documental de: *Normas complementarias sobre medidas de seguridad técnicas, administrativas y físicas para la protección de datos personales en posesión de la universidad.*	Revisión de los protocolos y medidas de las Normas, de las evaluaciones anteriores y actuales, con el fin de asegurar la integridad, confidencialidad y disponibilidad de la información personal que éstos contienen.	1 semana cada mes de Agosto	Todo el equipo de trabajo de la sede.

8.2 Programa de difusión de la protección a los datos personales

(Denominación del área específica del Área Universitaria A)*			
Identificador único*	**BOS-BE**		
(Nombre del sistema A1)*	**UNAM-BOSTON BECARIOS**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Jornada Anual para el mantenimiento y supervisión de tratamiento y archivo de datos personales al equipo de trabajo de la sede.	Asesoramiento del Comité de Transparencia de la UNAM y del Coordinador de la sede para evaluar y reforzar el trabajo del equipo en tratamiento de datos personales.	1 día	Todo el equipo de trabajo de la sede.

9 MEJORA CONTINUA

9.1 Actualización y mantenimiento de sistemas de información

(Denominación del área específica del Área Universitaria A)*			
Identificador único*	**BOS-BE**		
(Nombre del sistema A1)*	**UNAM-BOSTON BECARIOS**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Supervisión interna de los sistemas de tratamiento y archivo de datos personales	El Coordinador de la sede realizará jornadas trimestrales o semestrales para supervisar que la nube, las contraseñas, el disco duro, archivos digitales, las instalaciones y el equipo electrónico de trabajo estén dentro de los protocolos establecidos y medidas de seguridad implementadas	3 días en marzo, 3 días en junio y 3 días en septiembre	La nube (Google Drive), las contraseñas, el disco duro, archivos digitales, las instalaciones y el equipo electrónico de trabajo

9.2 Actualización y mantenimiento de equipo de cómputo

(Denominación del área específica del Área Universitaria A)*			
Identificador único*	**BOS-BE**		
(Nombre del sistema A1)*	**UNAM-BOSTON BECARIOS**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Apoyo del jefe de departamento de Tecnologías de la Información y Comunicación.	Revisión de anomalías que se presenten en el equipo y actualización de los sistemas computacionales que se utilizan en la Sede.	1 día por año	Sistema operativo software utilizado por la Sede.

9.3 Procesos para la conservación, preservación y respaldos de información

(Denominación del área específica del Área Universitaria A)*		
Identificador único*	**BOS-BE**	
(Nombre del sistema A1)*	**UNAM-BOSTON BECARIOS**	
Proceso*	**Descripción***	**Responsable***
Supervisión interna de los sistemas de tratamiento y archivo de datos personales y del seguimiento de procedimientos y mitigaciones de riesgo por parte del Coordinador de Relaciones y Gestión	Crear contraseñas digitales robustas y controlar accesos a las bases de datos y sistemas de datos personales. Asignar contraseñas a los archivos electrónicos que contengan datos personales. Borrar la información de la nube (Google Drive) y almacenarla en archivos digitales en un disco duro físico seguro con respaldo bajo el manejado del personal autorizado. Agregar cláusula de cesión de derechos sobre datos personales en todo sistema de recopilación de datos. Adquisición de un programa antivirus. Estrategias y protocolos para el uso de llaves y cerraduras de la oficina. Tener un disco duro en la oficina y otro en el domicilio de personal de confianza de la Sede.	**f)** Coordinador de Relaciones y Gestión, y Asistente de Planeación **g)** 5 días

9.4 Procesos de borrado seguro y disposición final de equipos y componentes informáticos

(Denominación del área específica del Área Universitaria)*		
Identificador único*	**BOS-BE**	
(Nombre del sistema A1)*	**UNAM-BOSTON BECARIOS**	
Proceso*	**Descripción***	**Responsable***
Borrado electrónico definitivo y eliminación de rastros y copias de los datos.	Borrado permanente de los archivos originales y cualquier copia, rastro o respaldo que pueda quedar en la nube (Google Drive)	**e)** Asistente de Planeación **f)** 5 días

10 PROCEDIMIENTOPARALACANCELACIÓNDEUNSISTEMADE TRATAMIENTO DE DATOS PERSONALES

(Informar y describir el procedimiento para la cancelación de un sistema de tratamiento de datos personales.)

F) DATOSDELSISTEMADE TRATAMIENTO DE DATOS PERSONALES QUESERÁCANCELADO:

a) Denominación
b) Motivo de la cancelación

G) PLAZOS Y CONDICIONES PARA EL BLOQUEO DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES:

(Señalar el periodo de bloqueo, considerando los plazos de prescripción para el ejercicio de algún derecho por parte de los titulares de conformidad con la normatividad de cada área universitaria. Así mismo, se debe señalar las condiciones y el procedimiento que se seguirá para realizar el bloqueo)

H) MEDIDAS DE SEGURIDAD PARA EL BLOQUEO Y POSTERIOR SUPRESIÓN DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES:
(Describir las medidas de seguridad aplicables al periodo de bloqueo y la supresión del sistema, considerando el nivel de protección requerido en virtud del tipo de Datos personales contenidos en el sistema)

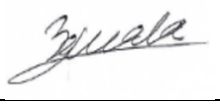
I) PROCEDIMIENTO PARA LA SUPRESIÓN DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

(Describir el procedimiento para suprimir el sistema, una vez cumplido el plazo de bloqueo)

J) MECANISMOS PARA LA SUPRESIÓN DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

(Describir las técnicas para la eliminación física del sistema)

11. APROBACIÓN DEL DOCUMENTO DE SEGURIDAD

		Nombre y firma de quienes revisaron el presente documento:
Responsable del desarrollo:	**Lic. Renata Gatica** Asistente de Planeación planeación@boston.unam.mx 55 1045 4864	Renata Gatica 
Revisó:	**Mtro. Héctor Zavala** Coordinador de Relaciones y Gestión Hector.zavala@boston.unam.mx +1 (857) 333-7591	Héctor Zavala 
Autorizó:	**Mtro. Javier Laguna** Director UNAM-Boston laguna@boston.unam.mx +1 (312) 391-7731	Javier Laguna 
Fecha de aprobación:	(Incluir la fecha de liberación del documento)	
Fecha de actualización:	(Incluir la primera versión e ir agregando las subsiguientes del documento)	

Inventario de sistemas de tratamiento de datos personales:

UNAM Boston Inscripciones a cursos

BOS-PEU

1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

UNAM-BOSTON	
Identificador único*	**BOS-PEU**
(Nombre del sistema A1) *	**PRE-REGISTRO DE SELECCIÓN EXAMEN UNAM**
Datos personales (sensibles o no)contenidos en el sistema*:	Nombre, nacionalidad, correo electrónico, celular, licenciatura, promedio, CURP, comprobante de domicilio.
Responsable*:	
Nombre*:	**Héctor Zavala Guzmán**
Cargo*:	**Coordinación de Relaciones y Gestión**
Funciones*:	• Definir el uso que se le dará a los datos personales de los alumnos. • Designar a los encargados del sistema que tendrán acceso a los datos personales. • Comunicar con los encargados del sistema las políticas de uso de los datos personales.
Obligaciones*:	• Mantener la protección de datos personales contenidos en el sistema implementando las medidas de seguridad. • No difundir datos personales de los alumnos. • No modificar la información almacenada en el servidor No hacer respaldos en equipo personal de la información de datos personales.
	Encargados:
(Nombre del Encargado 1*)	**Renata Gatica**
Cargo*:	**Planeación**
Funciones*:	• Validar la información de los registrados que son candidatos para presentar el examen de selección en la Sede de Boston. • Establecer comunicación con los alumnos durante el proceso de selección.
Obligaciones*:	• Mantener la protección de datos personales contenidos en el sistema implementando las medidas de seguridad. • No difundir datos personales de los alumnos. • No modificar la información almacenada en el servidor No hacer respaldos en equipo personal de la información de datos personales.

2. ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

UNAM-BOSTON	
Identificador único*	**BOS-PEU**
(Nombre del sistema A1*)	**PRE-REGISTRO DE SELECCIÓN EXAMEN UNAM**
Tipo de soporte:*	Electrónico
Descripción:*	Base de datos
Características del lugar donde se resguardan los soportes:*	• Nube privada en Google Drive a la que solo pueden acceder usuarios autorizados por el responsable del sistema. • Equipo de cómputo de la Sede. • Disco duro externo de la Sede.

3. ANÁLISIS DE RIESGOS

UNAM-BOSTON		
Identificador único*	**BOS-PEU**	
(Nombre del sistema A1) *	**PRE-REGISTRO DE SELECCIÓN EXAMEN UNAM**	
Riesgo*	**Impacto***	**Mitigación***
Hackeo de los correos electrónicos de los usuarios del sistema.	Perdida de documentación. Acceso y alteración de datos personales.	Contraseñas fuertes. Controlar accesos. Respaldar y borrar la información de la nube una vez concluido el curso.
Almacenamiento de datos personales en la nube.	Filtraciones y acceso a la información.	Borrar información de la nube y almacenarlo en un disco duro físico, bajo el manejado del personal autorizado.
Vulnerabilidad jurídica al no solicitar permiso de uso y almacenamiento de datos al titular.	Caer en responsabilidad jurídica por usar datos sin consentimiento.	Agregar cláusula de cesión de derechos sobre datos personales.
Infección del equipo de cómputo de la Sede por virus y malware.	Pérdida y filtración de información.	Evitar el uso de cómputo de la sede para navegar sitios web no relacionados a las actividades de la sede. Adquisición de un programa antivirus.
Robo del equipo de cómputo.	Pérdida y filtración de información.	Estrategias y protocolos para el uso de llaves y cerraduras de la oficina. Tener un disco duro en la oficina y otro en el domicilio de personal de confianza de la Sede.

4. ANÁLISIS DE BRECHA

UNAM-BOSTON		
Identificador único*	**BOS-PEU**	
(Nombre del sistema A1) *	**PRE-REGISTRO DE SELECCIÓN EXAMEN UNAM**	
Medida de seguridad actual*	**Medida de seguridad necesaria***	**Acciones para remediación***
Designar usuarios autorizados para el monitoreo de datos personales.	Definir contraseñas robustas para los usuarios del sistema	Tener un protocolo de contraseñas seguras y actualizar cada semestre.
No se cuentan con expedientes físicos en los que aparezcan datos personales de los alumnos para evitar su extravió y mal uso de la información	Correcto	No es necesario
Almacenamiento de datos en la nube.	Respaldo digital en almacenamiento de disco duro físico	Adquirir disco duro, bajar y eliminar información de la nube.

5. PLAN DE TRABAJO

UNAM-BOSTON			
Identificador único*	**BOS-PEU**		
(Nombre del sistema A1) *	**PRE-REGISTRO DE SELECCIÓN EXAMEN UNAM**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Indique actividad. Agregar un renglón por cada elemento	Describa el tipo de actividad, sus objetivos e impacto en la protección de datos personales	Indique duración en la ejecución de la actividad en horas, días, meses, su fecha de inicio y de término	Mencione los aspectos de la protección a datos personales que son resueltos, total o parcialmente, por la actividad.

6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

I. TRANSFERENCIAS DE DATOS PERSONALES

UNAM-BOSTON	
Identificador único*	**BOS-PEU**
(Nombre del sistema A1)*	**PRE-REGISTRO DE SELECCIÓN EXAMEN UNAM**
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	No aplica
Transferencias mediante el traslado de soportes electrónicos:	Se comparte de manera digital la información que contiene los datos personales de los alumnos con la Coordinación de Relaciones y Asuntos Internacionales como parte de la entrega de informes académicos y administrativos.
Transferencias mediante el traslado sobre redes electrónicas:	No aplica

II. RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS

El sistema de Pre-registro de selección examen UNAM no realiza tratamientos de datos personales son soportes físicos, ya que se encuentran en soporte electrónico mediante el uso de una base de datos.

i. Señalar las medidas de seguridad que ha implementado el área universitaria para el resguardo de los soportes físicos del sistema de manera que evite la alteración, pérdida o acceso no autorizado a los mismos.
ii. Señalar en un listado las personas (nombre, cargo, funciones y obligaciones) que tienen acceso a los soportes físicos del sistema.

III. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

1. Los datos que se registran en las bitácoras:

i. Quién accede a los Datos personales, fecha y hora en la que se realiza el acceso o se intenta el mismo, propósito del acceso, así como fecha y hora de salida;

ii. Para soportes físicos: Número o clave del expediente utilizado, y
iii. Para soportes electrónicos: Operaciones o acciones llevadas a cabo y registros utilizados de la base de datos.
3. Si las bitácoras están en soporte físico o en soporte electrónico;
4. Lugar dónde almacena las bitácoras y por cuánto tiempo;
5. La manera en que asegura la integridad de las bitácoras, y
6. Respecto del análisis de las bitácoras:

a) Quién es el responsable de analizar las (si es el área universitaria o si es un tercero) y cada cuándo las analiza, y
b) Para el caso de que las bitácoras estén en soporte electrónico: las herramientas de análisis utilizadas.

IV. REGISTRO DE INCIDENTES:

No se cuenta con un procedimiento de atención de incidentes

V. ACCESO A LAS INSTALACIONES

1. Seguridad perimetral exterior (las instalaciones del área universitaria):

¿Qué medidas ha implementado para controlar el acceso de personas a sus instalaciones? Por ejemplo, se espera que describa si cuenta con uno o más puntos de control de acceso y quienes los operan, si tiene vigilancia las 24 horas, si ha levantado bardas o cercas, si existe un sistema de tratamiento de datos personales de video vigilancia, entre otras posibles medidas.

La Sede de la UNAM en Boston se ubica en las instalaciones del campus de la Universidad de Massachusetts en esa ciudad. Por lo tanto, la seguridad perimetral exterior es gestionada por dicha institución.

Para las personas que acceden a sus instalaciones:

a) ¿Cómo las identifica?
No se cuenta con mecanismos de identificación
b) ¿Cómo las autentifica?
No se cuenta con los mecanismos de autentificación
c) ¿Cómo los autoriza?
No se cuenta con mecanismos de control de accesos

2. Seguridad perimetral interior (oficina, almacén o bodega para soportes físicos, centro de datos para soportes electrónicos):

¿Qué medidas de seguridad ha implementado para controlar el acceso a los espacios donde almacena los soportes físicos o electrónicos del sistema? Por ejemplo, se espera que precise el tipo de puertas y cerraduras instaladas, si tiene instalados controles biométricos, si administra la asignación de llaves y/o claves de acceso para abrir puertas y/o estantería, si cuenta con vigilancia las 24 horas, si hay un sistema de tratamiento de datos personales de video vigilancia, entre otras medidas.

Las oficinas de UNAM Boston se encuentran abiertas única y exclusivamente cuando algún funcionario de la Sede se encuentra físicamente en las instalaciones. De lo contrario, se encuentran cerradas bajo llave y ninguna persona ajena tiene acceso a los espacios.

Para las personas que acceden a dichos espacios interiores:

a) ¿Cómo las identifica?
El personal de UNAM-Boston dará acceso únicamente a personas citadas previamente o que se identifiquen como miembros de la comunidad de la Universidad de Massachusetts.
b) ¿Cómo las autentifica?
Correo electrónico institucional @umb.edu, credencial oficial de la universidad.
c) ¿Cómo les autoriza el acceso?
A través de un sistema citas.

VI. ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

En este apartado se deberá establecer un mecanismo o procedimiento institucional para la actualización de la información personal contenida en el sistema, en donde se establezca la frecuencia con la que se efectúa y la forma en que se está solicitando al titular acreditar de manera idónea sus requerimientos de rectificación de datos inexactos.

Las medidas de seguridad previstas a continuación en los incisos VII a XI, sólo aplican para soportes electrónicos

VII. PERFILES DE USUARIO Y CONTRASEÑAS

En este rubro el área universitaria deberá describir el esquema de perfiles de usuario y contraseñas que tiene implementado para control de acceso mediante una red electrónica.

1. Modelo de control de acceso (alguno de los siguientes):

Está basado en roles

2. Perfiles de usuario y contraseñas en el sistema operativo de red:

a) ¿Cuenta con un sistema operativo de red instalado en sus equipos?
No
b) ¿Proporciona dicho sistema operativo un manejo riguroso de perfiles de usuario y contraseñas?
No
c) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?
No

3. Perfiles de usuario y contraseñas manejados por el software aplicativo del sistema de tratamiento de datos personales:

a) ¿Ofrece dicho software un manejo riguroso de perfiles de usuario y contraseñas?
Si
b) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?
No

4. Administración de perfiles de usuario y contraseñas:

a) ¿Quién da de alta nuevos perfiles?
El responsable del sistema.
b) ¿Quién autoriza la creación de nuevos perfiles?
El responsable del sistema.
c) ¿Se lleva registro de la creación de nuevos perfiles?
Desde el sistema es posible visualizar la creación de perfiles.

5. Acceso remoto al sistema de tratamiento de datos personales:

a) ¿Requieren los usuarios acceso remoto al equipo de cómputo que por lo general utilizan para trabajar con el sistema?

No, cada usuario puede acceder al sistema desde cualquier equipo con conexión a internet.

b) ¿Requiere el administrador acceso remoto al equipo donde reside el sistema para realizar tareas de mantenimiento?

No

c) ¿Cómo se evita el acceso remoto no autorizado?

Se cuenta con controles de acceso basados en roles y privilegios, a través de la autorización de un teléfono o correo administrado por el Coordinador de Relaciones y gestión.

7. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

7.1 Herramientas y recursos para monitoreo de la protección de datos personales

(Denominación del área específica del Área Universitaria A)*		
Identificador único*	**BOS-PEU**	
(Nombre del sistema A1)*	**PRE-REGISTRO DE SELECCIÓN EXAMEN UNAM**	
Recurso*	**Descripción***	**Control***
Monitoreo de la nube (Google Drive)	Supervisión de la nube de parte de la Asistente de Planeación de UNAM Boston.	Revisión digital.
Monitoreo de las contraseñas	Supervisión de las contraseñas digitales de parte de la Asistente de Planeación de UNAM Boston.	Revisión digital, supervisión y comunicación con el personal que tenga uso de las contraseñas.
Monitoreo del disco duro y archivos digitales	Supervisión del respaldo del disco duro de parte de Coordinación de Relaciones y Gestión de UNAM Boston.	Revisión digital.
Monitoreo de las instalaciones y del equipo electrónico y de cómputo de trabajo	Supervisión del disco duro físico y las instalaciones de la sede.	Vigilancia física del recinto y de las herramientas electrónicas de trabajo.
Monitoreo general del tratamiento y archivo de datos personales.	Solicitud anual del Comité de Transparencia de la UNAM, para que se evalúé la adaptación, adecuación y eficacia de los controles, medidas y mecanismos de tratamiento de datos personales.	Solicitud administrativa, posterior a la evaluación del Comité de Transparencia de la UNAM y aplicación de medidas correctivas o de refuerzo para la protección de datos personales.

7.2 Procedimiento para la revisión de las medidas de seguridad

(Denominación del área específica del Área Universitaria A)*		
Identificador único*	**BOS-PEU**	
(Nombre del sistema A1)*	**PRE-REGISTRO DE SELECCIÓN EXAMEN UNAM**	
Medida de seguridad*	**Procedimiento***	**Responsable***
Supervisión de la nube	La persona Asistente de Planeación revisará que los formularios y demás sistemas se bajen y borren de la nube de Drive.	Asistente de Planeación 1 día
Supervisión de contraseñas	La persona Asistente de Planeación revisará la seguridad de contraseñas robustas para el acceso a la información del disco duro.	Asistente de Planeación 5 días
Supervisión del disco duro y archivos digitales	La persona de Coordinación de Relaciones y Gestión revisará que los datos se guarden en orden y se sigan los protocolos establecidos para la seguridad de los datos personales recogidos por la sede.	Coordinador de Relaciones y Gestión 3 día
Supervisión de las instalaciones y equipo electrónico y de computo	La persona de Coordinación de Relaciones y Gestión vigilará las instalaciones y se asegurará que el disco duro físico esté siempre en buen estado y seguro.	Coordinador de Relaciones y Gestión 1 día
Evaluación anual del Comité de Transparencia de la UNAM	Se le solicitará una evaluación al Comité de Transparencia de la UNAM de los sistemas y mecanismos de tratamiento de datos personales para seguir con la protección y mejoramiento de éstos.	Comité de Transparencia de la UNAM

7.3 Resultados de la evaluación y pruebas a las medidas de seguridad

(Denominación del área específica del Área Universitaria A)*		
Identificador único*	**BOS-PEU**	
(Nombre del sistema A1)*	**PRE-REGISTRO DE SELECCIÓN EXAMEN UNAM**	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***
Evaluación anual de la Unidad de Transparencia de la UNAM	En proceso	Representante del Comité de Transparencia de la UNAM

7.4 Acciones para la corrección y actualización de las medidas de seguridad

(Denominación del área específica del Área Universitaria A)*		
Identificador único*	**BOS-PEU**	
(Nombre del sistema A1)*	**PRE-REGISTRO DE SELECCIÓN EXAMEN UNAM**	
Medida de seguridad*	**Acciones***	**Responsable***
Evaluación anual del Comité de Transparencia de la UNAM.	En proceso.	Representante del Comité de Transparencia de la UNAM.

8 PROGRAMA ESPECÍFICO DE CAPACITACIÓN

8.1 Programa de capacitación a los responsables de tratamiento de datos personales

(Denominación del área específica del Área Universitaria A)*			
Identificador único*	**BOS-IC**		
(Nombre del sistema A1)*	**UNAM Boston Inscripciones a cursos**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Seguimiento del material documental de: *Normas complementarias sobre medidas de seguridad técnicas, administrativas y físicas para la protección de datos personales en posesión de la universidad.*	Revisión de los protocolos y medidas de las Normas, de las evaluaciones anteriores y actuales, con el fin de asegurar la integridad, confidencialidad y disponibilidad de la información personal que éstos contienen.	1 semana cada mes de Agosto	Todo el equipo de trabajo de la sede.

8.2 Programa de difusión de la protección a los datos personales

(Denominación del área específica del Área Universitaria A)*			
Identificador único*	**BOS-PEU**		
(Nombre del sistema A1)*	**PRE-REGISTRO DE SELECCIÓN EXAMEN UNAM**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Jornada Anual para el mantenimiento y supervisión de tratamiento y archivo de datos personales al equipo de trabajo de la sede	Asesoramiento del Comité de Transparencia de la UNAM y del Coordinador de la sede para evaluar y reforzar el trabajo del equipo en tratamiento de datos personales	1 día	Todo el equipo de trabajo de la sede

9 MEJORA CONTINUA

9.1 Actualización y mantenimiento de sistemas de información

(Denominación del área específica del Área Universitaria A)*			
Identificador único*	**BOS-PEU**		
(Nombre del sistema A1)*	**PRE-REGISTRO DE SELECCIÓN EXAMEN UNAM**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Supervisión interna de los sistemas de tratamiento y archivo de datos personales.	El Coordinador de la sede realizará jornadas trimestrales o semestrales para supervisar que la nube, las contraseñas, el disco duro, archivos digitales, las instalaciones y el equipo electrónico de trabajo estén dentro de los protocolos establecidos y medidas de seguridad implementadas.	3 días en marzo, 3 días en junio y 3 días en septiembre.	La nube (Google Drive), las contraseñas, el disco duro, archivos digitales, las instalaciones y el equipo electrónico de trabajo.

9.2 Actualización y mantenimiento de equipo de cómputo

(Denominación del área específica del Área Universitaria A)*			
Identificador único*	**BOS-PEU**		
(Nombre del sistema A1)*	**PRE-REGISTRO DE SELECCIÓN EXAMEN UNAM**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Apoyo del jefe de departamento de Tecnologías de la Información y Comunicación.	Revisión de anomalías que se presenten en el equipo y actualización de los sistemas computacionales que se utilizan en la Sede.	1 día por año	Sistema operativo software utilizado por la Sede.

9.3 Procesos para la conservación, preservación y respaldos de información

(Denominación del área específica del Área Universitaria A)*		
Identificador único*	**BOS-PEU**	
(Nombre del sistema A1)*	**PRE-REGISTRO DE SELECCIÓN EXAMEN UNAM**	
Proceso*	**Descripción***	**Responsable***
Supervisión interna de los sistemas de tratamiento y archivo de datos personales y del seguimiento de procedimientos y mitigaciones de riesgo por parte del Coordinador de Relaciones y Gestión	Crear contraseñas digitales robustas y controlar accesos a las bases de datos y sistemas de datos personales. Asignar contraseñas a los archivos electrónicos que contengan datos personales. Borrar la información de la nube (Google Drive) y almacenarla en archivos digitales en un disco duro físico seguro con respaldo bajo el manejado del personal autorizado. Agregar cláusula de cesión de derechos sobre datos personales en todo sistema de recopilación de datos. Adquisición de un programa antivirus. Estrategias y protocolos para el uso de llaves y cerraduras de la oficina. Tener un disco duro en la oficina y otro en el domicilio de personal de confianza de la Sede.	**h)** Coordinador de Relaciones y Gestión, y Asistente de Planeación **i)** 5 días

9.4 Procesos de borrado seguro y disposición final de equipos y componentes informáticos

(Denominación del área específica del Área Universitaria A)*		
Identificador único*	**BOS-PEU**	
(Nombre del sistema A1)*	**PRE-REGISTRO DE SELECCIÓN EXAMEN UNAM**	
Proceso*	**Descripción***	**Responsable***
Borrado electrónico definitivo y eliminación de rastros y copias de los datos.	Borrado permanente de los archivos originales y cualquier copia, rastro o respaldo que pueda quedar en la nube (Google Drive)	**g)** Asistente de Planeación **h)** 5 días

10 PROCEDIMIENTOPARALACANCELACIÓNDEUNSISTEMADE TRATAMIENTO DE DATOS PERSONALES

(Informar y describir el procedimiento para la cancelación de un sistema de tratamiento de datos personales.)

K) DATOSDELSISTEMADE TRATAMIENTO DE DATOS PERSONALES QUESERÁCANCELADO:

a) Denominación
b) Motivo de la cancelación

L) PLAZOS Y CONDICIONES PARA EL BLOQUEO DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES:

(Señalar el periodo de bloqueo, considerando los plazos de prescripción para el ejercicio de algún derecho por parte de los titulares de conformidad con la normatividad de cada área universitaria. Asi mismo, se debe señalar las condiciones y el procedimiento que se seguirá para realizar el bloqueo)

M) MEDIDAS DE SEGURIDAD PARA EL BLOQUEO Y POSTERIOR SU PRESIÓN DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES:
(Describir las medidas de seguridad aplicables al periodo de bloqueo y la supresión del sistema, considerando el nivel de protección requerido en virtud del tipo de Datos personales contenidos en el sistema)

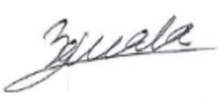
N) PROCEDIMIENTO PARA LA SUPRESIÓN DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

(Describir el procedimiento para suprimir el sistema, una vez cumplido el plazo de bloqueo)

O) MECANISMOS PARA LA SUPRESIÓN DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

(Describir las técnicas para la eliminación física del sistema)

11. APROBACIÓN DEL DOCUMENTO DE SEGURIDAD

		Nombre y firma de quienes revisaron el presente documento:
Responsable del desarrollo:	**Lic. Renata Gatica** Asistente de Planeación planeación@boston.unam.mx 55 1045 4864	Renata Gatica 
Revisó:	**Mtro. Héctor Zavala** Coordinador de Relaciones y Gestión Hector.zavala@boston.unam.mx +1 (857) 333-7591	Héctor Zavala 
Autorizó:	**Mtro. Javier Laguna** Director UNAM-Boston laguna@boston.unam.mx +1 (312) 391-7731	Javier Laguna 
Fecha de aprobación:	(Incluir la fecha de liberación del documento)	
Fecha de actualización:	(Incluir la primera versión e ir agregando las subsiguientes del documento)	

UNAM-FRANCIA

CENTRO DE ESTUDIOS MEXICANOS

1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Centro de estudios mexicanos, UNAM-Francia	
Identificador único	**UNAM-Francia CIAP (Control de Información Académica y Personal)**
(Nombre del sistema A1) *	**Control de registro Verano PUMA**
Datos personales (sensibles o no) contenidos en el sistema*:	Datos de identificación: Nombre, domicilio, teléfono celular, correo electrónico, firma, fecha de nacimiento, fotografía. Datos académicos: Trayectoria educativa, títulos, certificados.
Responsable*:	
Nombre*:	Rodolfo Zanella Specia
Cargo*:	Director de la sede UNAM-Francia
Funciones*:	Definir los datos personales, académicos y administrativos que serán requeridos para el funcionamiento de los programas de la sede
Obligaciones*:	No difundir los datos personales y asegurar que la sede cuenta con el personal a cargo del resguardo y los medios de seguridad de los mismos.
	Encargados:
(Nombre del Encargado 1*)	Verónica Ontiveros Hernández
Cargo*:	Jefa del departamento de gestión
Funciones*:	Encargada de solicitar, recolectar y archivar digitalmente los datos personales.
Obligaciones*:	No difundir información de los datos personales. No modificar la información recolectada. No hacer respaldos en equipo personal de la información de datos personales.
	Usuarios
(Nombre del Usuario 1*)	Mariel de Lourdes Mera Cázares
Cargo*:	Enlace de la sede UNAM-Francia en México
Funciones*:	Realizar estadística para incluirla en los reportes de actividades
Obligaciones*:	No difundir información de los datos personales. No modificar la información recolectada. No hacer respaldos en equipo personal de la información de datos personales.
Sistema (Nombre del A2)*:	**Control de Becarios**
Datos personales contenidos en el sistema*:	Datos de identificación: Nombre, domicilio, teléfono celular, correo electrónico, fecha de nacimiento, nacionalidad, edad, nombres de familiares, fotografía. Datos académicos: Institución de procedencia, grado Datos patrimoniales: seguros médicos. Datos de tránsito y movimientos migratorios: Información migratoria.
	Responsable:
Nombre*:	Rodolfo Zanella Specia
Cargo*:	Director de la sede UNAM-Francia
Funciones*:	Definir los datos personales, académicos y administrativos que serán requeridos para el funcionamiento de los programas de la sede
Obligaciones*:	No difundir los datos personales y asegurar que la sede cuenta con el personal a cargo del resguardo y los medios de seguridad

	de los mismos.
	Encargados:
(Nombre del Encargado 1*)	Verónica Ontiveros Hernández
Cargo*:	Jefa del departamento de gestión
Funciones*:	Encargada de solicitar, recolectar y archivar física y digitalmente los datos personales.
Obligaciones*:	No difundir información de los datos personales. No modificar la información recolectada. No hacer respaldos en equipo personal de la información de datos personales.
	Usuarios:
(Nombre del Usuario 1*)	Mariel de Lourdes Mera Cázares
Cargo*:	Enlace de la sede UNAM-Francia en México
Funciones*:	Realizar documentos probatorios de las estancias de los becarios en la sede, utilizando la información proporcionada por ellos mismos.
Obligaciones*:	No difundir información de los datos personales. No modificar la información recolectada. No hacer respaldos en equipo personal de la información de datos personales.
Sistema (Nombre del A3)*:	**Control de asistentes a eventos en línea**
Datos personales contenidos en el sistema*:	Datos de identificación: Nombre, correo electrónico. Datos académicos: Institución de procedencia
	Responsable:
Nombre*:	Rodolfo Zanella Specia
Cargo*:	Director de la sede UNAM-Francia
Funciones*:	Definir los datos personales, académicos y administrativos que serán requeridos para el funcionamiento de los programas de la sede
Obligaciones*:	No difundir los datos personales y asegurar que la sede cuenta con el personal a cargo del resguardo y los medios de seguridad de los mismos.
	Encargados:
(Nombre del Encargado 1*)	Verónica Ontiveros Hernández
Cargo*:	Jefa del departamento de gestión
Funciones*:	Encargada de solicitar, recolectar y archivar digitalmente los datos personales.
Obligaciones*:	No difundir información de los datos personales. No modificar la información recolectada. No hacer respaldos en equipo personal de la información de datos personales.
	Usuarios:
(Nombre del Usuario 1*)	Mariel de Lourdes Mera Cázares
Cargo*:	Enlace de la sede UNAM-Francia en México
Funciones*:	Verter la información requerida en la Matriz de indicadores de resultados, en el formato de Actividades Académicas y Culturales y en el reporte del Programa de Desarrollo Institucional.
Obligaciones*:	No difundir información de los datos personales. No modificar la

	información almacenada en el servidor. No hacer respaldos en equipo personal de la información de datos personales.
(Nombre del Usuario 2*)	Paola Suyette Mendieta Verdejo
Cargo*:	Jefa del Departamento de Apoyo Académico a las sedes en el extranjero
Funciones*:	Comprobar la información vertida en el formato de Actividades Académicas y Culturales
Obligaciones*:	No difundir información de los datos personales. No modificar la información almacenada en el servidor. No hacer respaldos en equipo personal de la información de datos personales.
Sistema (Nombre del A4)*:	**Control de asistentes a eventos presenciales**
Datos personales contenidos en el sistema*:	Datos de identificación: Nombre, correo electrónico. Datos académicos: Institución de procedencia.
	Responsable:
Nombre*:	Rodolfo ZanellaSpecia
Cargo*:	Director de la sede UNAM-Francia
Funciones*:	Definir los datos personales, académicos y administrativos que serán requeridos para el funcionamiento de los programas de la sede
Obligaciones*:	No difundir los datos personales y asegurar que la sede cuenta con el personal a cargo del resguardo y los medios de seguridad de los mismos.
	Encargados:
(Nombre del Encargado 1*)	Verónica Ontiveros Hernández
Cargo*:	Jefa del departamento de gestión
Funciones*:	Encargada de solicitar, recolectar y archivar digitalmente los datos personales.
Obligaciones*:	No difundir información de los datos personales. No modificar la información recolectada. No hacer respaldos en equipo personal de la información de datos personales.
	Usuarios:
(Nombre del Usuario 1*)	Mariel de Lourdes Mera Cázares
Cargo*:	Enlace de la sede UNAM-Francia en México
Funciones*:	Verter la información requerida en la Matriz de indicadores de resultados, en el formato de Actividades Académicas y Culturales y en el reporte del Programa de Desarrollo Institucional.
Obligaciones*:	No difundir información de los datos personales. No modificar la información almacenada en el servidor. No hacer respaldos en equipo personal de la información de datos personales.
(Nombre del Usuario 2*)	Paola Suyette Mendieta Verdejo
Cargo*:	Jefa del Departamento de Apoyo Académico a las sedes en el extranjero
Funciones*:	Comprobar la información vertida en el formato de Actividades Académicas y Culturales
Obligaciones*:	No difundir información de los datos personales. No modificar la información almacenada en el servidor. No hacer respaldos en equipo personal de la información de datos personales.
Sistema (Nombre del A5)*:	**Control Interno de Personal UNAM-Francia**

Datos personales contenidos en el sistema*:	Datos de identificación: Nombre, domicilio, teléfono particular, teléfono celular, correo electrónico, estado civil, RFC, CURP, fecha de nacimiento, nacionalidad, edad, nombres de familiares, dependientes y beneficiarios, fotografía. Datos laborales: Documentos de nombramiento, puesto, domicilio de trabajo, correo electrónico institucional, teléfono institucional. Datos patrimoniales: seguros médicos. Datos de tránsito y movimientos migratorios: Información migratoria.
	Responsable:
Nombre*:	Rodolfo ZanellaSpecia
Cargo*:	Director de la sede UNAM-Francia
Funciones*:	Definir los datos personales, académicos y administrativos que serán requeridos para el funcionamiento de los programas de la sede
Obligaciones*:	No difundir los datos personales y asegurar que la sede cuenta con el personal a cargo del resguardo y los medios de seguridad de los mismos.
	Encargados:
(Nombre del Encargado 1*)	Verónica Ontiveros Hernández
Cargo*:	Jefa del departamento de gestión
Funciones*:	Encargada de solicitar, recolectar y archivar física y digitalmente los datos personales.
Obligaciones*:	No difundir información de los datos personales. No modificar la información recolectada. No hacer respaldos en equipo personal de la información de datos personales.
	Usuarios:
(Nombre del Usuario 1*)	Verónica Ontiveros Hernández
Cargo*:	Jefa del departamento de gestión
Funciones*:	Utilizar los datos según lo requerido por los procesos administrativos internos.
Obligaciones*:	No difundir información de los datos personales. No modificar la información recolectada. No hacer respaldos en equipo personal de la información de datos personales.
Sistema (Nombre del A6)*:	**Control de Académicos MEXICO-FRANCIA**
Datos personales contenidos en el sistema*:	**Datos de identificación**: Nombre, correo electrónico. **Datos académicos**: Trayectoria académica, áreas de trabajo, Institución de procedencia.
	Responsable:
Nombre*:	**Rodolfo ZanellaSpecia**
Cargo*:	**Director de la sede UNAM-Francia**
Funciones*:	Definir los datos personales, académicos y administrativos que serán requeridos para el funcionamiento de los programas de la sede
Obligaciones*:	No difundir los datos personales y asegurar que la sede cuenta con el personal a cargo del resguardo y los medios de seguridad de los mismos.
	Encargados:
(Nombre del Encargado 1*)	**Verónica Ontiveros Hernández**

Cargo*:	**Jefa del departamento de gestión**
Funciones*:	Encargada de solicitar, recolectar y archivar digitalmente los datos personales.
Obligaciones*:	No difundir información de los datos personales. No modificar la información recolectada. No hacer respaldos en equipo personal de la información de datos personales.
(Nombre del Encargado 2*)	
Cargo*:	Becarios de UNAM-Francia
Funciones*:	Actualizar la base de datos de forma regular
Obligaciones*:	No difundir información de los datos personales. No modificar la información recolectada. No hacer respaldos en equipo personal de la información de datos personales.
	Usuarios:
(Nombre del Usuario 1*)	Patricia Montiel Rogel
Cargo*:	Encargada de Comunicación de la sede UNAM-Francia.
Funciones*:	Establecer vínculos y enviar comunicaciones con académicos en la base de datos, según su interés en las áreas de colaboración y en los eventos organizados.
Obligaciones*:	No difundir información de los datos personales. No modificar la información recolectada. No hacer respaldos en equipo personal de la información de datos personales.

2. ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

(Denominación del área específica del Área Universitaria A)*	
Identificador único¨*	**UNAM-Francia_CIAP**
(Nombre del sistema A1*)	**Control de registro Verano PUMA**
Tipo de soporte:*	Soporte electrónico
Descripción:*	Hoja de cálculo
Características del lugar donde se resguardan los soportes:*	Alojamiento en Google Drive, vía el correo la cuenta de correo institucional asignada por la CRAI
(Nombre del sistema A2*)	**Control de Becarios**
Tipo de soporte*:	Soporte físico y electrónico.
Descripción*:	Expedientes.
Características del lugar donde se resguardan los soportes*:	Soporte electrónico: alojamiento en Google Drive, vía la cuenta de correo institucional asignada por la CRAI Soporte físico: oficina con ventilación natural, luz natural y artificial, sin puerta, aislada de humedad, con archiveros y libreros con chapa que permiten la conservación adecuada de los documentos.
(Nombre del sistema A3*)	**Control de asistentes a eventos en línea**
Tipo de soporte:*	Soporte electrónico
Descripción:*	Hoja de cálculo
Características del lugar donde se resguardan los soportes:*	Alojamiento en Google Drive, vía el correo la cuenta de correo institucional asignada por la CRAI
(Nombre del sistema A4*)	**Control de asistentes a eventos presenciales**
Tipo de soporte:*	Soporte electrónico
Descripción:*	Hoja de cálculo
Características del lugar donde se resguardan los soportes:*	Alojamiento en Google Drive, vía la cuenta de correo institucional asignada por la CRAI
(Nombre del sistema A5*)	**Control Interno de Personal UNAM-Francia**
Tipo de soporte:*	Soporte físico y electrónico.
Descripción:*	Expedientes.
Características del lugar donde se resguardan los soportes:*	**Soporte electrónico:** alojamiento en Google Drive, vía el correo la cuenta de correo institucional asignada por la CRAI **Soporte físico:** oficina con ventilación natural, luz natural y artificial, sin puerta, aislada de humedad, con archiveros y libreros con chapa que permiten la conservación adecuada de los documentos.
(Nombre del sistema A6*)	**Control de Académicos MEXICO-FRANCIA**
Tipo de soporte:*	Soporte electrónico
Descripción:*	Hoja de cálculo
Características del lugar donde se resguardan los soportes:*	Alojamiento en Google Drive, vía la cuenta de correo institucional asignada por la CRAI

2. ANÁLISIS DE RIESGOS

Centro de estudios mexicanos, UNAM-Francia		
Identificador único*	**UNAM-Francia_CIAP**	
(Nombre del sistema A1) *	**Control de registro Verano PUMA**	
Riesgo*	**Impacto***	**Mitigación***
Intervención al Google Drive de una persona ajena a la sede**.**	Fuga o pérdida de información personal de los participantes en el programa.	Revisión regular de los permisos de acceso al Google Drive.
(Nombre del sistema A2) *	**Control de Becarios**	
Riesgo*	**Impacto***	**Mitigación***
Intervención al Google Drive de una persona ajena a la sede Intervención de los archivos físicos por una persona ajena a la sede**.**	Fuga o pérdida de información personal de los participantes en el programa.	Revisión regular de los permisos de acceso al Google Drive. Revisión regular de las chapas de los estantes de resguardo.
(Nombre del sistema A3) *	**Control de asistentes a eventos en línea**	
Riesgo*	**Impacto***	**Mitigación***
Intervención al Google Drive de una persona ajena a la sede**.**	Fuga o pérdida de información personal de los participantes en el programa.	Revisión regular de los permisos de acceso al Google Drive.
(Nombre del sistema A4) *	**Control de asistentes a eventos presenciales**	
Riesgo*	**Impacto***	**Mitigación***
Intervención al Google Drive de una persona ajena a la sede**.**	Fuga o pérdida de información personal de los participantes en el programa.	Revisión regular de los permisos de acceso al Google Drive.
(Nombre del sistema A5) *	**Control Interno de Personal UNAM-Francia**	
Riesgo*	**Impacto***	**Mitigación***
Intervención al Google Drive de una persona ajena a la sede Intervención de los archivos físicos por una persona ajena a la sede**.**	Fuga o pérdida de información personal de los participantes en el programa.	Revisión regular de los permisos de acceso al Google Drive. Revisión regular de las chapas de los estantes de resguardo
(Nombre del sistema A6) *	**Control de Académicos MÉXICO-FRANCIA**	
Riesgo*	**Impacto***	**Mitigación***
Intervención al Google Drive de una persona ajena a la sede**.**	Fuga o pérdida de información personal de los participantes en el programa.	Revisión regular de los permisos de acceso al Google Drive.

4. ANÁLISIS DE BRECHA

(Denominación del área específica del Área Universitaria A)*		
Identificador único*	**UNAM-Francia_CIAP**	
(Nombre del sistema A1) *	**Control de registro Verano PUMA**	
Medida de seguridad actual*	**Medida de seguridad necesaria***	**Acciones para remediación***
Claves de acceso personales a la cuenta de Google Drive institucional	Cambio regular de claves de acceso a Google Drive. Alojamiento de archivos en nube privada o servidor local.	Generar un protocolo de periodos de vigencia y renovación de claves de acceso. Solicitar alojamiento en nube privada o servidor local.
(Nombre del sistema A2) *	**Control de becarios**	
Medida de seguridad actual*	**Medida de seguridad necesaria***	**Acciones para remediación***
Claves de acceso personales a la cuenta de Google Drive institucional	Cambio regular de claves de acceso a Google Drive. Alojamiento de archivos en nube privada o servidor local Control de quienes tienen acceso a los archivos físicos.	Generar un protocolo de periodos de vigencia y renovación de claves de acceso. Solicitar alojamiento en nube privada o servidor local. Realización de bitácora para el acceso a los archivos físicos.
(Nombre del sistema A3) *	**Control de asistentes a eventos en línea**	
Medida de seguridad actual*	**Medida de seguridad necesaria***	**Acciones para remediación***
Claves de acceso personales a la cuenta de Google Drive institucional	Cambio regular de claves de acceso a Google Drive. Alojamiento de archivos en nube privada o servidor local.	Generar un protocolo de periodos de vigencia y renovación de claves de acceso. Solicitar alojamiento en nube privada o servidor local.
(Nombre del sistema A4) *	**Control de asistentes a eventos presenciales**	
Medida de seguridad actual*	**Medida de seguridad necesaria***	**Acciones para remediación***
Claves de acceso personales a la cuenta de Google Drive institucional	*Cambio regular de claves de acceso a Google Drive.* *Alojamiento de archivos en nube privada o servidor local.*	*Generar un protocolo de periodos de vigencia y renovación de claves de acceso.* *Solicitar alojamiento en nube privada o servidor local.*
(Nombre del sistema A5) *	**Control Interno de Personal UNAM-Francia**	
Medida de seguridad actual*	**Medida de seguridad necesaria***	**Acciones para remediación***
Claves de acceso personales a la cuenta de Google Drive institucional	Cambio regular de claves de acceso a Google Drive. Alojamiento de archivos en nube privada o servidor local Control de quienes tienen acceso a los archivos físicos.	Generar un protocolo de periodos de vigencia y renovación de claves de acceso. Solicitar alojamiento en nube privada o servidor local.

		Realización de bitácora para el acceso a los archivos físicos.
(Nombre del sistema A6) *	**Control de Académicos MÉXICO-FRANCIA**	
Medida de seguridad actual*	**Medida de seguridad necesaria***	**Acciones para remediación***
Claves de acceso personales a la cuenta de Google Drive institucional	*Cambio regular de claves de acceso a Google Drive.* *Alojamiento de archivos en nube privada o servidor local.*	*Generar un protocolo de periodos de vigencia y renovación de claves de acceso.* *Solicitar alojamiento en nube privada o servidor local.*

5. PLAN DE TRABAJO

Centro de estudios mexicanos, UNAM-Francia			
Identificador único*	**UNAM-Francia_CIAP**		
(Nombre del sistema A1) *	**Control de registro Verano PUMA**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Protocolo de vigencia y renovación de claves de acceso Google Drive	Renovación de claves de acceso. Control de claves y folders compartidos	Renovación de las claves cada 6 meses.	Esta actividad permitirá el control externo e interno al acceso de los datos resguardados.
Alojamiento en nube privada o servidor local independiente de la nube en Google Drive	Solicitar el alojamiento en nube privada o servidor local	Anual	El respaldo de los datos en una nube de acceso restringido tanto al interior como al exterior de la sede.
(Nombre del sistema A2) *	**Control de Becarios**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Protocolo de vigencia y renovación de claves de acceso Google Drive	Renovación de claves de acceso. Control de claves y folders compartidos	Renovación de las claves cada 6 meses.	Esta actividad permitirá el control externo e interno al acceso de los datos resguardados.
Alojamiento en nube privada o servidor local independiente de la nube en Google Drive	Solicitar el alojamiento en nube privada o servidor local	Anual	El respaldo de los datos en una nube de acceso restringido tanto al interior como al exterior de la sede.
Bitácora de consulta de archivos físicos	Elaborar y mantener una bitácora de consulta de los archivos físicos	Anual	Controlar y registrar el acceso a los archivos físicos.
(Nombre del sistema A3) *	**Control de asistentes a eventos en línea**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Protocolo de vigencia y renovación de claves de acceso Google Drive	Renovación de claves de acceso. Control de claves y folders compartidos	Renovación de las claves cada 6 meses.	Esta actividad permitirá el control externo e interno al acceso de los datos resguardados.
Alojamiento en nube privada o servidor local independiente de la nube en Google Drive	Solicitar el alojamiento en nube privada o servidor local	Anual	El respaldo de los datos en una nube de acceso restringido tanto al interior como al exterior de la sede.
(Nombre del sistema A4) *	**Control de asistentes a eventos en presencial**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Protocolo de vigencia y renovación de claves de acceso Google Drive	Renovación de claves de acceso. Control de claves y folders compartidos	Renovación de las claves cada 6 meses.	Esta actividad permitirá el control externo e interno al acceso de los datos resguardados.

Alojamiento en nube privada o servidor local independiente de la nube en Google Drive	Solicitar el alojamiento en nube privada o servidor local	Anual	El respaldo de los datos en una nube de acceso restringido tanto al interior como al exterior de la sede.
(Nombre del sistema A5) *	**Control Interno de Personal UNAM-Francia**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Protocolo de vigencia y renovación de claves de acceso Google Drive	Renovación de claves de acceso. Control de claves y folders compartidos	Renovación de las claves cada 6 meses.	Esta actividad permitirá el control externo e interno al acceso de los datos resguardados.
Alojamiento en nube privada o servidor local independiente de la nube en Google Drive	Solicitar el alojamiento en nube privada o servidor local	Anual	El respaldo de los datos en una nube de acceso restringido tanto al interior como al exterior de la sede.
Bitácora de consulta de archivos físicos	Elaborar y mantener una bitácora de consulta de los archivos físicos	Anual	Controlar y registrar el acceso a los archivos físicos.
(Nombre del sistema A6) *	**Control de Académicos MÉXICO-FRANCIA**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Protocolo de vigencia y renovación de claves de acceso Google Drive	Renovación de claves de acceso. Control de claves y folders compartidos	Renovación de las claves cada 6 meses.	Esta actividad permitirá el control externo e interno al acceso de los datos resguardados.
Alojamiento en nube privada o servidor local independiente de la nube en Google Drive	Solicitar el alojamiento en nube privada o servidor local	Anual	El respaldo de los datos en una nube de acceso restringido tanto al interior como al exterior de la sede.

6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

I. TRANSFERENCIAS DE DATOS PERSONALES

Centro de estudios mexicanos, UNAM-Francia	
Identificador único*	**UNAM-Francia_CIAP**
(Nombre del sistema A1)	**Control de registro Verano PUMA**
	● No se realiza transferencia física. ● No se realiza traslado de soportes electrónicos. ● Los archivos electrónicos no están cifrados antes de su transferencia por medios electrónicos. ● La transferencia se realiza por internet mediante correo electrónico y/o compartiendo archivos en Google drive. ● Se desconoce si el destinatario cuenta con dispositivos de detección de intrusiones. ● No se solicita acuse de recibo. ● La transferencia no se formaliza mediante un instrumento jurídico.

II. RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS

(Nombre del sistema A1.1) *	**UNAM-Francia_CIAP**

1. Señalar las medidas de seguridad que ha implementado el área universitaria para el resguardo de los soportes físicos del sistema de manera que evite la alteración, pérdida o acceso no autorizado a los mismos.

La estantería cuenta con puertas con chapa, cuya llave se encuentra a resguardo del responsable y del encargado del sistema.

2. Señalar en un listado las personas (nombre, cargo, funciones y obligaciones) que tienen acceso a los soportes físicos del sistema.

Rodolfo Zanella Specia.
Director de la sede UNAM-Francia. Responsable del sistema.
Verónica Ontiveros Hernández.
Jefa del departamento de gestión de la sede UNAM-Francia. Encargada del sistema.

III. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

HASTA LA FECHA, LA SEDE NO CUENTA CON UNA BITÁCORA DE ACCESO Y OPERACIÓN COTIDIANA

1. Los datos que se registran en las bitácoras: Los incisos del 1-5 siguientes no aplican para el caso de la sede, pues no se lleva actualmente un control con bitácora.

a) Quién accede a los datos personales, fecha y hora en la que se realiza el acceso o se intenta el mismo, propósito del acceso, así como fecha y hora de salida; **N/A**
b) Para soportes físicos: Número o clave del expediente utilizado, y **N/A**
c) Para soportes electrónicos: Operaciones o acciones llevadas a cabo y registros utilizados de la base de datos. **N/A**

2. Si las bitácoras están en soporte físico o en soporte electrónico; **N/A**
3. Lugar dónde almacena las bitácoras y por cuánto tiempo; **N/A**
4. La manera en que asegura la integridad de las bitácoras, y **N/A**
5. Respecto del análisis de las bitácoras:

a) Quién es el responsable de analizarlas (si es el área universitaria o si es un tercero) y cada cuándo las analiza, y **N/A**
b) Para el caso de que las bitácoras estén en soporte electrónico: las herramientas de análisis utilizadas. **N/A**

IV. REGISTRO DE INCIDENTES:

HASTA LA FECHA, LA SEDE NO CUENTA CON UN REGISTRO DE INCIDENTES

Describir el procedimiento de atención de incidentes que tiene implementado el área universitaria y especificar si lleva registro de los incidentes relativos a soportes físicos, como lo son la pérdida o alteración no autorizada de expedientes, y para el caso de soportes electrónicos, ofrecer detalles sobre el registro de incidentes en el cual consigne los procedimientos realizados para la recuperación de los datos o para permitir la disponibilidad del proceso. **Hasta el presente la sede no cuenta con un registro de incidentes, por lo que los incisos del 1 al 4 no aplican para la sede.**

1. Los datos que registra:

a) La persona que resolvió el incidente; **N/A**

b) La metodología aplicada; **N/A**

c) Para soportes físicos: Los oficios, documentos, expedientes, estantes o archiveros, tanto los dañados como los recuperados, y **N/A**

d) Para soportes electrónicos: Los campos, registros, tablas, bases de datos o archivos electrónicos, tanto dañados como recuperados, el nombre de los sistemas y la infraestructura afectada, indicar si el incidente afectó el servidor principal y los servidores de respaldo, etc. **N/A**

2. Si el registro está en soporte físico o en soporte electrónico; **N/A**

3. Cómo asegura la integridad de dicho registro, y **N/A**

4. Para el caso de soportes electrónicos, quién autoriza la recuperación de datos. **N/A**

V. ACCESO A LAS INSTALACIONES

1. Seguridad perimetral exterior (las instalaciones del área universitaria):

La Universidad que aloja la sede en Francia cuenta con una única entrada con un vigilante en el acceso. No se permite la entrada a visitantes en horarios fuera de oficina, en fines de semana ni en días festivos.
El personal que ingrese a las instalaciones en fines de semana o días festivos debe contar con una tarjeta digital para abrir la puerta de entrada, así como registrarse en el libro de entradas y salidas.

Para las personas que acceden a sus instalaciones:

a) Se les solicita indicar la dependencia a la que asisten y motivo de visita.

2. Seguridad perimetral interior (oficina, almacén o bodega para soportes físicos, centro de datos para soportes electrónicos):

¿Qué medidas de seguridad ha implementado para controlar el acceso a los espacios donde almacena los soportes físicos o electrónicos del sistema? Por ejemplo, se espera que precise el tipo de puertas y cerraduras instaladas, si tiene instalados controles biométricos, si administra la asignación de llaves y/o claves de acceso para abrir puertas y/o estantería, si cuenta con vigilancia las 24 horas, si hay un sistema de tratamiento de datos personales de video vigilancia, entre otras medidas.

Para las personas que acceden a dichos espacios interiores:

a) Se les identifica a través de una cámara al exterior de la puerta de entrada a la oficina.

b) Se les solicita autentificación verbal en la entrada a la oficina y motivo de visita.

c) Se autoriza el acceso a las instalaciones en caso de tener un motivo académico o estudiantil, siempre y cuando alguien del personal permanente de la sede esté presente en el lugar.

d) No se les autoriza el acceso a los archivos físicos de la sede.

VI. ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

Los datos personales obtenidos mediante inscripciones a cursos, Verano Puma y otros eventos no se actualizan.

Los datos personales de la base de datos de Profesores-investigadores UNAM relacionados con universidades francófonas europeas tienen una actualización constante, aunque no periódica.

Los datos personales del personal de la sede, tanto los del personal de tiempo completo como los del personal por honorarios se actualizan conforme se actualiza el personal.

Las medidas de seguridad previstas a continuación en los incisos VII al IX, sólo aplican para soportes electrónicos

VII. PERFILES DE USUARIO Y CONTRASEÑAS

En este rubro el área universitaria deberá describir el esquema de perfiles de usuario y contraseñas que tiene implementado para control de acceso mediante una red electrónica.

1. Modelo de control de acceso (alguno de los siguientes):

a) ¿Es obligatorio (etiquetas para objetos y acreditación para sujetos)?
SÍ
b) ¿Es discrecional (matriz de control de acceso)?
SÍ
c) ¿Está basado en roles (perfiles) o grupos?
SÍ
d) ¿Está basado en reglas?
SÍ

Es obligatorio para el acceso a las carpetas en Drive que se compartan con el usuario. Cada miembro de la sede gestiona una cuenta de correo institucional (@francia.unam.mx) con su propio espacio de Google Drive. El dueño de cada carpeta es responsable de la información compartida.

2. Perfiles de usuario y contraseñas en el sistema operativo de red:

a) ¿Cuenta con un sistema operativo de red instalado en sus equipos?
NO
b) ¿Proporciona dicho sistema operativo un manejo riguroso de perfiles de usuario y contraseñas?
NO
c) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?
NO

3. Perfiles de usuario y contraseñas manejados por el software aplicativo del sistema de tratamiento de datos personales: No se cuenta con un software aplicativo del sistema de tratamiento de datos personales.

a) ¿Ofrece dicho software un manejo riguroso de perfiles de usuario y contraseñas?
N/A
b) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?
No se cuenta con un software aplicativo del sistema de tratamiento de datos personales.

4. Administración de perfiles de usuario y contraseñas:

a) ¿Quién da de alta nuevos perfiles?
La CRAI para las cuentas de Google con las que se accede a Google Drive.
b) ¿Quién autoriza la creación de nuevos perfiles?
El director de la sede
c) ¿Se lleva registro de la creación de nuevos perfiles?
SÍ

5. Acceso remoto al sistema de tratamiento de datos personales:

a) ¿Requieren los usuarios acceso remoto al equipo de cómputo que por lo general utilizan para trabajar con el sistema?

NO

b) ¿Requiere el administrador acceso remoto al equipo donde reside el sistema para realizar tareas de mantenimiento?

NO

c) ¿Cómo se evita el acceso remoto no autorizado?

Los equipos no cuentan con el acceso remoto autorizado

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

1. Señalar si realiza respaldos

a) Completos__, diferenciales _X__ o incrementales___;

b) De forma automática ____ o Manual __X___,

c) Periodicidad con que los realiza: _No existe una periodización para el respaldo de los datos.

2. El tipo de medios (por ejemplo: cintas magnéticas, discos duros, CD-ROM, entre otros) que utiliza para almacenar las copias de seguridad;

Se almacenan en la nube de Google Docs.

3. Cómo y dónde archiva esos medios, y

Actualmente no se hacen respaldos en *hardware* externos, solo mediante las nubes de almacenamiento de Google Drive.

4. Quién es el responsable de realizar estas operaciones (el área universitaria o un tercero).

La sede es responsable de sus respaldos.

IX. PLAN DE CONTINGENCIA

1. Presentar el plan de contingencia con el cual garantiza la continuidad de la operación del sistema o informar si no lo tiene, pero se encuentra desarrollándolo. **Actualmente no se cuenta con un plan de contingencia, pero se encuentra en desarrollo.**

2. Si cuenta con plan de contingencia y lo ha implementado, deberá indicar si realiza pruebas de eficiencia de este. **N/A**

3. Informar si cuenta con un sitio redundante (alterno) y señalar lo siguiente: **No se cuenta con un sitio redundante o alterno para el funcionamiento de la sede.**

a) El tipo de sitio (caliente, tibio o frío); N/A

b) Si el sitio es propio o subcontratado con un tercero; N/A

c) Los procedimientos, el equipo y el personal que designa para poner en marcha tal sitio y N/A

d) Tiempo que le lleva poner en marcha el sitio, según las pruebas de eficiencia. N/A

I. TRANSFERENCIAS DE DATOS PERSONALES

Centro de estudios mexicanos, UNAM-Francia	
Identificador único*	**UNAM-Francia_CIAP**
(Nombre del sistema A2)	**● Control de Becarios**
	● No se realiza transferencia física. ● No se realiza traslado de soportes electrónicos. ● Los archivos electrónicos no están cifrados antes de su transferencia por medios electrónicos. ● La transferencia se realiza por internet mediante correo electrónico y/o compartiendo archivos en Google drive. ● Se desconoce si el destinatario cuenta con dispositivos de detección de intrusiones. ● No se solicita acuse de recibo. ● La transferencia no se formaliza mediante un instrumento jurídico.

II. RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS

5. Señalar las medidas de seguridad que ha implementado el área universitaria para el resguardo de los soportes físicos del sistema de manera que evite la alteración, pérdida o acceso no autorizado a los mismos.

La estantería cuenta con puertas con chapa, cuya llave se encuentra a resguardo del responsable y del encargado del sistema.

6. Señalar en un listado las personas (nombre, cargo, funciones y obligaciones) que tienen acceso a los soportes físicos del sistema.

Rodolfo Zanella Specia.
Director de la sede UNAM-Francia. Responsable del sistema.
Verónica Ontiveros Hernández.
Jefa del departamento de gestión de la sede UNAM-Francia. Encargada del sistema.

III. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

HASTA LA FECHA, LA SEDE NO CUENTA CON UNA BITÁCORA DE ACCESO Y OPERACIÓN COTIDIANA

1. Los datos que se registran en las bitácoras: Los incisos del 1-5 siguientes no aplican para el caso de la sede, pues no se lleva actualmente un control con bitácora.

a) Quién accede a los datos personales, fecha y hora en la que se realiza el acceso o se intenta el mismo, propósito del acceso, así como fecha y hora de salida; **N/A**
b) Para soportes físicos: Número o clave del expediente utilizado, y **N/A**
c) Para soportes electrónicos: Operaciones o acciones llevadas a cabo y registros utilizados de la base de datos. **N/A**

6. Si las bitácoras están en soporte físico o en soporte electrónico;**N/A**
7. Lugar dónde almacena las bitácoras y por cuánto tiempo; **N/A**
8. La manera en que asegura la integridad de las bitácoras, y **N/A**
9. Respecto del análisis de las bitácoras:

c) Quién es el responsable de analizarlas (si es el área universitaria o si es un tercero) y cada cuándo las analiza, y **N/A**
d) Para el caso de que las bitácoras estén en soporte electrónico: las herramientas

de análisis utilizadas. **N/A**

IV. REGISTRO DE INCIDENTES:

HASTA LA FECHA, LA SEDE NO CUENTA CON UN REGISTRO DE INCIDENTES

Describir el procedimiento de atención de incidentes que tiene implementado el área universitaria y especificar si lleva registro de los incidentes relativos a soportes físicos, como lo son la pérdida o alteración no autorizada de expedientes, y para el caso de soportes electrónicos, ofrecer detalles sobre el registro de incidentes en el cual consigne los procedimientos realizados para la recuperación de los datos o para permitir la disponibilidad del proceso. **Hasta el presente la sede no cuenta con un registro de incidentes, por lo que los incisos del 1 al 4 no aplican para la sede.**

1. Los datos que registra:
   - **a)** La persona que resolvió el incidente; **N/A**
   - **b)** La metodología aplicada; **N/A**
   - **c)** Para soportes físicos: Los oficios, documentos, expedientes, estantes o archiveros, tanto los dañados como los recuperados, y **N/A**
   - **d)** Para soportes electrónicos: Los campos, registros, tablas, bases de datos o archivos electrónicos, tanto dañados como recuperados, el nombre de los sistemas y la infraestructura afectada, indicar si el incidente afectó el servidor principal y los servidores de respaldo, etc. **N/A**

2. Si el registro está en soporte físico o en soporte electrónico; **N/A**
3. Cómo asegura la integridad de dicho registro, y **N/A**
4. Para el caso de soportes electrónicos, quién autoriza la recuperación de datos. **N/A**

V. ACCESO A LAS INSTALACIONES

3. Seguridad perimetral exterior (las instalaciones del área universitaria):

La Universidad que aloja la sede en Francia cuenta con una única entrada con un vigilante en el acceso. No se permite la entrada a visitantes en horarios fuera de oficina, en fines de semana ni en días festivos.
El personal que ingrese a las instalaciones en fines de semana o días festivos debe contar con una tarjeta digital para abrir la puerta de entrada, así como registrarse en el libro de entradas y salidas.

Para las personas que acceden a sus instalaciones:

a) Se les solicita indicar la dependencia a la que asisten y motivo de visita.

4. Seguridad perimetral interior (oficina, almacén o bodega para soportes físicos, centro de datos para soportes electrónicos):

¿Qué medidas de seguridad ha implementado para controlar el acceso a los espacios donde almacena los soportes físicos o electrónicos del sistema? Por ejemplo, se espera que precise el tipo de puertas y cerraduras instaladas, si tiene instalados controles biométricos, si administra la asignación de llaves y/o claves de acceso para abrir puertas y/o estantería, si cuenta con vigilancia las 24 horas, si hay un sistema de tratamiento de datos personales de video vigilancia, entre otras medidas.

Para las personas que acceden a dichos espacios interiores:

a) Se les identifica a través de una cámara al exterior de la puerta de entrada a la oficina.
b) Se les solicita autentificación verbal en la entrada a la oficina y motivo de visita.
c) Se autoriza el acceso a las instalaciones en caso de tener un motivo académico o estudiantil, siempre y cuando alguien del personal permanente de la sede esté presente en el lugar.
d) No se les autoriza el acceso a los archivos físicos de la sede.

VI. ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

Los datos personales obtenidos mediante inscripciones a cursos, Verano Puma y otros eventos no se actualizan.

Los datos personales de la base de datos de Profesores-investigadores UNAM relacionados con universidades francófonas europeas tienen una actualización constante, aunque no periódica.

Los datos personales del personal de la sede, tanto los del personal de tiempo completo como los del personal por honorarios se actualizan conforme se actualiza el personal.

Las medidas de seguridad previstas a continuación en los incisos VII al IX, sólo aplican para soportes electrónicos

VII. PERFILES DE USUARIO Y CONTRASEÑAS

En este rubro el área universitaria deberá describir el esquema de perfiles de usuario y contraseñas que tiene implementado para control de acceso mediante una red electrónica.

1. Modelo de control de acceso (alguno de los siguientes):

a) ¿Es obligatorio (etiquetas para objetos y acreditación para sujetos)?
SÍ
b) ¿Es discrecional (matriz de control de acceso)?
SÍ
c) ¿Está basado en roles (perfiles) o grupos?
SÍ
d) ¿Está basado en reglas?
SÍ

Es obligatorio para el acceso a las carpetas en Drive que se compartan con el usuario. Cada miembro de la sede gestiona una cuenta de correo institucional (@francia.unam.mx) con su propio espacio de Google Drive. El dueño de cada carpeta es responsable de la información compartida.

2. Perfiles de usuario y contraseñas en el sistema operativo de red:

a) ¿Cuenta con un sistema operativo de red instalado en sus equipos?
NO
b) ¿Proporciona dicho sistema operativo un manejo riguroso de perfiles de usuario y contraseñas?
NO
c) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?
NO

3. Perfiles de usuario y contraseñas manejados por el software aplicativo del sistema de tratamiento de datos personales: No se cuenta con un software aplicativo del sistema de tratamiento de datos personales.

a) ¿Ofrece dicho software un manejo riguroso de perfiles de usuario y contraseñas?
N/A
b) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?
No se cuenta con un software aplicativo del sistema de tratamiento de datos personales.

4. Administración de perfiles de usuario y contraseñas:
a) ¿Quién da de alta nuevos perfiles?
La CRAI para las cuentas de Google con las que se accede a Google Drive.
b) ¿Quién autoriza la creación de nuevos perfiles?
El director de la sede
c) ¿Se lleva registro de la creación de nuevos perfiles?
SÍ

5. Acceso remoto al sistema de tratamiento de datos personales:
a) ¿Requieren los usuarios acceso remoto al equipo de cómputo que por lo general utilizan para trabajar con el sistema?
NO
b) ¿Requiere el administrador acceso remoto al equipo donde reside el sistema para realizar tareas de mantenimiento?
NO
c) ¿Cómo se evita el acceso remoto no autorizado?
Los equipos no cuentan con el acceso remoto autorizado

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

1. Señalar si realiza respaldos
a) Completos __, diferenciales _X__ o incrementales___;
b) De forma automática ____ o Manual __X___,
c) Periodicidad con que los realiza: _No existe una periodización para el respaldo de los datos.

2. El tipo de medios (por ejemplo: cintas magnéticas, discos duros, CD-ROM, entre otros) que utiliza para almacenar las copias de seguridad;
Se almacenan en la nube de Google Docs.

3. Cómo y dónde archiva esos medios, y
Actualmente no se hacen respaldos en *hardware* externos, solo mediante las nubes de almacenamiento de Google Drive.

4. Quién es el responsable de realizar estas operaciones (el área universitaria o un tercero).
La sede es responsable de sus respaldos.

IX. PLAN DE CONTINGENCIA

1. Presentar el plan de contingencia con el cual garantiza la continuidad de la operación del sistema o informar si no lo tiene, pero se encuentra desarrollándolo. **Actualmente no se cuenta con un plan de contingencia, pero se encuentra en desarrollo.**
2. Si cuenta con plan de contingencia y lo ha implementado, deberá indicar si realiza pruebas de eficiencia de este. **N/A**

3. Informar si cuenta con un sitio redundante (alterno) y señalar lo siguiente: **No se cuenta con un sitio redundante o alterno para el funcionamiento de la sede.**

a) El tipo de sitio (caliente, tibio o frío); **N/A**
b) Si el sitio es propio o subcontratado con un tercero; **N/A**
c) Los procedimientos, el equipo y el personal que designa para poner en marcha tal sitio y **N/A**
d) Tiempo que le lleva poner en marcha el sitio, según las pruebas de eficiencia. **N/A**

I. TRANSFERENCIAS DE DATOS PERSONALES

Centro de estudios mexicanos, UNAM-Francia	
Identificador único*	**UNAM-Francia_CIAP**
(Nombre del sistema A3)	**Control de asistentes a eventos en línea**
	● No se realiza transferencia física. ● No se realiza traslado de soportes electrónicos. ● Los archivos electrónicos no están cifrados antes de su transferencia por medios electrónicos. ● La transferencia se realiza por internet mediante correo electrónico y/o compartiendo archivos en Google drive. ● Se desconoce si el destinatario cuenta con dispositivos de detección de intrusiones. ● No se solicita acuse de recibo. ● La transferencia no se formaliza mediante un instrumento jurídico.

II. RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS

1. Señalar las medidas de seguridad que ha implementado el área universitaria para el resguardo de los soportes físicos del sistema de manera que evite la alteración, pérdida o acceso no autorizado a los mismos.

La estantería cuenta con puertas con chapa, cuya llave se encuentra a resguardo del responsable y del encargado del sistema.

2. Señalar en un listado las personas (nombre, cargo, funciones y obligaciones) que tienen acceso a los soportes físicos del sistema.

Rodolfo Zanella Specia.
Director de la sede UNAM-Francia. Responsable del sistema.
Verónica Ontiveros Hernández.
Jefa del departamento de gestión de la sede UNAM-Francia. Encargada del sistema.

III. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

HASTA LA FECHA, LA SEDE NO CUENTA CON UNA BITÁCORA DE ACCESO Y OPERACIÓN COTIDIANA

1. Los datos que se registran en las bitácoras:Los incisos del 1-5 siguientes no aplican para el caso de la sede, pues no se lleva actualmente un control con bitácora.

a) Quién accede a los datos personales, fecha y hora en la que se realiza el acceso o se intenta el mismo, propósito del acceso, así como fecha y hora de salida; **N/A**
b) Para soportes físicos: Número o clave del expediente utilizado, y **N/A**
c) Para soportes electrónicos: Operaciones o acciones llevadas a cabo y registros utilizados de la base de datos. **N/A**

1. Si las bitácoras están en soporte físico o en soporte electrónico;**N/A**
2. Lugar dónde almacena las bitácoras y por cuánto tiempo; **N/A**
3. La manera en que asegura la integridad de las bitácoras, y **N/A**
4. Respecto del análisis de las bitácoras:

a) Quién es el responsable de analizarlas (si es el área universitaria o si es un tercero) y cada cuándo las analiza, y **N/A**
b) Para el caso de que las bitácoras estén en soporte electrónico: las herramientas de análisis utilizadas. **N/A**

IV. REGISTRO DE INCIDENTES:

HASTA LA FECHA, LA SEDE NO CUENTA CON UN REGISTRO DE INCIDENTES

Describir el procedimiento de atención de incidentes que tiene implementado el área universitaria y especificar si lleva registro de los incidentes relativos a soportes físicos, como lo son la pérdida o alteración no autorizada de expedientes, y para el caso de soportes electrónicos, ofrecer detalles sobre el registro de incidentes en el cual consigne los procedimientos realizados para la recuperación de los datos o para permitir la disponibilidad del proceso. **Hasta el presente la sede no cuenta con un registro de incidentes, por lo que los incisos del 1 al 4 no aplican para la sede.**

1. Los datos que registra:

a) La persona que resolvió el incidente; N/A
b) La metodología aplicada; **N/A**
c) Para soportes físicos: Los oficios, documentos, expedientes, estantes o archiveros, tanto los dañados como los recuperados, y **N/A**
d) Para soportes electrónicos: Los campos, registros, tablas, bases de datos o archivos electrónicos, tanto dañados como recuperados, el nombre de los sistemas y la infraestructura afectada, indicar si el incidente afectó el servidor principal y los servidores de respaldo, etc. **N/A**

2. Si el registro está en soporte físico o en soporte electrónico; **N/A**
3. Cómo asegura la integridad de dicho registro, y **N/A**
4. Para el caso de soportes electrónicos, quién autoriza la recuperación de datos. **N/A**

V. ACCESO A LAS INSTALACIONES

1. Seguridad perimetral exterior (las instalaciones del área universitaria):

La Universidad que aloja la sede en Francia cuenta con una única entrada con un vigilante en el acceso. No se permite la entrada a visitantes en horarios fuera de oficina, en fines de semana ni en días festivos.

El personal que ingrese a las instalaciones en fines de semana o días festivos debe contar con una tarjeta digital para abrir la puerta de entrada, así como registrarse en el libro de entradas y salidas.

Para las personas que acceden a sus instalaciones:

a) Se les solicita indicar la dependencia a la que asisten y motivo de visita.

2. Seguridad perimetral interior (oficina, almacén o bodega para soportes físicos, centro de datos para soportes electrónicos):

¿Qué medidas de seguridad ha implementado para controlar el acceso a los espacios donde almacena los soportes físicos o electrónicos del sistema? Por ejemplo, se espera que precise el tipo de puertas y cerraduras instaladas, si tiene instalados controles biométricos, si administra la asignación de llaves y/o claves de acceso para abrir puertas y/o estantería, si cuenta con vigilancia las 24 horas, si hay un sistema de tratamiento de datos personales de video vigilancia, entre otras medidas.

Para las personas que acceden a dichos espacios interiores:

a) Se les identifica a través de una cámara al exterior de la puerta de entrada a la oficina.
b) Se les solicita autentificación verbal en la entrada a la oficina y motivo de visita.
c) Se autoriza el acceso a las instalaciones en caso de tener un motivo académico o estudiantil, siempre y cuando alguien del personal permanente de la sede esté presente en el lugar.
d) No se les autoriza el acceso a los archivos físicos de la sede.

VI. ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

Los datos personales obtenidos mediante inscripciones a cursos, Verano Puma y otros eventos no se actualizan.

Los datos personales de la base de datos de Profesores-investigadores UNAM relacionados con universidades francófonas europeas tienen una actualización constante, aunque no periódica.

Los datos personales del personal de la sede, tanto los del personal de tiempo completo como los del personal por honorarios se actualizan conforme se actualiza el personal.

Las medidas de seguridad previstas a continuación en los incisos VII al IX, sólo aplican para soportes electrónicos

VII. PERFILES DE USUARIO Y CONTRASEÑAS

En este rubro el área universitaria deberá describir el esquema de perfiles de usuario y contraseñas que tiene implementado para control de acceso mediante una red electrónica.

1. Modelo de control de acceso (alguno de los siguientes):

a) ¿Es obligatorio (etiquetas para objetos y acreditación para sujetos)?
SÍ
b) ¿Es discrecional (matriz de control de acceso)?
SÍ
c) ¿Está basado en roles (perfiles) o grupos?
SÍ
d) ¿Está basado en reglas?
SÍ

Es obligatorio para el acceso a las carpetas en Drive que se compartan con el usuario. Cada miembro de la sede gestiona una cuenta de correo institucional (@francia.unam.mx) con su propio espacio de Google Drive. El dueño de cada carpeta es responsable de la información compartida.

2. Perfiles de usuario y contraseñas en el sistema operativo de red:

a) ¿Cuenta con un sistema operativo de red instalado en sus equipos?
NO
b) ¿Proporciona dicho sistema operativo un manejo riguroso de perfiles de usuario y contraseñas?
NO
c) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?
NO

3. Perfiles de usuario y contraseñas manejados por el software aplicativo del sistema de tratamiento de datos personales: No se cuenta con un software aplicativo del sistema de tratamiento de datos personales.

a) ¿Ofrece dicho software un manejo riguroso de perfiles de usuario y contraseñas?
N/A
b) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?
No se cuenta con un software aplicativo del sistema de tratamiento de datos personales.

4. Administración de perfiles de usuario y contraseñas:

a) ¿Quién da de alta nuevos perfiles?
La CRAI para las cuentas de Google con las que se accede a Google Drive.
b) ¿Quién autoriza la creación de nuevos perfiles?
El director de la sede
c) ¿Se lleva registro de la creación de nuevos perfiles?
SÍ

5. Acceso remoto al sistema de tratamiento de datos personales:

a) ¿Requieren los usuarios acceso remoto al equipo de cómputo que por lo general utilizan para trabajar con el sistema?
NO
b) ¿Requiere el administrador acceso remoto al equipo donde reside el sistema para realizar tareas de mantenimiento?
NO
c) ¿Cómo se evita el acceso remoto no autorizado?
Los equipos no cuentan con el acceso remoto autorizado

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

1. Señalar si realiza respaldos

a) Completos __, diferenciales _X__ o incrementales___;
b) De forma automática ____ o Manual __X___,
c) Periodicidad con que los realiza: _No existe una periodización para el respaldo de los datos.

2. El tipo de medios (por ejemplo: cintas magnéticas, discos duros, CD-ROM, entre otros) que utiliza para almacenar las copias de seguridad:
Se almacenan en la nube de Google Docs.

3. Cómo y dónde archiva esos medios, y
Actualmente no se hacen respaldos en *hardware* externos, solo mediante las nubes de almacenamiento de Google Drive.

4. Quién es el responsable de realizar estas operaciones (el área universitaria o un tercero).
La sede es responsable de sus respaldos.

IX. PLAN DE CONTINGENCIA

1. Presentar el plan de contingencia con el cual garantiza la continuidad de la operación del sistema o informar si no lo tiene, pero se encuentra desarrollándolo. **Actualmente no se cuenta con un plan de contingencia, pero se encuentra en desarrollo.**
2. Si cuenta con plan de contingencia y lo ha implementado, deberá indicar si realiza pruebas de eficiencia de este. **N/A**
3. Informar si cuenta con un sitio redundante (alterno) y señalar lo siguiente: **No se cuenta con un sitio redundante o alterno para el funcionamiento de la sede.**

a) El tipo de sitio (caliente, tibio o frío); **N/A**
b) Si el sitio es propio o subcontratado con un tercero; **N/A**
c) Los procedimientos, el equipo y el personal que designa para poner en marcha tal sitio y **N/A**
d) Tiempo que le lleva poner en marcha el sitio, según las pruebas de eficiencia. **N/A**

I. TRANSFERENCIAS DE DATOS PERSONALES

Centro de estudios mexicanos, UNAM-Francia	
Identificador único*	**UNAM-Francia_CIAP**
(Nombre del sistema A4)	**Control de asistentes a eventos en presencial**
	● No se realiza transferencia física. ● No se realiza traslado de soportes electrónicos. ● Los archivos electrónicos no están cifrados antes de su transferencia por medios electrónicos. ● La transferencia se realiza por internet mediante correo electrónico y/o compartiendo archivos en Google drive. ● Se desconoce si el destinatario cuenta con dispositivos de detección de intrusiones. ● No se solicita acuse de recibo. ● La transferencia no se formaliza mediante un instrumento jurídico.

II. RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS

1. Señalar las medidas de seguridad que ha implementado el área universitaria para el resguardo de los soportes físicos del sistema de manera que evite la alteración, pérdida o acceso no autorizado a los mismos.

La estantería cuenta con puertas con chapa, cuya llave se encuentra a resguardo del responsable y del encargado del sistema.

2. Señalar en un listado las personas (nombre, cargo, funciones y obligaciones) que tienen acceso a los soportes físicos del sistema.

1.- Rodolfo Zanella Specia.
Director de la sede UNAM-Francia. Responsable del sistema.
2.- Verónica Ontiveros Hernández.
Jefa del departamento de gestión de la sede UNAM-Francia. Encargada del sistema.

III. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

HASTA LA FECHA, LA SEDE NO CUENTA CON UNA BITÁCORA DE ACCESO Y OPERACIÓN COTIDIANA

1. Los datos que se registran en las bitácoras:Los incisos del 1-5 siguientes no aplican para el caso de la sede, pues no se lleva actualmente un control con bitácora.

a) Quién accede a los datos personales, fecha y hora en la que se realiza el acceso o se intenta el mismo, propósito del acceso, así como fecha y hora de salida; **N/A**
b) Para soportes físicos: Número o clave del expediente utilizado, y **N/A**
c) Para soportes electrónicos: Operaciones o acciones llevadas a cabo y registros utilizados de la base de datos. **N/A**

5. Si las bitácoras están en soporte físico o en soporte electrónico;**N/A**
6. Lugar dónde almacena las bitácoras y por cuánto tiempo; **N/A**
7. La manera en que asegura la integridad de las bitácoras, y **N/A**
8. Respecto del análisis de las bitácoras:

a) Quién es el responsable de analizarlas (si es el área universitaria o si es un tercero) y cada cuándo las analiza, y **N/A**
b) Para el caso de que las bitácoras estén en soporte electrónico: las herramientas de análisis utilizadas. **N/A**

IV. REGISTRO DE INCIDENTES:

HASTA LA FECHA, LA SEDE NO CUENTA CON UN REGISTRO DE INCIDENTES

Describir el procedimiento de atención de incidentes que tiene implementado el área universitaria y especificar si lleva registro de los incidentes relativos a soportes físicos, como lo son la pérdida o alteración no autorizada de expedientes, y para el caso de soportes electrónicos, ofrecer detalles sobre el registro de incidentes en el cual consigne los procedimientos realizados para la recuperación de los datos o para permitir la disponibilidad del proceso. **Hasta el presente la sede no cuenta con un registro de incidentes, por lo que los incisos del 1 al 4 no aplican para la sede.**

1. Los datos que registra:

a) La persona que resolvió el incidente; **N/A**
b) La metodología aplicada; **N/A**
c) Para soportes físicos: Los oficios, documentos, expedientes, estantes o archiveros, tanto los dañados como los recuperados, y **N/A**
d) Para soportes electrónicos: Los campos, registros, tablas, bases de datos o archivos electrónicos, tanto dañados como recuperados, el nombre de los sistemas y la infraestructura afectada, indicar si el incidente afectó el servidor principal y los servidores de respaldo, etc. **N/A**

2. Si el registro está en soporte físico o en soporte electrónico; **N/A**
3. Cómo asegura la integridad de dicho registro, y **N/A**
4. Para el caso de soportes electrónicos, quién autoriza la recuperación de datos. **N/A**

V. ACCESO A LAS INSTALACIONES

3. Seguridad perimetral exterior (las instalaciones del área universitaria):

La Universidad que aloja la sede en Francia cuenta con una única entrada con un vigilante en el acceso. No se permite la entrada a visitantes en horarios fuera de oficina, en fines de semana ni en días festivos.
El personal que ingrese a las instalaciones en fines de semana o días festivos debe contar con una tarjeta digital para abrir la puerta de entrada, así como registrarse en el libro de entradas y salidas.

Para las personas que acceden a sus instalaciones:

a) Se les solicita indicar la dependencia a la que asisten y motivo de visita.

4. Seguridad perimetral interior (oficina, almacén o bodega para soportes físicos, centro de datos para soportes electrónicos):

¿Qué medidas de seguridad ha implementado para controlar el acceso a los espacios donde almacena los soportes físicos o electrónicos del sistema? Por ejemplo, se espera que precise el tipo de puertas y cerraduras instaladas, si tiene instalados controles biométricos, si administra la asignación de llaves y/o claves de acceso para abrir puertas y/o estantería, si cuenta con vigilancia las 24 horas, si hay un sistema de tratamiento de datos personales de video vigilancia, entre otras medidas.

Para las personas que acceden a dichos espacios interiores:

a) Se les identifica a través de una cámara al exterior de la puerta de entrada a la oficina.
b) Se les solicita autentificación verbal en la entrada a la oficina y motivo de visita.
c) Se autoriza el acceso a las instalaciones en caso de tener un motivo académico o estudiantil, siempre y cuando alguien del personal permanente de la sede esté presente en el lugar.
d) No se les autoriza el acceso a los archivos físicos de la sede.

VI. ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

Los datos personales obtenidos mediante inscripciones a cursos, Verano Puma y otros eventos no se actualizan.

Los datos personales de la base de datos de Profesores-investigadores UNAM relacionados con universidades francófonas europeas tienen una actualización constante, aunque no periódica.

Los datos personales del personal de la sede, tanto los del personal de tiempo completo como los del personal por honorarios se actualizan conforme se actualiza el personal.

Las medidas de seguridad previstas a continuación en los incisos VII al IX, sólo aplican para soportes electrónicos

VII. PERFILES DE USUARIO Y CONTRASEÑAS

En este rubro el área universitaria deberá describir el esquema de perfiles de usuario y contraseñas que tiene implementado para control de acceso mediante una red electrónica.

1. Modelo de control de acceso (alguno de los siguientes):

a) ¿Es obligatorio (etiquetas para objetos y acreditación para sujetos)?
SÍ
b) ¿Es discrecional (matriz de control de acceso)?
SÍ
c) ¿Está basado en roles (perfiles) o grupos?
SÍ
d) ¿Está basado en reglas?
SÍ

Es obligatorio para el acceso a las carpetas en Drive que se compartan con el usuario. Cada miembro de la sede gestiona una cuenta de correo institucional (@francia.unam.mx) con su propio espacio de Google Drive. El dueño de cada carpeta es responsable de la información compartida.

2. Perfiles de usuario y contraseñas en el sistema operativo de red:

a) ¿Cuenta con un sistema operativo de red instalado en sus equipos?
NO
b) ¿Proporciona dicho sistema operativo un manejo riguroso de perfiles de usuario y contraseñas?
NO
c) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?
NO

3. Perfiles de usuario y contraseñas manejados por el software aplicativo del sistema de tratamiento de datos personales: No se cuenta con un software aplicativo del sistema de tratamiento de datos personales.

a) ¿Ofrece dicho software un manejo riguroso de perfiles de usuario y contraseñas?
N/A
b) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?
No se cuenta con un software aplicativo del sistema de tratamiento de datos personales.

4. Administración de perfiles de usuario y contraseñas:

a) ¿Quién da de alta nuevos perfiles?
La CRAI para las cuentas de Google con las que se accede a Google Drive.
b) ¿Quién autoriza la creación de nuevos perfiles?
El director de la sede
c) ¿Se lleva registro de la creación de nuevos perfiles?
SÍ

5. Acceso remoto al sistema de tratamiento de datos personales:

a) ¿Requieren los usuarios acceso remoto al equipo de cómputo que por lo general utilizan para trabajar con el sistema?
NO
b) ¿Requiere el administrador acceso remoto al equipo donde reside el sistema para realizar tareas de mantenimiento?
NO
c) ¿Cómo se evita el acceso remoto no autorizado?
Los equipos no cuentan con el acceso remoto autorizado

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

1. Señalar si realiza respaldos

a) Completos __, diferenciales _X__ o incrementales___;

b) De forma automática ____ o Manual __X___,

c) Periodicidad con que los realiza: _No existe una periodización para el respaldo de los datos.

2. El tipo de medios (por ejemplo: cintas magnéticas, discos duros, CD-ROM, entre otros) que utiliza para almacenar las copias de seguridad;
Se almacenan en la nube de Google Docs.

3. Cómo y dónde archiva esos medios, y
Actualmente no se hacen respaldos en *hardware* externos, solo mediante las nubes de almacenamiento de Google Drive.

4. Quién es el responsable de realizar estas operaciones (el área universitaria o un tercero).
La sede es responsable de sus respaldos.

IX. PLAN DE CONTINGENCIA

1. Presentar el plan de contingencia con el cual garantiza la continuidad de la operación del sistema o informar si no lo tiene, pero se encuentra desarrollándolo. **Actualmente no se cuenta con un plan de contingencia, pero se encuentra en desarrollo.**

2. Si cuenta con plan de contingencia y lo ha implementado, deberá indicar si realiza pruebas de eficiencia de este. **N/A**

3. Informar si cuenta con un sitio redundante (alterno) y señalar lo siguiente: **No se cuenta con un sitio redundante o alterno para el funcionamiento de la sede.**

a) El tipo de sitio (caliente, tibio o frío); **N/A**

b) Si el sitio es propio o subcontratado con un tercero; **N/A**

c) Los procedimientos, el equipo y el personal que designa para poner en marcha tal sitio y **N/A**

d) Tiempo que le lleva poner en marcha el sitio, según las pruebas de eficiencia. **N/A**

I. TRANSFERENCIAS DE DATOS PERSONALES

Centro de estudios mexicanos, UNAM-Francia	
Identificador único*	**UNAM-Francia_CIAP**
(Nombre del sistema A5)	**Control Interno de Personal UNAM-Francia**
	● No se realiza transferencia física.
	● No se realiza traslado de soportes electrónicos.
	● Los archivos electrónicos no están cifrados antes de su transferencia por medios electrónicos.
	● La transferencia se realiza por internet mediante correo electrónico y/o compartiendo archivos en Google drive.
	● Se desconoce si el destinatario cuenta con dispositivos de detección de intrusiones.
	● No se solicita acuse de recibo.
	● La transferencia no se formaliza mediante un instrumento jurídico.

II. RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS

1. Señalar las medidas de seguridad que ha implementado el área universitaria para el resguardo de los soportes físicos del sistema de manera que evite la alteración, pérdida o acceso no autorizado a los mismos.

La estantería cuenta con puertas con chapa, cuya llave se encuentra a resguardo del responsable y del encargado del sistema.

2. Señalar en un listado las personas (nombre, cargo, funciones y obligaciones) que tienen acceso a los soportes físicos del sistema.

Rodolfo Zanella Specia.
Director de la sede UNAM-Francia. Responsable del sistema.
Verónica Ontiveros Hernández.
Jefa del departamento de gestión de la sede UNAM-Francia. Encargada del sistema.

III. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

HASTA LA FECHA, LA SEDE NO CUENTA CON UNA BITÁCORA DE ACCESO Y OPERACIÓN COTIDIANA

1. Los datos que se registran en las bitácoras: Los incisos del 1-5 siguientes no aplican para el caso de la sede, pues no se lleva actualmente un control con bitácora.

a) Quién accede a los datos personales, fecha y hora en la que se realiza el acceso o se intenta el mismo, propósito del acceso, así como fecha y hora de salida; **N/A**
b) Para soportes físicos: Número o clave del expediente utilizado, y **N/A**
c) Para soportes electrónicos: Operaciones o acciones llevadas a cabo y registros utilizados de la base de datos. **N/A**

1. Si las bitácoras están en soporte físico o en soporte electrónico; **N/A**
2. Lugar dónde almacena las bitácoras y por cuánto tiempo; **N/A**
3. La manera en que asegura la integridad de las bitácoras, y **N/A**
4. Respecto del análisis de las bitácoras:

c) Quién es el responsable de analizarlas (si es el área universitaria o si es un tercero) y cada cuándo las analiza, y **N/A**

d) Para el caso de que las bitácoras estén en soporte electrónico: las herramientas de análisis utilizadas. **N/A**

IV. REGISTRO DE INCIDENTES:

HASTA LA FECHA, LA SEDE NO CUENTA CON UN REGISTRO DE INCIDENTES

Describir el procedimiento de atención de incidentes que tiene implementado el área universitaria y especificar si lleva registro de los incidentes relativos a soportes físicos, como lo son la pérdida o alteración no autorizada de expedientes, y para el caso de soportes electrónicos, ofrecer detalles sobre el registro de incidentes en el cual consigne los procedimientos realizados para la recuperación de los datos o para permitir la disponibilidad del proceso. **Hasta el presente la sede no cuenta con un registro de incidentes, por lo que los incisos del 1 al 4 no aplican para la sede.**

1. Los datos que registra:

a) La persona que resolvió el incidente; **N/A**
b) La metodología aplicada; **N/A**
c) Para soportes físicos: Los oficios, documentos, expedientes, estantes o archiveros, tanto los dañados como los recuperados, y **N/A**
d) Para soportes electrónicos: Los campos, registros, tablas, bases de datos o archivos electrónicos, tanto dañados como recuperados, el nombre de los sistemas y la infraestructura afectada, indicar si el incidente afectó el servidor principal y los servidores de respaldo, etc. **N/A**

2. Si el registro está en soporte físico o en soporte electrónico; **N/A**
3. Cómo asegura la integridad de dicho registro, y **N/A**
4. Para el caso de soportes electrónicos, quién autoriza la recuperación de datos. **N/A**

V. ACCESO A LAS INSTALACIONES

1. Seguridad perimetral exterior (las instalaciones del área universitaria):

La Universidad que aloja la sede en Francia cuenta con una única entrada con un vigilante en el acceso. No se permite la entrada a visitantes en horarios fuera de oficina, en fines de semana ni en días festivos.
El personal que ingrese a las instalaciones en fines de semana o días festivos debe contar con una tarjeta digital para abrir la puerta de entrada, así como registrarse en el libro de entradas y salidas.

Para las personas que acceden a sus instalaciones:

a) Se les solicita indicar la dependencia a la que asisten y motivo de visita.

2. Seguridad perimetral interior (oficina, almacén o bodega para soportes físicos, centro de datos para soportes electrónicos):

¿Qué medidas de seguridad ha implementado para controlar el acceso a los espacios donde almacena los soportes físicos o electrónicos del sistema? Por ejemplo, se espera que precise el tipo de puertas y cerraduras instaladas, si tiene instalados controles biométricos, si administra la asignación de llaves y/o claves de acceso para abrir puertas y/o estantería, si cuenta con vigilancia

las 24 horas, si hay un sistema de tratamiento de datos personales de video vigilancia, entre otras medidas.

Para las personas que acceden a dichos espacios interiores:

a) Se les identifica a través de una cámara al exterior de la puerta de entrada a la oficina.
b) Se les solicita autentificación verbal en la entrada a la oficina y motivo de visita.
c) Se autoriza el acceso a las instalaciones en caso de tener un motivo académico o estudiantil, siempre y cuando alguien del personal permanente de la sede esté presente en el lugar.
d) No se les autoriza el acceso a los archivos físicos de la sede.

VI. ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

Los datos personales obtenidos mediante inscripciones a cursos, Verano Puma y otros eventos no se actualizan.

Los datos personales de la base de datos de Profesores-investigadores UNAM relacionados con universidades francófonas europeas tienen una actualización constante, aunque no periódica.

Los datos personales del personal de la sede, tanto los del personal de tiempo completo como los del personal por honorarios se actualizan conforme se actualiza el personal.

Las medidas de seguridad previstas a continuación en los incisos VII al IX, sólo aplican para soportes electrónicos

VII. PERFILES DE USUARIO Y CONTRASEÑAS

En este rubro el área universitaria deberá describir el esquema de perfiles de usuario y contraseñas que tiene implementado para control de acceso mediante una red electrónica.

1. Modelo de control de acceso (alguno de los siguientes):

a) ¿Es obligatorio (etiquetas para objetos y acreditación para sujetos)?
SÍ
b) ¿Es discrecional (matriz de control de acceso)?
SÍ
c) ¿Está basado en roles (perfiles) o grupos?
SÍ
d) ¿Está basado en reglas?
SÍ

Es obligatorio para el acceso a las carpetas en Drive que se compartan con el usuario. Cada miembro de la sede gestiona una cuenta de correo institucional (@francia.unam.mx) con su propio espacio de Google Drive. El dueño de cada carpeta es responsable de la información compartida.

2. Perfiles de usuario y contraseñas en el sistema operativo de red:

a) ¿Cuenta con un sistema operativo de red instalado en sus equipos?
NO
b) ¿Proporciona dicho sistema operativo un manejo riguroso de perfiles de usuario y contraseñas?
NO
c) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?
NO

3. Perfiles de usuario y contraseñas manejados por el software aplicativo del sistema de tratamiento de datos personales: No se cuenta con un software aplicativo del sistema de tratamiento de datos personales.

a) ¿Ofrece dicho software un manejo riguroso de perfiles de usuario y contraseñas?
N/A
b) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?
No se cuenta con un software aplicativo del sistema de tratamiento de datos personales.

4. Administración de perfiles de usuario y contraseñas:
a) ¿Quién da de alta nuevos perfiles?
La CRAI para las cuentas de Google con las que se accede a Google Drive.
b) ¿Quién autoriza la creación de nuevos perfiles?
El director de la sede
c) ¿Se lleva registro de la creación de nuevos perfiles?
SÍ

5. Acceso remoto al sistema de tratamiento de datos personales:

a) ¿Requieren los usuarios acceso remoto al equipo de cómputo que por lo general utilizan para trabajar con el sistema?
NO
b) ¿Requiere el administrador acceso remoto al equipo donde reside el sistema para realizar tareas de mantenimiento?
NO
c) ¿Cómo se evita el acceso remoto no autorizado?
Los equipos no cuentan con el acceso remoto autorizado

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

1. Señalar si realiza respaldos
a) Completos __, diferenciales _X__ o incrementales___;
b) De forma automática ____ o Manual __X___,
c) Periodicidad con que los realiza: _No existe una periodización para el respaldo de los datos.
2. El tipo de medios (por ejemplo: cintas magnéticas, discos duros, CD-ROM, entre otros) que utiliza para almacenar las copias de seguridad:
Se almacenan en la nube de Google Docs.

3. Cómo y dónde archiva esos medios, y
Actualmente no se hacen respaldos en *hardware* externos, solo mediante las nubes de almacenamiento de Google Drive.

4. Quién es el responsable de realizar estas operaciones (el área universitaria o un tercero).
La sede es responsable de sus respaldos.

IX. PLAN DE CONTINGENCIA

1. Presentar el plan de contingencia con el cual garantiza la continuidad de la operación del sistema o informar si no lo tiene, pero se encuentra desarrollándolo. **Actualmente no se cuenta con un plan de contingencia, pero se encuentra en desarrollo.**
2. Si cuenta con plan de contingencia y lo ha implementado, deberá indicar si realiza pruebas de eficiencia de este. **N/A**

3. Informar si cuenta con un sitio redundante (alterno) y señalar lo siguiente: **No se cuenta con un sitio redundante o alterno para el funcionamiento de la sede.**

a) El tipo de sitio (caliente, tibio o frío); **N/A**
b) Si el sitio es propio o subcontratado con un tercero; **N/A**
c) Los procedimientos, el equipo y el personal que designa para poner en marcha tal sitio y **N/A**
d) Tiempo que le lleva poner en marcha el sitio, según las pruebas de eficiencia. **N/A**

I. TRANSFERENCIAS DE DATOS PERSONALES

Centro de estudios mexicanos, UNAM-Francia	
Identificador único*	**UNAM-Francia_CIAP**
(Nombre del sistema A6)	**Control de Académicos MEXICO-FRANCIA**
	● No se realiza transferencia física. ● No se realiza traslado de soportes electrónicos. ● Los archivos electrónicos no están cifrados antes de su transferencia por medios electrónicos. ● La transferencia se realiza por internet mediante correo electrónico y/o compartiendo archivos en Google drive. ● Se desconoce si el destinatario cuenta con dispositivos de detección de intrusiones. ● No se solicita acuse de recibo. ● La transferencia no se formaliza mediante un instrumento jurídico.

II. RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS

1. Señalar las medidas de seguridad que ha implementado el área universitaria para el resguardo de los soportes físicos del sistema de manera que evite la alteración, pérdida o acceso no autorizado a los mismos.

La estantería cuenta con puertas con chapa, cuya llave se encuentra a resguardo del responsable y del encargado del sistema.

2. Señalar en un listado las personas (nombre, cargo, funciones y obligaciones) que tienen acceso a los soportes físicos del sistema.

1.- Rodolfo Zanella Specia.
Director de la sede UNAM-Francia. Responsable del sistema.
2.- Verónica Ontiveros Hernández.
Jefa del departamento de gestión de la sede UNAM-Francia. Encargada del sistema.

III. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

HASTA LA FECHA, LA SEDE NO CUENTA CON UNA BITÁCORA DE ACCESO Y OPERACIÓN COTIDIANA

1. Los datos que se registran en las bitácoras: Los incisos del 1-5 siguientes no aplican para el caso de la sede, pues no se lleva actualmente un control con bitácora.

a) Quién accede a los datos personales, fecha y hora en la que se realiza el acceso o se intenta el mismo, propósito del acceso, así como fecha y hora de salida; **N/A**

b) Para soportes físicos: Número o clave del expediente utilizado, y **N/A**

c) Para soportes electrónicos: Operaciones o acciones llevadas a cabo y registros utilizados de la base de datos. **N/A**

2. Si las bitácoras están en soporte físico o en soporte electrónico; **N/A**

3. Lugar dónde almacena las bitácoras y por cuánto tiempo; **N/A**

4. La manera en que asegura la integridad de las bitácoras, y **N/A**

5. Respecto del análisis de las bitácoras:

a) Quién es el responsable de analizarlas (si es el área universitaria o si es un tercero) y cada cuándo las analiza, y **N/A**

b) Para el caso de que las bitácoras estén en soporte electrónico: las herramientas de análisis utilizadas. **N/A**

IV. REGISTRO DE INCIDENTES:

HASTA LA FECHA, LA SEDE NO CUENTA CON UN REGISTRO DE INCIDENTES

Describir el procedimiento de atención de incidentes que tiene implementado el área universitaria y especificar si lleva registro de los incidentes relativos a soportes físicos, como lo son la pérdida o alteración no autorizada de expedientes, y para el caso de soportes electrónicos, ofrecer detalles sobre el registro de incidentes en el cual consigne los procedimientos realizados para la recuperación de los datos o para permitir la disponibilidad del proceso. **Hasta el presente la sede no cuenta con un registro de incidentes, por lo que los incisos del 1 al 4 no aplican para la sede.**

1. Los datos que registra:

a) La persona que resolvió el incidente; **N/A**

b) La metodología aplicada; **N/A**

c) Para soportes físicos: Los oficios, documentos, expedientes, estantes o archiveros, tanto los dañados como los recuperados, y **N/A**

d) Para soportes electrónicos: Los campos, registros, tablas, bases de datos o archivos electrónicos, tanto dañados como recuperados, el nombre de los sistemas y la infraestructura afectada, indicar si el incidente afectó el servidor principal y los servidores de respaldo, etc. **N/A**

2. Si el registro está en soporte físico o en soporte electrónico; **N/A**

3. Cómo asegura la integridad de dicho registro, y **N/A**

4. Para el caso de soportes electrónicos, quién autoriza la recuperación de datos. **N/A**

V. ACCESO A LAS INSTALACIONES

3. Seguridad perimetral exterior (las instalaciones del área universitaria):

La Universidad que aloja la sede en Francia cuenta con una única entrada con un vigilante en el acceso. No se permite la entrada a visitantes en horarios fuera de oficina, en fines de semana ni en días festivos.
El personal que ingrese a las instalaciones en fines de semana o días festivos debe contar con una tarjeta digital para abrir la puerta de entrada, así como registrarse en el libro de entradas y salidas.

Para las personas que acceden a sus instalaciones:

a) Se les solicita indicar la dependencia a la que asisten y motivo de visita.

4. Seguridad perimetral interior (oficina, almacén o bodega para soportes físicos, centro de datos para soportes electrónicos):

¿Qué medidas de seguridad ha implementado para controlar el acceso a los espacios donde almacena los soportes físicos o electrónicos del sistema? Por ejemplo, se espera que precise el tipo de puertas y cerraduras instaladas, si tiene instalados controles biométricos, si administra la asignación de llaves y/o claves de acceso para abrir puertas y/o estantería, si cuenta con vigilancia las 24 horas, si hay un sistema de tratamiento de datos personales de video vigilancia, entre otras medidas.

Para las personas que acceden a dichos espacios interiores:

a) Se les identifica a través de una cámara al exterior de la puerta de entrada a la oficina.
b) Se les solicita autentificación verbal en la entrada a la oficina y motivo de visita.
c) Se autoriza el acceso a las instalaciones en caso de tener un motivo académico o estudiantil, siempre y cuando alguien del personal permanente de la sede esté presente en el lugar.
d) No se les autoriza el acceso a los archivos físicos de la sede.

VI. ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

Los datos personales obtenidos mediante inscripciones a cursos, Verano Puma y otros eventos no se actualizan.

Los datos personales de la base de datos de Profesores-investigadores UNAM relacionados con universidades francófonas europeas tienen una actualización constante, aunque no periódica.

Los datos personales del personal de la sede, tanto los del personal de tiempo completo como los del personal por honorarios se actualizan conforme se actualiza el personal.

Las medidas de seguridad previstas a continuación en los incisos VII al IX, sólo aplican para soportes electrónicos

VII. PERFILES DE USUARIO Y CONTRASEÑAS

En este rubro el área universitaria deberá describir el esquema de perfiles de usuario y contraseñas que tiene implementado para control de acceso mediante una red electrónica.

1. Modelo de control de acceso (alguno de los siguientes):

a) ¿Es obligatorio (etiquetas para objetos y acreditación para sujetos)?
SÍ
b) ¿Es discrecional (matriz de control de acceso)?
SÍ
c) ¿Está basado en roles (perfiles) o grupos?
SÍ
d) ¿Está basado en reglas?
SÍ

Es obligatorio para el acceso a las carpetas en Drive que se compartan con el usuario. Cada miembro de la sede gestiona una cuenta de correo institucional (@francia.unam.mx) con su propio espacio de Google Drive. El dueño de cada carpeta es responsable de la información compartida.

2. Perfiles de usuario y contraseñas en el sistema operativo de red:
a) ¿Cuenta con un sistema operativo de red instalado en sus equipos?

NO

b) ¿Proporciona dicho sistema operativo un manejo riguroso de perfiles de usuario y contraseñas?

NO

c) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?

NO

3. Perfiles de usuario y contraseñas manejados por el software aplicativo del sistema de tratamiento de datos personales: No se cuenta con un software aplicativo del sistema de tratamiento de datos personales.

a) ¿Ofrece dicho software un manejo riguroso de perfiles de usuario y contraseñas?

N/A

b) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?

No se cuenta con un software aplicativo del sistema de tratamiento de datos personales.

4. Administración de perfiles de usuario y contraseñas:

a) ¿Quién da de alta nuevos perfiles?

La CRAI para las cuentas de Google con las que se accede a Google Drive.

b) ¿Quién autoriza la creación de nuevos perfiles?

El director de la sede

c) ¿Se lleva registro de la creación de nuevos perfiles?

SÍ

5. Acceso remoto al sistema de tratamiento de datos personales:

a) ¿Requieren los usuarios acceso remoto al equipo de cómputo que por lo general utilizan para trabajar con el sistema?

NO

b) ¿Requiere el administrador acceso remoto al equipo donde reside el sistema para realizar tareas de mantenimiento?

NO

c) ¿Cómo se evita el acceso remoto no autorizado?

Los equipos no cuentan con el acceso remoto autorizado

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

1. Señalar si realiza respaldos

a) Completos __, diferenciales _X__ o incrementales___;

b) De forma automática ____ o Manual __X___,

c) Periodicidad con que los realiza: _No existe una periodización para el respaldo de los datos.

2. El tipo de medios (por ejemplo: cintas magnéticas, discos duros, CD-ROM, entre otros) que utiliza para almacenar las copias de seguridad;

Se almacenan en la nube de Google Docs.

3. Cómo y dónde archiva esos medios, y

Actualmente no se hacen respaldos en *hardware* externos, solo mediante las nubes de almacenamiento de Google Drive.

4. Quién es el responsable de realizar estas operaciones (el área universitaria o un tercero).

La sede es responsable de sus respaldos.

IX. PLAN DE CONTINGENCIA

1. Presentar el plan de contingencia con el cual garantiza la continuidad de la operación del sistema o informar si no lo tiene, pero se encuentra desarrollándolo. **Actualmente no se cuenta con un plan de contingencia, pero se encuentra en desarrollo.**

2. Si cuenta con plan de contingencia y lo ha implementado, deberá indicar si realiza pruebas de eficiencia de este. **N/A**

3. Informar si cuenta con un sitio redundante (alterno) y señalar lo siguiente: **No se cuenta con un sitio redundante o alterno para el funcionamiento de la sede.**

a) El tipo de sitio (caliente, tibio o frío); **N/A**

b) Si el sitio es propio o subcontratado con un tercero; **N/A**

c) Los procedimientos, el equipo y el personal que designa para poner en marcha tal sitio y **N/A**

d) Tiempo que le lleva poner en marcha el sitio, según las pruebas de eficiencia. **N/A**

7. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

7.1. Herramientas y recursos para monitoreo de la protección de datos personales

Centro de estudios mexicanos, UNAM-Francia		
Identificador único*	UNAM-Francia_CIAP	
(Nombre del sistema A1)*	Control registro Verano Puma	
Recurso*	Descripción*	Control*
Acceso restringido a la carpeta de Google Drive y a la hoja de cálculo en la que se almacena y resguarda la información	Auditoria constante de los permisos de acceso a la carpeta en Google Drive	Revisión manual
(Nombre del sistema A2)*	Control de Becarios	
Recurso*	Descripción*	Control*
Acceso restringido a la carpeta de Google Drive y a la hoja de cálculo en la que se almacena y resguarda la información	Auditoría constante de los permisos de acceso a la carpeta en Google Drive	.Revisión manual
Acceso controlado a las instalaciones de la UNAM-Francia.	Registro de visitantes a la entrada de las instalaciones de la sede.	Registro físico de los visitantes.
(Nombre del sistema A3)*	Control de asistentes a eventos en línea	
Recurso*	Descripción*	Control*
Acceso restringido a la carpeta de Google Drive y a la hoja de cálculo en la que se almacena y resguarda la información	Auditoría constante de los permisos de acceso a la carpeta en Google Drive	Revisión manual
(Nombre del sistema A4)*	Control de asistentes a eventos presenciales	
Recurso*	Descripción*	Control*
Acceso restringido a la carpeta de Google Drive y a la hoja de cálculo en la que se almacena y resguarda la información	Auditoría constante de los permisos de acceso a la carpeta en Google Drive	Revisión manual
(Nombre del sistema A5)*	Control de Personal UNAM-Francia	
Recurso*	Descripción*	Control*
Acceso restringido a la carpeta de Google Drive y a la hoja de cálculo en la que se almacena y resguarda la información	Auditoría constante de los permisos de acceso a la carpeta en Google Drive	Revisión manual
Acceso controlado a las instalaciones de la UNAM-Francia.	Registro de visitantes a la entrada de las instalaciones de la sede.	Registro físico de los visitantes.
(Nombre del sistema A6)*	Control de Académicos MÉXICO-FRANCIA	
Recurso*	Descripción*	Control*

Acceso restringido a la carpeta de Google Drive y a la hoja de cálculo en la que se almacena y resguarda la información	Auditoría constante de los permisos de acceso a la carpeta en Google Drive	Revisión manual

7.2. Procedimiento para la revisión de las medidas de seguridad

Centro de estudios mexicanos, UNAM-Francia		
Identificador único*	UNAM-Francia_CIAP	
(Nombre del sistema A1)*	Control registro Verano Puma	
Recurso*	Descripción*	Control*
Acceso restringido a la carpeta de Google Drive y a la hoja de cálculo en la que se almacena y resguarda la información	Auditoria constante de los permisos de acceso a la carpeta en Google Drive	Revisión manual
(Nombre del sistema A2)*	Control de Becarios	
Recurso*	Descripción*	Control*
Acceso restringido a la carpeta de Google Drive y a la hoja de cálculo en la que se almacena y resguarda la información	Auditoría constante de los permisos de acceso a la carpeta en Google Drive	.Revisión manual
Acceso controlado a las instalaciones de la UNAM-Francia.	Registro de visitantes a la entrada de las instalaciones de la sede.	Registro físico de los visitantes.
(Nombre del sistema A3)*	Control de asistentes a eventos en línea	
Recurso*	Descripción*	Control*
Acceso restringido a la carpeta de Google Drive y a la hoja de cálculo en la que se almacena y resguarda la información	Auditoría constante de los permisos de acceso a la carpeta en Google Drive	Revisión manual
(Nombre del sistema A4)*	Control de asistentes a eventos presenciales	
Recurso*	Descripción*	Control*
Acceso restringido a la carpeta de Google Drive y a la hoja de cálculo en la que se almacena y resguarda la información	Auditoría constante de los permisos de acceso a la carpeta en Google Drive	Revisión manual
(Nombre del sistema A5)*	Control de Personal UNAM-Francia	
Recurso*	Descripción*	Control*
Acceso restringido a la carpeta de Google Drive y a la hoja de cálculo en la que se almacena y resguarda la información	Auditoría constante de los permisos de acceso a la carpeta en Google Drive	Revisión manual
Acceso controlado a las instalaciones de la UNAM-Francia.	Registro de visitantes a la entrada de las instalaciones de la sede.	Registro físico de los visitantes.
(Nombre del sistema A6)*	Control de Académicos MÉXICO-FRANCIA	
Recurso*	Descripción*	Control*
Acceso restringido a la carpeta de Google Drive y a la hoja de cálculo en la	Auditoría constante de los permisos de acceso a la carpeta en Google Drive	Revisión manual

que se almacena y resguarda la información		

7.3. Resultados de la evaluación y pruebas a las medidas de seguridad

No se han realizado pruebas a las medidas de seguridad. El protocolo se encuentra en proceso.

Centro de estudios mexicanos, UNAM-Francia		
Identificador único*	**UNAM-Francia_CIAP**	
(Nombre del sistema A1)*	**Control de registro Verano Puma**	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***
N/A	*N/A*	*N/A*
(Nombre del sistema A2)*	**Control de Becarios**	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***
N/A	*N/A*	*N/A*
(Nombre del sistema A3)*	**Control de asistentes a eventos en línea**	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***
N/A	*N/A*	*N/A*
(Nombre del sistema A4)*	**Control de asistentes a eventos presenciales**	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***
N/A	*N/A*	*N/A*
(Nombre del sistema A5)*	**Control Interno de Personal UNAM-Francia**	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***
N/A	*N/A*	*N/A*
(Nombre del sistema A6)*	**Control de Académicos MÉXICO-FRANCIA**	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***
N/A	*N/A*	*N/A*

7.4. Acciones para la corrección y actualización de las medidas de seguridad

Medida de seguridad*	**Acciones***	**Responsable***
Las carpetas físicas se resguardan bajo llave y su acceso es restringido.	*Elaboración de bitácora de consulta.*	*Dra. Verónica Ontiveros*
(Nombre del sistema A5)*	**Control Interno de Personal UNAM-Francia**	
Medida de seguridad*	**Acciones***	**Responsable***
Las carpetas físicas se resguardan bajo llave y su acceso es restringido.	*Elaboración de bitácora de consulta.*	*Dra. Verónica Ontiveros*
Las carpetas físicas se resguardan bajo llave y su acceso es restringido.	*Elaboración de bitácora de consulta.*	*Dra. Verónica Ontiveros*
(Nombre del sistema A6)*	**Control de Académicos MÉXICO-FRANCIA**	
Medida de seguridad*	**Acciones***	**Responsable***
Las carpetas físicas se resguardan bajo llave y su acceso es restringido.	*Elaboración de bitácora de consulta.*	*a) Dra. Verónica Ontiveros*

8. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

8.1. Programa de capacitación a los responsables de tratamiento de datos personales

Al momento la sede no cuenta con un programa específico de capacitación para los responsables de tratamiento de datos personales.

Centro de estudios mexicanos, UNAM-Francia			
Identificador único*	**UNAM-Francia_CIAP**		
(Nombre del sistema A1)*	**Control registro Verano Puma**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
N/A	**N/A**	**N/A**	**N/A**
(Nombre del sistema A2)*	**Control de Becarios**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
N/A	**N/A**	**N/A**	**N/A**
(Nombre del sistema A3)*	**Control de asistentes a eventos virtuales.**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
N/A	**N/A**	**N/A**	**N/A**
(Nombre del sistema A4)*	**Control de asistentes a eventos presenciales.**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
N/A	**N/A**	**N/A**	**N/A**
(Nombre del sistema A5)*	**Control Interno de Personal UNAM-Francia**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
N/A	**N/A**	**N/A**	**N/A**
(Nombre del sistema A6)*	**Control de Académicos MÉXICO-FRANCIA**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
N/A	**N/A**	**N/A**	**N/A**

8.2. Programa de difusión de la protección a los datos personales

No se realiza la difusión de datos personales.

Centro de estudios mexicanos, UNAM-Francia			
Identificador único*	**UNAM-Francia_CIAP**		
(Nombre del sistema A1)*	**Control de Registro Verano Puma**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
N/A	**N/A**	**N/A**	**N/A**
(Nombre del sistema A2)*	**Control de Becarios**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
N/A	**N/A**	**N/A**	**N/A**
(Nombre del sistema A3)*	**Control de asistentes a eventos virtuales**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
N/A	**N/A**	**N/A**	**N/A**
(Nombre del sistema A4)*	**Control de asistentes a eventos presenciales**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
N/A	**N/A**	**N/A**	**N/A**
(Nombre del sistema A5)*	**Control Interno de Personal UNAM-Francia**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
N/A	**N/A**	**N/A**	**N/A**
(Nombre del sistema A6)*	**Control de Académicos MÉXICO-FRANCIA**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
N/A	**N/A**	**N/A**	**N/A**

9. MEJORA CONTINUA

9.1. Actualización y mantenimiento de sistemas de información

Se iniciará con las medidas y protocolos establecidos en el inciso 5.

Centro de estudios mexicanos, UNAM-Francia			
Identificador único*	**UNAM-Francia_CIAP**		
(Nombre del sistema A1) *	**Control de registro Verano PUMA**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Protocolo de vigencia y renovación de claves de acceso Google Drive	Renovación de claves de acceso. Control de claves y folders compartidos	Renovación de las claves cada 6 meses.	Esta actividad permitirá el control externo e interno al acceso de los datos resguardados.
Alojamiento en nube privada o servidor local independiente de la nube en Google Drive	Solicitar el alojamiento en nube privada o servidor local	Anual	El respaldo de los datos en una nube de acceso restringido tanto al interior como al exterior de la sede.
(Nombre del sistema A2) *	**Control de Becarios**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Protocolo de vigencia y renovación de claves de acceso Google Drive	Renovación de claves de acceso. Control de claves y folders compartidos	Renovación de las claves cada 6 meses.	Esta actividad permitirá el control externo e interno al acceso de los datos resguardados.
Alojamiento en nube privada o servidor local independiente de la nube en Google Drive	Solicitar el alojamiento en nube privada o servidor local	Anual	El respaldo de los datos en una nube de acceso restringido tanto al interior como al exterior de la sede.
Bitácora de consulta de archivos físicos	Elaborar y mantener una bitácora de consulta de los archivos físicos	Anual	Controlar y registrar el acceso a los archivos físicos.
(Nombre del sistema A3) *	**Control de asistentes a eventos en línea**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Protocolo de vigencia y renovación de claves de acceso Google Drive	Renovación de claves de acceso. Control de claves y folders compartidos	Renovación de las claves cada 6 meses.	Esta actividad permitirá el control externo e interno al acceso de los datos resguardados.
Alojamiento en nube privada o servidor local independiente de la nube en Google Drive	Solicitar el alojamiento en nube privada o servidor local	Anual	El respaldo de los datos en una nube de acceso restringido tanto al interior como al exterior de la sede.
(Nombre del sistema A4) *	**Control de asistentes a eventos en presencial**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
	Renovación de claves de acceso.		Esta actividad permitirá el control externo e

Protocolo de vigencia y renovación de claves de acceso Google Drive	Control de claves y folders compartidos	Renovación de las claves cada 6 meses.	interno al acceso de los datos resguardados.
Alojamiento en nube privada o servidor local independiente de la nube en Google Drive	Solicitar el alojamiento en nube privada o servidor local	Anual	El respaldo de los datos en una nube de acceso restringido tanto al interior como al exterior de la sede.
(Nombre del sistema A5) *	**Control Interno de Personal UNAM-Francia**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Protocolo de vigencia y renovación de claves de acceso Google Drive	Renovación de claves de acceso. Control de claves y folders compartidos	Renovación de las claves cada 6 meses.	Esta actividad permitirá el control externo e interno al acceso de los datos resguardados.
Alojamiento en nube privada o servidor local independiente de la nube en Google Drive	Solicitar el alojamiento en nube privada o servidor local	Anual	El respaldo de los datos en una nube de acceso restringido tanto al interior como al exterior de la sede.
Bitácora de consulta de archivos físicos	Elaborar y mantener una bitácora de consulta de los archivos físicos	Anual	Controlar y registrar el acceso a los archivos físicos.
(Nombre del sistema A6) *	**Control de Académicos MÉXICO-FRANCIA**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Protocolo de vigencia y renovación de claves de acceso Google Drive	Renovación de claves de acceso. Control de claves y folders compartidos	Renovación de las claves cada 6 meses.	Esta actividad permitirá el control externo e interno al acceso de los datos resguardados.
Alojamiento en nube privada o servidor local independiente de la nube en Google Drive	Solicitar el alojamiento en nube privada o servidor local	Anual	El respaldo de los datos en una nube de acceso restringido tanto al interior como al exterior de la sede.

9.2. Actualización y mantenimiento de equipo de cómputo

Centro de estudios mexicanos, UNAM-Francia			
Identificador único*	**UNAM-Francia_CIAP**		
(Nombre del sistema A1)*	**Control de Registro Verano Puma**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
N/A	**N/A**	**N/A**	**N/A**
(Nombre del sistema A2)*	**Control de Becarios**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
N/A	**N/A**	**N/A**	**N/A**
(Nombre del sistema A3)*	**Control de asistentes a eventos virtuales**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
N/A	**N/A**	**N/A**	**N/A**
(Nombre del sistema A4)*	**Control de asistentes a eventos presenciales**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
N/A	**N/A**	**N/A**	**N/A**
(Nombre del sistema A5)*	**Control Interno de Personal UNAM-Francia**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
N/A	**N/A**	**N/A**	**N/A**
(Nombre del sistema A6)*	**Control de Académicos MÉXICO-FRANCIA**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
N/A	**N/A**	**N/A**	**N/A**

9.3. Procesos para la conservación, preservación y respaldos de información

Centro de estudios mexicanos, UNAM-Francia		
Identificador único*	**UNAM-Francia_CIAP**	
(Nombre del sistema A1)*	**Control de registro Verano Puma**	
Proceso*	**Descripción***	**Responsable***
Respaldo de la información en disco duro externo.	*Respaldar la información en un disco duro externo al finalizar de armar los expedientes de los participantes. Resguardo del* hardware *bajo llave.*	*Dra. Verónica Ontiveros* *1 día*
(Nombre del sistema A2)*	**Control de Becarios**	
Proceso*	**Descripción***	**Responsable***
Respaldo de la información en disco duro externo.	*Respaldar la información en un disco duro externo al finalizar de armar los expedientes de los participantes. Resguardo del* hardware *bajo llave.*	*Dra. Verónica Ontiveros* *1 día*
(Nombre del sistema A3)*	**Control de asistentes a eventos virtuales**	
Proceso*	**Descripción***	**Responsable***
N/A	**N/A**	**N/A**
(Nombre del sistema A4)*	**Control de asistentes a eventos presenciales**	
Proceso*	**Descripción***	**Responsable***
N/A	**N/A**	**N/A**
(Nombre del sistema A5)*	**Control Interno de Personal UNAM-Francia**	
Proceso*	**Descripción***	**Responsable***
Respaldo de la información en disco duro externo.	*Respaldar la información en un disco duro externo al finalizar de armar los expedientes de los participantes. Resguardo del* hardware *bajo llave.*	*Dra. Verónica Ontiveros* *1 día*
(Nombre del sistema A6)*	**Control de Académicos UNAM-Francia**	
Proceso*	**Descripción***	**Responsable***
Respaldo de la información en disco duro externo.	*Respaldar la información en un disco duro externo al finalizar de armar los expedientes de los participantes. Resguardo del* hardware *bajo llave.*	*Dra. Verónica Ontiveros* *1 día*

9.4. Procesos de borrado seguro y disposición final de equipos y componentes informáticos

Al momento no se cuenta con procesos de borrado seguro y disposición final de equipos y componentes informáticos.

Centro de estudios mexicanos, UNAM-Francia		
Identificador único*	**UNAM-Francia_CIAP**	
(Nombre del sistema A1)*	**Control de registro Verano Puma**	
Proceso*	**Descripción***	**Responsable***
N/A	**N/A**	**N/A**
(Nombre del sistema A2)*	**Control de Becarios**	
Proceso*	**Descripción***	**Responsable***
N/A	**N/A**	**N/A**
(Nombre del sistema A3)*	**Control de asistentes a eventos virtuales**	
Proceso*	**Descripción***	**Responsable***
N/A	**N/A**	**N/A**
(Nombre del sistema A4)*	**Control de asistentes a eventos presenciales**	
Proceso*	**Descripción***	**Responsable***
N/A	**N/A**	**N/A**
(Nombre del sistema A5)*	**Control Interno de Personal UNAM-Francia**	
Proceso*	**Descripción***	**Responsable***
N/A	**N/A**	**N/A**
(Nombre del sistema A6)*	**Control de Académicos MÉXICO-FRANCIA**	
Proceso*	**Descripción***	**Responsable***
N/A	**N/A**	**N/A**

10. PROCEDIMIENTO PARA LA CANCELACIÓN DE UN SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

(Informar y describir el procedimiento para la cancelación de un sistema de tratamiento de datos personales.)

No se cuenta en la sede con un sistema de tratamiento de datos personales.

A) DATOS DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES QUE SERÁ CANCELADO: **N/A**

a) Denominación
b) Motivo de la cancelación

B) PLAZOS Y CONDICIONES PARA EL BLOQUEO DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES: **N/A**

(Señalar el periodo de bloqueo, considerando los plazos de prescripción para el ejercicio de algún derecho por parte de los titulares de conformidad con la normatividad de cada área universitaria. Asimismo, se debe señalar las condiciones y el procedimiento que se seguirá para realizar el bloqueo)

C) MEDIDAS DE SEGURIDAD PARA EL BLOQUEO Y POSTERIOR SUPRESIÓN DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES: **N/A**
(Describir las medidas de seguridad aplicables al periodo de bloqueo y la supresión del sistema, considerando el nivel de protección requerido en virtud del tipo de datos personales contenidos en el sistema)

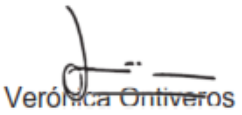
D) PROCEDIMIENTO PARA LA SUPRESIÓN DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES **N/A**

(Describir el procedimiento para suprimir el sistema, una vez cumplido el plazo de bloqueo)

E) MECANISMOS PARA LA SUPRESIÓN DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES **N/A**

(Describir las técnicas para la eliminación física del sistema)

11. APROBACIÓN DEL DOCUMENTO DE SEGURIDAD

		Nombre y firma de quienes revisaron el presente documento:
Responsable del desarrollo:	Mtra. Mariel de Lourdes Mera Cázares Enlace en México de UNAM-Francia enlace@francia.unam.mx	
Revisó:	Dra. Verónica Ontiveros Hernández Responsable de proyectos académicos. +33(0)144275373 veronica@francia.unam.mx	
Autorizó:	Dr. Rodolfo ZanellaSpecia Director rodolfo.zanella@francia.unam.mx +33(0)144275374	
Fecha de aprobación:	(Incluir la fecha de liberación del documento)	11 de noviembre de 2022
Fecha de actualización:	(Incluir la primer versión e ir agregando las subsiguientes del documento)	19 de agosto de 2022

ANEXO II. FORMATO UNIVERSITARIO DE "SOLICITUD DE EJERCICIO DE DERECHOS ARCO"

Formato de solicitud de ejercicio de derechos Acceso, Rectificación, Cancelación y Oposición (ARCO)

Con fundamento en el artículo 54 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, esta área universitaria le solicita llenar el presente formato para ejercer sus derechos de Acceso, Rectificación, Cancelación y Oposición.

1. Datos del Área Universitaria de la UNAM responsable de tratar los datos personales*:

2. Datos del Titular de los Datos Personales*:

Primer apellido:	Segundo apellido:	Nombre(s):
CURP (para evitar homónimos):		

3. Datos del solicitante:

Primer apellido:	Segundo apellido:	Nombre(s):
Indicar si los datos corresponden a:		
☐Titular		
☐Menor de edad		
☐Persona que se encuentren en estado de interdicción o incapacidad establecida por ley.		
☐Fallecida		
Datos de identidad y representación legal (opcional, solo si usted no es el titular de los datos personales)		
☐Persona física:		
☐Nombre completo del representante:		
☐Representación de un menor de edad:		
☐Representación de una persona que se encuentren en estado de interdicción o incapacidad establecida por ley.		
☐Persona moral:		
☐Nombre o razón social del representante:		
Registro Federal de Contribuyentes (RFC):		
Documento con el que acredita la representación:		
☐Poder notarial ☐Carta poder simple signada ante dos testigos (con copia de los documentos que acrediten la identidad de los testigos y titular) ☐Declaración en comparecencia del Titular (en las instalaciones del área universitaria).		

4. Documento oficial de identificación del titular o solicitante (sólo originales) *:

☐Credencial para votar (INE)	☐Pasaporte	☐Licencia de conducir

☐Cédula profesional	☐Cartilla del Servicio militar nacional	☐Documento migratorio
☐Acta de nacimiento	☐Acta de defunción	☐Otra identificación con fotografía (especifique):

5. Medio por el cual prefiere que le sea notificada la puesta a disposición de la respuesta*:

☐Acudir al área universitaria donde presentó este formato	☐Correo electrónico (especificar):

6. Modalidad en la cual prefiere le sean entregados los datos, en caso de ser procedente. *

☐Copia simple	☐Correo electrónico
☐Copia certificada	☐ Otro medio electrónico como USB/CD ROOM/ DVD *(previo depósito de ficha de pago):*
☐Consultas directas	☐Yo proporciono el medio magnético o electrónico para reproducir los datos personales.

7. Tipo de solicitud de ejercicio de Derechos Acceso, Rectificación, Cancelación y Oposición (ARCO) a datos personales*:

☐ACCESO
Describir la información datos personales que obran en posesión del área universitaria y a los que requiere tener acceso*: _____ _____ _____
Señalar el nombre y ubicación del archivo o registro de datos personales*: _____ _____ _____
☐RECTIFICACIÓN
☐Son inexactos.
☐Son incompletos.
☐Requieren ser actualizados
Justificación y documentación original que acompaña para motivar su petición*: _____ _____ _____
CANCELACIÓN (supresión o eliminación)
Causas que motivan la cancelación*:
OPOSICIÓN (cese del tratamiento)

Causas que motivan la oposición (daño o perjuicio que le causa la persistencia del tratamiento de sus datos)*****:_____ _____
Señalar si es para una finalidad específica o para todos los sistemas de información que obren en el área universitaria*._____
Documentación original que acompaña para motivar su petición*: _____
Señalar la referencia o documento que facilite la localización de sus datos personales*
_____ _____

Leí el Aviso de privacidad del área universitaria a la que acudo y en este acto otorgo el consentimiento para que mis datos personales sean tratados conforme al mismo.

_____

Firma o huella dactilar*****

Plazos y procedimiento para la atención de las solicitudes de ejercicio de derechos ARCO:
Una vez que se presentó la solicitud, esta área universitaria cuenta con:

- Un plazo de 20 días hábiles, contados a partir del día siguiente a la recepción de la solicitud, para informarle si procede o no el ejercicio del derecho solicitado.
- Un plazo de 15 días hábiles, contados a partir del día siguiente en el que le haya notificado la respuesta anterior, en caso de que haya procedido el ejercicio del derecho, deberá llevar a cabo las acciones necesarias para hacerlo efectivo.

El ejercicio de los derechos ARCO será sencillo y gratuito, siempre que no rebase las 20 hojas simples, por lo que las áreas universitarias realizarán el cobro del costo de reproducción de acuerdo con los Lineamientos para la determinación de los costos de reproducción y envío en el marco de solicitudes de acceso a Información y entrega de datos personales en la Universidad Nacional Autónoma de México.

ANEXO III. CARTA DE CONFIDENCIALIDAD

Carta compromiso de confidencialidad, no divulgación, reserva y resguardo de información y datos personales

(Este documento debe firmarse por todas aquellas personas que por su empleo, cargo o comisión en la Universidad reciban y traten información confidencial de otras personas)

CIUDAD DE _____, A (DD-MM-AAAA)

(Nombre completo), (cargo), adscrita(o) *(dependencia/entidad de adscripción)* de la Universidad Nacional Autónoma de México (en adelante la UNAM) acepto los términos y condiciones, que se describen más adelante, de resguardo, reserva, custodia y protección de la seguridad y confidencialidad de la información, datos personales y de todo tipo de documentos propiedad de la UNAM de los que tenga conocimiento, con motivo de las funciones que desempeño en la Universidad.

El presente compromiso me responsabiliza respecto de la información que me sea proporcionada por la UNAM, ya sea de forma oral, escrita, impresa, sonora, visual, electrónica, informática u holográfica, contenida en cualquier tipo de documento, que puede consistir en: expedientes, reportes, estudios, actas, resoluciones, oficios, correspondencia, acuerdos, directivas, directrices, circulares, contratos, convenios, instructivos, notas, memorandos, estadísticas, o bien, cualquier otro registro en medio conocido o por conocer que documente el ejercicio de las facultades, funciones y competencias del área universitaria y de los servidores universitarios, sin importar su fuente o fecha de elaboración.

La información que me sea proporcionada podría ser considerada, según el caso, como reservada, privilegiada y confidencial, en los términos de las leyes aplicables, por lo que me obligo a protegerla, reservarla, resguardarla y no divulgarla, utilizándola única y exclusivamente para llevar a cabo y cumplir con las actividades y obligaciones que expresamente me sean conferidas por la Universidad.

Es mi responsabilidad no reproducir, hacer pública o divulgar a terceros la información objeto de la presente Carta, y de cumplir con las medidas de seguridad adecuadas al tipo de documento con el que se trabaje.

Mi obligación de confidencialidad no es aplicable en los siguientes casos:

a) Cuando la información se encuentre en el dominio público en el momento en que me sea suministrada o, una vez suministrada, ésta se haga pública.
b) Cuando la legislación vigente o un mandato judicial exija su divulgación.
c) Cuando la información se desarrolle o reciba legítimamente de terceros, de forma totalmente independiente a mi relación con la Universidad.

A t e n t a m e n t e

_____
Firma o huella dactilar

ANEXO IV. RUTA CRÍTICA PARA CUMPLIMIENTO DE LAS MEDIDAS DE SEGURIDAD TÉCNICAS (MST)

A continuación, se presentan los requisitos técnicos para sistemas de información, descritos en las MST del capítulo II de las Normas Complementarias, por orden de prioridad, esto es: de los mínimos indispensables para asegurar los datos personales hasta los necesarios para incrementar la protección de dichos datos.

Dada la complejidad de diversos sistemas en la UNAM, se ha dispuesto la ruta crítica para el cumplimiento de las MST en tres etapas para los sistemas de información que a la fecha de publicación de esta guía estén en producción o funcionamiento. Todo sistema de información deberá satisfacer a cabalidad el 100% de las MST en un tiempo máximo de un año contado a partir de la publicación de las MST para conservar su registro y publicación dentro del dominio institucional ***.unam.mx***.

A) **Etapa 1. Corto plazo**. Requisitos de misión crítica y mínimos indispensables para la protección de datos personales y datos personales sensibles. Cumplimiento obligatorio en menos de treinta días hábiles.
B) **Etapa 2. Mediano plazo**. Requisitos importantes para garantizar la protección de datos personales y datos personales sensibles. Ejecución estimada entre un mes y seis meses.
C) **Etapa 3. Largo plazo**. Requisitos necesarios para reforzar la seguridad en la protección de datos personales y datos personales sensibles. Ejecución estimada entre seis y doce meses.

Instrucciones

- Para cada MST se ha diseñado un formato, el cual está numerado en correspondencia con la ruta crítica de cumplimiento.
- Se deberán completar todos los formatos aplicables por cada uno de los sistemas de información a cargo del Área Universitaria.
- Todos los formatos deberán integrar el anexo del documento de seguridad de datos personales.
- En el caso de los sistemas que estén en desarrollo al momento de la publicación de las Normas complementarias, deberán cumplir con el 100% de las MST, previo a su publicación como sistema en producción.
- Es requisito indispensable el cumplimiento de las MST para conservar el registro dominio institucional ***.unam.mx*** en el caso de servicios Web.

Núm. formato	Etapa	Duración estimada	Medidas de seguridad técnicas y proceso recomendado para su cumplimiento
ETAPA 1			
Anexo I, numerales 1 y 2	1	Un día hábil	**Generar el inventario de sistemas de tratamiento de datos personales y la Estructura de descripción de los sistemas de tratamiento de datos personales.**
			A) Integrar la información correspondiente a todos los sistemas que dan tratamiento de datos personales en el área universitaria.
			B) Llenar formatos y colocar nombre y firma de quien realizó la acción.
1	1	Un día hábil	**Artículo 18. I. c) Utilizar datos no personales durante el desarrollo y pruebas de los sistemas.**
			A) Realizar respaldo completo de la base de datos.
			B) Ejecutar consulta en el sistema de información, por medio de formato o comandos.

			C) Verificar que los datos usados en el desarrollo no correspondan a personas identificables.
			D) Si se usan datos de personas identificables, cambiar por datos genéricos o datos ficticios y regresar al punto B.
			E) Si no se usan datos de personas identificables, llenar formato 1 con nombre y firma de quien realizó la acción, fecha de inicio y de conclusión.
2	1	Un día hábil	**Artículo 18. I. e) Asignar o revocar los privilegios de acceso para los usuarios teniendo como base el principio del menor privilegio.**
			A) Realizar respaldo completo de la base de datos.
			B) Ejecutar consulta en el sistema de información de la lista de usuarios y sus niveles o privilegios de acceso.
			C) Validar que los niveles de acceso son acordes a la relación del usuario con el tratamiento de datos personales.
			D) Si hay usuarios con privilegios mayores a los que les son necesarios, cambiar al mínimo indispensable e informarlo al usuario. Regresar al punto B.
			E) Si los privilegios de acceso son correctos para los usuarios, llenar formato 2 con nombre y firma de quien realizó la acción, fecha de inicio y de conclusión.
3	1	Tres días hábiles	**Artículo 18. I. g) Instalar y mantener vigentes certificados de comunicación segura SSL en el caso de servicios basados en Web.**
			A) En caso de no tener un certificado SSL vigente, enviar correo electrónico al Departamento de Firma Electrónica de DGTIC a firma.tic@unam.mx solicitando la asignación.
			B) El Departamento de Firma Electrónica Avanzada envía procedimiento para obtención de CSR del servidor, formato de la solicitud y costos de recuperación en función del tipo de certificado requerido (organizacional, comodín o corporativo).
			C) Completar documentación, proceso y pago de costo de recuperación. Enviar comprobantes a firma.tic@unam.mx.
			D) Al recibir el certificado SSL, instalarlo en el servidor de acuerdo con las instrucciones recibidas junto con el certificado.
			E) Llenar formato 3 y colocar nombre y firma de quien realizó la acción.
4	1	Dos días hábiles	**Artículo 18. I. h) Definir el plan de respaldos de la información, incluyendo periodicidad y alcance.**
			A) Elaborar documento con la secuencia de respaldos al menos con el siguiente orden:
			- Diario – incremental.
			- Semanal – incremental.
			- Mensual – total.
			B) Establecer en el plan los medios para resguardo del respaldo y su forma de identificación:
			- En línea: mismo equipo donde se ejecuta el sistema.
			- Respaldo como servicio: otro equipo de almacenamiento.
			- Fuera de línea: medios magnéticos (cintas, discos) y/u ópticos.
			C) Incluir en el plan:

			- Responsables de cada tipo y medio de respaldo.
			- Rotación de respaldos y medios.
			- Áreas de resguardo.
			- Métodos de cifrado.
			- RTO: *Recovery Time Objective*. Tiempo objetivo de recuperación.
			- RPO: *Recovery Point Objective*: Punto objetivo de recuperación.
			D) Concluir este documento, adjuntarlo a SGPDP, llenar formato 4 y colocar nombre y firma de quien realizó la acción.
5	1	Un día hábil	**Artículo 18. I. i)Definir el procedimiento para el borrado seguro.**
			A) Elaborar documento con el procedimiento y la herramienta para borrado seguro en función del tipo de base de datos para registros, tablas y base de datos.
			B) Incluir en el documento de borrado seguro el proceso de verificación de la no existencia del dato, generalmente por medio de consultas y de copias de respaldo.
			C) El borrado seguro debe incluirse en los respaldos incrementales y totales y en cualquiera de los medios de respaldo, así como máquinas virtuales o contenedores.
			D) Concluir este documento, adjuntarlo a SGPDP llenar formato 5 y colocar nombre y firma de quien realizó la acción.
6	1	Un día hábil	**Artículo 18. II. a) Sincronizar la fecha y hora con el servidor NTP (Network Time Protocol) oficial de la UNAM**
			A) Realizar la verificación y configuración con privilegio de administrador del sistema operativo.
			B) En función del sistema operativo, acceder a la configuración de servidor de tiempo (NTP) en interfaz gráfica o por medio de línea de comandos. *Por ejemplo*, en el caso del sistema operativo Linux:
			- Verificar la existencia del archivo */etc/ntp.conf*
			- Editar el archivo *ntp.conf* incluyendo en la primera línea:
			server ntpdgtic.redunam.unam.mx ***ó***
			server 132.247.169.17
			- Reiniciar el demonio del cliente NTP con el comando *sudo servicentpreload.*
			C) En caso de no tener el cliente NTP instalado, descargarlo del repositorio de aplicaciones del sistema operativo, instalarlo y regresar al punto B.
			D) Llenar formato 6 y colocar nombre y firma de quien realizó la acción.
7	1	Dos días hábiles	**Artículo 18. II. b) Instalar y mantener actualizado el software antimalware.**
			A) En función del sistema operativo, instalar uno o varios programas para la contención de malware. *Por ejemplo*, para el caso del sistema operativo Linux existen herramientas de código abierto y uso libre como *chkrootkit, rootkit hunter, bothunter, clamAV, avast*, entre otros, que se pueden instalar desde el repositorio correspondiente a la distribución de Linux en uso.

			B) Disponer de comandos para la localización de amenazas. *Por ejemplo*, para el caso de Linux, se recomienda usar el comando *grep* para la detección de cadenas regulares de texto en las invocaciones al *shell*.
			C) Una vez instalada la solución, verificar periódicamente su actualización.
			D) Llenar formato 7 y colocar nombre y firma de quien realizó la acción.
8	1	Cuatro días hábiles	**Artículo 18. II. c) Instalar las actualizaciones de seguridad más recientes disponibles.**
			A) En función del sistema operativo, se debe revisar la vigencia y actualización de las herramientas de seguridad de la información. *Por ejemplo*, en el sistema operativo Linux ejecutar *apt-getupdate* para obtener la lista de actualizaciones, especialmente en el repositorio *security*de la respectiva distribución.
			B) Realizar un respaldo del sistema para garantizar retorno a versión anterior en caso de incompatibilidad con alguna aplicación de las actualizaciones de seguridad.
			C) Instalar las actualizaciones en el sistema operativo.
			D) Llenar formato 8 y colocar nombre y firma de quien realizó la acción.
9	1	Cuatro días hábiles	**Artículo 19. I. a) Aplicar un mecanismo de autenticación para las personas autorizadas con base en el principio del menor privilegio.**
			A) Verificar el tipo de control de acceso al sistema, esto es: a través de contraseñas, claves, identificadores, nombres de usuario, nombres de dominio, entre otros. Según sea aplicable al sistema de información en lo particular. En caso de no tener un control de acceso establecer al menos uno como: usuarios de sistema operativo, cuenta y contraseña de sistema.
			B) Revisar que los privilegios de acceso sean los adecuados en función del rol del usuario. *Por ejemplo:* el usuario de conexión a la base de datos no debe estar asignado a alguna cuenta del personal que tiene acceso al sistema.
			D) Llenar formato 9 y colocar nombre y firma de quien realizó la acción.
10	1	Dos días hábiles	**Artículo 19. II. b) Evitar la instalación de cualquier elemento de software que implique algún riesgo para el tratamiento de datos personales.**
			A) Dependiendo del sistema operativo, configurar las actualizaciones solamente para versiones maduras o revisiones certificadas de las aplicaciones. *Por ejemplo*: en sistemas Linux desactivar la instalación de versiones *beta, test, debug, non-official.*
			B) De la lista de software instalado, verificar el consumo de recursos de aplicaciones *TSR (Terminal and StayResident)*. Identificar demonios que ocupen excesiva RAM o tiempo de ejecución en el procesador. *Por ejemplo*: En sistemas Windows usar el Administrador de Tareas para identificar programas de alto consumo.
			C) Desinstalar toda aquella aplicación, librería, programa, paquetería o servicio que no sea estrictamente necesario para la operación del sistema. *Por ejemplo*, si el servidor Linux no

			proporcionará direcciones IP, el demonio o servicio *dchpd* no debe estar instalado.
			D) Llenar formato 10 y colocar nombre y firma de quien realizó la acción.
11	1	Dos días hábiles	**Artículo 19. III. a) Establecer las medidas físicas de seguridad que controlen el acceso a los equipos.**
			A) Identificar las medidas físicas que restrinjan el acceso físico a equipos, tales como chapas, puertas, biométricos.
			B) En función de la ubicación del equipo de cómputo, hacer una relación de las condiciones más adecuadas para su protección que aún sean necesarias implementar.
			C) Establecer y seguir un plan de mejoramiento de la protección física de equipos. *Por ejemplo*; cámaras de video vigilancia, bitácoras, vigilantes, cuartos cerrados, racks con puerta y chapa, candados en equipos, bloqueo o desconexión física de puertos USB, alarmas y sensores, según sea lo más conveniente como mínimo para la protección de los datos.
			D) Llenar formato 11 y colocar nombre y firma de quien realizó la acción.
12	1	Un día hábil	**Artículo 19. III. b) Restringir la salida de equipos de las instalaciones de cada área universitaria.**
			A) Diseñar una bitácora o formato para el registro de entrada y salida de equipos de cómputo y periféricos asociados como discos duros, cintas, unidades flash, discos ópticos, monitores, teclados, ratones y en lo general todo componente de un equipo.
			B) La bitácora de entrada y salida debe incluir el registro de número de serie e inventario UNAM. responsable de ingreso o egreso del componente y firma autorizada del responsable del área.
			C) Incluir en el procedimiento la revisión periódica (al menos una vez al mes) de la consistencia del inventario registrado contra la bitácora de entrada y salida.
			D) Llenar 12 y colocar nombre y firma de quien realizó la acción.
13	1	Tres días hábiles	**Artículo 19. IV. a) Realizar la transmisión de datos personales a través de un canal cifrado.**
			A) Identificar, mediante el administrador de aplicaciones que corresponda al sistema operativo, los protocolos y aplicaciones instalados para comunicación cifrada. *Por ejemplo*: *SFTP (Secure File Transfer Protocol), SSH (Secure Shell), SCP (SecureCopy*).
			B) Instalar con el administrador de aplicaciones o comando similar los protocolos de comunicación cifrada que sean necesarios para el tipo de transacciones y accesos del sistema. *Por ejemplo*, en el caso de requerir ejecutar comandos de forma remota en un servidor Linux, instalarlo con el comando *apt-getinstallopenssh-server.*
			C) Activar los protocolos de comunicación encriptada en el servidor. *Por ejemplo*: en Linux con el comando *sudo systemctlenablessh*.
			D) Llenar formato 13 y colocar nombre y firma de quien realizó la acción.

14	1	Tres días hábiles	**Artículo 20.Aplicar el procedimiento de borrado seguro que impida la recuperación en las bases de datos y todos sus respaldos.**
			A) Realizar una copia integral del sistema de información y colocarla en un servicio temporal. *Por ejemplo:* máquina virtual o directorio temporal en el servidor.
			B) Ingresar a la copia del sistema de información y realizar el borrado de un registro. Verificar que el dato no persiste en la base de datos por medio de forma de consulta o comando.
			C) Realizar el mismo proceso del punto B para una tabla y finalmente para la base de datos completa.
			D) En caso de persistencia del dato, instalar y ejecutar herramientas para borrado seguro. *Por ejemplo*: en Linux se dispone *de shred, wipe, secure-delete, srm, sfill, sswap, sdmem,* que se pueden instalar desde el administrador de aplicaciones.
			D) Llenar formato 14 y colocar nombre y firma de quien realizó la acción.
ETAPA 2			
15	2	Hito	**Artículo 18. I. a) Utilizar los datos personales preexistentes que estén disponibles, de acuerdo con sus respectivas políticas de uso y acceso, en bases de datos a cargo de otras áreas universitarias.**
			A) Disponer del inventario de datos del sistema de información, esto es: documento con la descripción de tablas, campos, tipo de datos, relaciones y consultas.
			B) Con el Área Universitaria que esté identificada como la instancia autoritativa en materia de datos personales, comparar el inventario de datos. *Por ejemplo*: La Dirección General de Administración Escolar es la dependencia autoritativa en materia de datos personales de estudiantes.
			C) Establecer el acuerdo por escrito para el uso de campos específicos de datos personales de la instancia autoritativa.
			D) Establecer el mecanismo de comunicación entre el sistema de información y el de la instancia autoritativa. *Por ejemplo*: *Webservices*, transferencia *SFTP.*
			E) Llenar 15 y colocar nombre y firma de quien realizó la acción.
16	2	Ocho días hábiles	**Artículo 18. I. d) Permitir el acceso al código fuente de los sistemas exclusivamente a la administración del sistema y personal para el desarrollo.**
			A) Recopilar el código fuente y documentación del sistema de información en todas sus versiones disponibles.
			B) Depositar en un equipo central de desarrollo todas las versiones de código fuente y su documentación (inventario de datos, manual de administración, manual de programador).
			C) Establecer control de acceso por usuario y contraseña hacia el equipo central de desarrollo.
			D) Activar bitácoras de acceso (*log*) hacia el equipo central de desarrollo.
			E) Proporcionar las credenciales de acceso al equipo central de desarrollo exclusivamente al personal a cargo de programación y mantenimiento de código y manuales.
			F) Llenar formato 16 y colocar nombre y firma de quien realizó la acción.

17	2	Cuatro días hábiles	**Artículo 19. I. b) Establecer las medidas de seguridad en los periodos de inactividad o mantenimiento.**
			A) Elaborar documento con las medidas necesarias de seguridad para períodos vacacionales, contingencias y ventanas de mantenimiento, incluyendo: control de acceso físico y lógico a los equipos, ejecución de respaldos, sistemas de alta disponibilidad (redundancia).
			B) Incluir en el documento la descripción de los procedimientos en caso de contingencia por falla de servicio de red, falla de equipo de cómputo, falla lógica en sistema operativo.
			C) Incluir en el documento el directorio de responsables de cada uno de los puntos a atender: apagado seguro, apagado fortuito, apagado programado, verificación de integridad de información, activación de servicios locales o de respaldo.
			D) Llenar formato 17 y colocar nombre y firma de quien realizó la acción.
18	2	Ocho días hábiles	**Artículo 19. I. c) Generar respaldos y aplicar los mecanismos de control y protección para su resguardo.**
			A) De acuerdo con el plan de respaldos establecido, ejecutar la secuencia de respaldos.
			B) Designar responsables de respaldos y responsables de verificación de respaldos.
			C) Completar bitácora de control de los respaldos, indicando fecha, hora, tipo de respaldo (integral, total, parcial de registros), ejecutor y revisor del respaldo, ubicación del respaldo, medio y etiqueta.
			D) Llenar formato 18 y colocar nombre y firma de quien realizó la acción.
19	2	Veinte días hábiles	**Artículo 19. I. d) Impedir el uso de cuentas y servicios gestionados por personas físicas para el tratamiento de los datos personales.**
			A) Realizar revisión integral del sistema de información en materia de accesos, cuentas y servicios. *Por ejemplo*: En caso de consultar vía un *Webservice* a un sistema autoritativo de datos personales en la DGAE, identificar la cuenta de acceso a ese sistema.
			B) Determinar si las cuentas de acceso a servicios locales o remotos están bajo el control de la administración del sistema. *Por ejemplo*: Si la cuenta de acceso a un *Webservice* – su usuario y contraseña – está bajo el control del administrador del sistema, o si un respaldo que se realiza en un equipo remoto es con una cuenta y contraseña controlada por el administrador del sistema.
			C) Si las cuentas de acceso a servicios locales o remotos pertenecen a personas del Área Universitaria, cambiarlas por cuentas institucionales dentro del control de la instancia universitaria. *Por ejemplo*: si la identificación para acceder a un respaldo remoto es del tipo xxx@google.com, deberá cambiarse por una cuenta del tipo xxxx@unam.mx.
			D) Llenar formato 19 y colocar nombre y firma de quien realizó la acción.

20	2	Cuatro días hábiles	**Artículo 19. II. a) Proteger ante manipulaciones indebidas y accesos no autorizados las bitácoras y los dispositivos donde se almacenan.**
			A) Elaborar una lista de las bitácoras relacionadas con el sistema de información, tanto en medio digital como físico. *Por ejemplo*: En el equipo de cómputo las bitácoras de acceso de usuarios al sistema operativo y al sistema de información (*logs*), de forma física las bitácoras de acceso al área donde está el equipo de cómputo.
			B) Junto a la lista elaborar el cronograma de revisión de integridad y respaldo de las bitácoras. *Por ejemplo*: diario, semanal, mensual.
			C) Establecer en el documento el procedimiento de resguardo de las bitácoras. *Por ejemplo*: respaldo y protección de *logs* en el caso de equipo de cómputo o zonas seguras de almacenamiento de bitácoras en papel, digitalización de registros.
			D) Llenar formato 20 y colocar nombre y firma de quien realizó la acción.
21	2	Cuatro días hábiles	**Artículo 19. IV. b) Supervisar los controles de seguridad en la red de datos donde opere el sistema para tratamiento de datos personales.**
			A) Identificar los equipos activos de red que permiten la conexión del equipo de cómputo con el sistema de información, incluyendo marca, modelo, versión de software, vigencia de mantenimiento y capacidades de protección de las comunicaciones.
			B) Determinar las reglas de seguridad físicas (acceso restringido, cuartos de telecomunicaciones) y lógicas (cuentas de acceso, puertos activos, protocolos activos) para el equipo de red.
			C) Incluir en las acciones para aseguramiento de la red de datos aquellas que sean necesarias en función de los controles actuales. Definir un plan de regularización de la seguridad en caso de ser aplicable.
			D) Mantener actualizados los equipos activos de red y con un programa de mantenimiento.
			E) Identificar y en su caso programar la instalación de equipo para seguridad perimetral de la red de datos.
			D) Llenar formato 21 y colocar nombre y firma de quien realizó la acción.
22	2	Cuatro días hábiles	**Artículo 19. IV. c) Proporcionar el acceso exclusivamente desde redes y servicios autorizados.**
			A) Revisar los puertos de comunicación (*TCP y UDP*) que requiera el sistema de información para su operación. *Por ejemplo*: para servicios *Web* los puertos 80 y 8080 son los convencionales.
			B) Activar en el sistema operativo la herramienta correspondiente para el control de puertos de comunicación. *Por ejemplo*, en Linux puede tratarse de un *firewall* a nivel de software o las herramientas que para tal efecto contenga la distribución correspondiente del sistema operativo.
			C) Dejar activos solamente los puertos necesarios para la operación del sistema.
			D) Activar el filtrado de la comunicación por direccionamiento IP en caso de ser posible para la operación del sistema. *Por ejemplo*: Permitir el acceso al puerto de *SSH* solamente a

			direcciones IP en una subred de la UNAM (132.248.x.y) o a un grupo de direcciones IP específicas.
			E) Llenar formato 22 y colocar nombre y firma de quien realizó la acción.
ETAPA 3			
23	3	Veinte días hábiles	**Artículo 18. I. b) Contar con entornos para desarrollo, pruebas y operación.**
			A) Instalar y configurar equipos similares en características, preferentemente virtuales, a los equipos donde se instalará el sistema de información en su nueva o actualizada versión.
			B) Crear un repositorio en un equipo central de desarrollo para el resguardo de códigos, documentación, inventarios de datos y manuales de usuario, administrador y programador.
			C) Ejecutar las pruebas de nuevas versiones o actualizaciones del sistema de información en el equipo dispuesto para tal efecto. Nunca usar -equipos físicos o virtuales con el sistema actualmente en producción como las plataformas para evaluación de versiones en desarrollo.
			D) Llenar formato 23 y colocar nombre y firma de quien realizó la acción.
24	3	Veinte días hábiles	**Artículo 18. I. f) Cumplir con las especificaciones de seguridad informática previo a la puesta en operación.**
			A) Una vez concluido el desarrollo o actualización de un sistema de información, solicitar al área de seguridad del Área Universitaria la revisión de seguridad informática del sistema, lo que incluye: pruebas de penetración, pruebas de estabilidad, pruebas de carga y endurecimiento de la seguridad. En caso de no contar con esa área, requerirlo a UNAM CERT al correo seguridad.tic@unam.mx .
			B) Una vez recibido el reporte del área de seguridad, aplicar las medidas de corrección que incluya el reporte. Regresar al punto A.
			C) Habiendo resuelto los hallazgos y sugerencias de mejora de la seguridad señalados por el área especializada, realizar la instalación del sistema en la plataforma definitiva de cómputo, extrayéndolo del entorno de desarrollo.
			D) Llenar formato 24 y colocar nombre y firma de quien realizó la acción.
25	3	Hito	**Artículo 18. III. a) Utilizar equipos con componentes actualizados, protegidos con garantías y soporte, y con la capacidad suficiente para atender la demanda del servicio y de los usuarios.**
			A) Elaborar una lista del inventario de los equipos de cómputo, periféricos y de almacenamiento necesarios para la ejecución del sistema de información.
			B) Determinar la razón por la que el sistema de información requerirá estar localizado en un equipo físico y no en un servidor virtual. Con ello justificar una adquisición o actualización. Por ejemplo: por incompatibilidad con hipervisores, necesidades de comunicación exclusivamente locales en la entidad y dependencia o el no necesitar de un entorno de alta disponibilidad automática.

			C) Identificar en el inventario versiones, introducción en el mercado, vida útil, contratos de mantenimiento y soporte para todos y cada uno de los componentes, en el caso de emplear equipo físico.
			D) Adquirir los componentes y elementos necesarios para la actualización, vigencia de soporte y capacidad para atención a los usuarios en el equipo de cómputo físico.
			E) Llenar formato 25 y colocar nombre y firma de quien realizó la acción.
26	3	Hito	**Artículo 18. III. b) Definir el programa de mantenimiento preventivo.**
			A) De la lista de equipo de cómputo físico necesario para la operación del sistema de información, extraer las vigencias de mantenimiento.
			B) En caso de no estar en posibilidad de aplicar el mantenimiento preventivo por el personal del Área Universitaria, cotizar pólizas de mantenimiento de acuerdo con el tipo de componente, preferentemente una sola póliza para el conjunto del equipo físico.
			C) Adquirir las pólizas de mantenimiento preventivo y observar su vigencia. La vigencia no podrá ser menor de un año.
			D) Llenar formato 26 y colocar nombre y firma de quien realizó la acción.
27	3	Seis días hábiles	**Artículo 19. III. c) Aplicar el programa de mantenimiento preventivo a los equipos.**
			A) En caso de que el personal del Área Universitaria pueda realizar el mantenimiento preventivo, definir el calendario de inactividad del sistema de información, notificar a los usuarios y aplicar el plan en caso de mantenimiento o inactividad.
			B) En caso de que sea a través de un proveedor que se proporcione el mantenimiento al equipo de cómputo, ejecutar el calendario de acciones preventivas en un período no superior a cada 3 meses hasta la conclusión del contrato o póliza respectivo.
			C) Llenar formato 27 y colocar nombre y firma de quien realizó la acción.
28	3	Hito	**Artículo 21.Solo se permitirá el uso de servicios de nube pública para el resguardo de archivos cifrados que contengan respaldos de la información.**
			A) Identificar los respaldos que se tengan resguardados en servicios de nube pública.
			B) Verificar el cifrado en cada uno de los respaldos que se almacenen en nube pública. El cifrado no deberá ser de menor capacidad al equivalente a AES de 128 bits.
			C) Llenar formato 28 y colocar nombre y firma de quien realizó la acción.

ANEXO V. FORMATOS PARA CUMPLIMIENTO DE LAS MST

(Nombre del sistema A1)			Identificador único A1	
Formato	**1**	**Verificación anual**	**Acción concluida**	( )
Medida de seguridad técnica:		**Artículo 18. I. c) Utilizar datos no personales durante el desarrollo y pruebas de los sistemas.**		
Aplicable en:		I. Bases de datos y sistemas de tratamiento.		
Tiempo estimado:		Un día hábil.		
Importancia de la acción:		Evitar usar datos personales mientras se está desarrollando, actualizando o modificando el código fuente de un sistema de información.		
Proceso recomendado:		**A)** Realizar respaldo completo de la base de datos. **B)** Ejecutar consulta en el sistema de información, por medio de formato o comandos. **C)** Verificar que los datos usados en el desarrollo no correspondan a personas identificables. **D)** Si se usan datos de personas identificables, cambiar por datos genéricos o datos ficticios y regresar al punto B. **E)** Si no se usan datos de personas identificables, llenar formato con nombre y firma de quien realizó la acción, fecha de inicio y de conclusión.		
Mejores prácticas, referencias:		**1.-** Se recomienda al desarrollar un sistema de información no usar datos personales sino ficticios. **2.-** Se sugiere incluir en la documentación del desarrollo de un sistema de información el inventario de datos y el tipo de información de prueba.		
Conocimientos requeridos:		Administración de bases de datos. Consulta y actualización de tablas.		
Ejecución			**Fecha inicio**	
Nombre y firma			**Fecha término**	
Programador, desarrollador o diseñador del sistema de información				
Observaciones / anotaciones				

(Nombre del sistema A1)			Identificador único A1	
Formato:	**2**	**Verificación anual**	**Acción concluida**	( )
Medidas de seguridad técnicas:		**Artículo 18. I. e) Asignar o revocar los privilegios de acceso para los usuarios teniendo como base el principio del menor privilegio.**		
Aplicable en:		I. Bases de datos y sistemas de tratamiento.		
Tiempo estimado:		Un día hábil.		
Importancia de la acción:		No se deben asignar privilegios de acceso a los usuarios en niveles que no estén relacionados con su responsabilidad en el tratamiento de datos.		
Proceso recomendado:		**A)** Realizar respaldo completo de la base de datos. **B)** Ejecutar consulta en el sistema de información de la lista de usuarios y sus niveles o privilegios de acceso. **C)** Validar que los niveles de acceso son acordes a la relación del usuario con el tratamiento de datos personales. **D)** Si hay usuarios con privilegios mayores a los que les son necesarios, cambiar al mínimo indispensable e informarlo al usuario. Regresar al punto B. **E)** Si los privilegios de acceso son correctos para los usuarios, llenar formato con nombre y firma de quien realizó la acción, fecha de inicio y de conclusión.		
Mejores prácticas, referencias:		**1.-** Definir niveles de acceso adecuados para cada perfil o tipo de usuario. **2.-** Tener un mínimo de administradores o usuarios con altos privilegios en el sistema.		
Conocimientos requeridos:		Administración de bases de datos. Consulta y actualización de usuarios.		
Ejecución			**Fecha inicio**	
Nombre y firma Administrador del sistema de información			**Fecha término**	
Observaciones / anotaciones				

(Nombre del sistema A1)			Identificador único A1	
Formato:	**3**	**Verificación anual**	**Acción concluida**	( )
Medidas de seguridad técnicas:		**Artículo 18. I. g) Instalar y mantener vigentes certificados de comunicación segura SSL en el caso de servicios basados en Web.**		
Aplicable en:		I. Bases de datos y sistemas de tratamiento.		
Tiempo estimado:		Tres días hábiles.		
Importancia de la acción:		El instalar un certificado SSL en servidores web incrementa la seguridad al encriptar la transferencia de datos y la unicidad del sitio para los usuarios.		
Proceso recomendado:		A) En caso de no tener un certificado SSL vigente, enviar correo electrónico al Departamento de Firma Electrónica de DGTIC a firma.tic@unam.mx solicitando la asignación. **B)** El Departamento de Firma Electrónica Avanzada envía procedimiento para obtención de CSR del servidor, formato de la solicitud y costos de recuperación en función del tipo de certificado requerido (organizacional, comodín o corporativo). C) Completar documentación, proceso y pago de costo de recuperación. Enviar comprobantes a firma.tic@unam.mx. **D)** Al recibir el certificado SSL, instalarlo en el servidor de acuerdo con las instrucciones recibidas junto con el certificado.		
Mejores prácticas, referencias:		**1.-** Los certificados SSL deben tener una vigencia de al menos un año. **2.-** En caso de tener varios sistemas de información bajo un mismo dominio, se recomienda obtener un certificado SSL del tipo comodín (*wildcard*). **3.-** Se debe realizar el proceso de renovación del certificado al menos 10 días hábiles antes de su vencimiento.		
Conocimientos requeridos:		Administración de sistema operativo. Administración de servicios Web.		
Ejecución			**Fecha inicio**	
Nombre y firma			**Fecha término**	
Administrador del sistema de información o servidor				
Observaciones / anotaciones				

(Nombre del sistema A1)			Identificador único A1	
Formato:	**4**	**Verificación anual**	**Acción concluida**	( )
Medidas de seguridad técnicas:	**Artículo 18. I. h) Definir el plan de respaldos de la información, incluyendo periodicidad y alcance.**			
Aplicable en:	I. Bases de datos y sistemas de tratamiento.			
Tiempo estimado:	Dos días hábiles.			
Importancia de la acción:	En todo sistema de información es indispensable contar con un plan de respaldos periódicos, y especialmente en aquellos que contienen datos personales.			
Proceso recomendado:	**A)** Elaborar documento con la secuencia de respaldos al menos con el siguiente orden: - Diario – incremental. - Semanal – incremental. - Mensual – total. **B)** Establecer en el plan los medios para resguardo del respaldo y su forma de identificación: - En línea: mismo equipo donde se ejecuta el sistema. - Respaldo como servicio: otro equipo de almacenamiento. - Fuera de línea: medios magnéticos (cintas, discos) y/u ópticos. **C)** Incluir en el plan: - Responsables de cada tipo y medio de respaldo. - Rotación de respaldos y medios. - Áreas de resguardo. - Métodos de cifrado. - RTO: *Recovery Time Objective*. Tiempo objetivo de recuperación. - RPO: *Recovery Point Objective*: Punto objetivo de recuperación. **D)** Concluir este documento, adjuntarlo a SGPDP, llenar y firmar formato.			
Mejores prácticas, referencias:	**1.-** Se deben tener al menos 3 respaldos del sistema y sus bases de datos en distintos medios.			
Conocimientos requeridos:	Administración de sistema operativo. Gestión y programación de respaldos.			
Ejecución			**Fecha inicio**	
Nombre y firma			**Fecha término**	
Administrador del sistema de información o servidor				
Observaciones / anotaciones				

(Nombre del sistema A1)			Identificador único A1	
Formato:	**5**	**Verificación anual**	**Acción concluida**	( )
Medidas de seguridad técnicas:		**Artículo 18. I. i) Definir el procedimiento para el borrado seguro.**		
Aplicable en:		I. Bases de datos y sistemas de tratamiento.		
Tiempo estimado:		Un día hábil.		
Importancia de la acción:		Al igual que el procedimiento de respaldo, el borrado seguro de la información debe estar definido en cualquier sistema de información.		
Proceso recomendado:		**A)** Elaborar documento con el procedimiento y la herramienta para borrado seguro en función del tipo de base de datos para registros, tablas y base de datos. **B)** Incluir en el documento de borrado seguro el proceso de verificación de la no existencia del dato, generalmente por medio de consultas y de copias de respaldo. **C)** El borrado seguro debe incluirse en los respaldos incrementales y totales y en cualquiera de los medios de respaldo, así como máquinas virtuales o contenedores. **D)** Concluir este documento, adjuntarlo a SGPDP, llenar y firmar formato.		
Mejores prácticas, referencias:		**1.-** Para el caso de baja de equipo, se debe llenar el formato con la declaración de borrado seguro del Patronato Universitario, disponible en: http://www.patrimonio.unam.mx/patrimonio/descargas/formato_responsiva_borrado_datos.pdf **2.-** Se recomienda utilizar herramientas de borrado seguro por medio de sobre escritura aleatoria, llenado de ceros (0x00), llenado de unos o protocolos de borrado del estándar *DOD-5220.22-M*.		
Conocimientos requeridos:		Administración de sistema operativo. Comandos de borrado.		
Ejecución			**Fecha inicio**	
Nombre y firma			**Fecha término**	
Administrador del sistema de información o servidor				
Observaciones / anotaciones				

(Nombre del sistema A1)			Identificador único A1	
Formato:	**6**	**Verificación anual**	**Acción concluida**	( )
Medidas de seguridad técnicas:		**Artículo 18. II. a) Sincronizar la fecha y hora con el servidor NTP (Network Time Protocol) oficial de la UNAM**		
Aplicable en:		II. Sistemas operativos y servicios.		
Tiempo estimado:		Un día hábil.		
Importancia de la acción:		A fin de poseer información consistente, los sistemas de información deben estar sincronizados con una instancia central de tiempo, en este caso el servidor NTP de la UNAM.		
Proceso recomendado:		**A)** Realizar la verificación y configuración con privilegio de administrador del sistema operativo. **B)** En función del sistema operativo, acceder a la configuración de servidor de tiempo (NTP) en interfaz gráfica o por medio de línea de comandos. *Por ejemplo*, en el caso del sistema operativo Linux: - Verificar la existencia del archivo */etc/ntp.conf* - Editar el archivo *ntp.conf* incluyendo en la primera línea: *server ntpdgtic.redunam.unam.mx* ***ó*** *server 132.247.169.17* - Reiniciar el demonio del cliente NTP con el comando *sudo servicentpreload.* **C)** En caso de no tener el cliente NTP instalado, descargarlo del repositorio de aplicaciones del sistema operativo, instalarlo y regresar al punto B. **D)** Llenar y firmar formato.		
Mejores prácticas, referencias:		**1.-** Los servidores virtuales y contenedores hospedados en el Centro de Datos en DGTIC son configurados de origen con sincronización al servidor NTP de la UNAM. **2.-** No se deben usar otros servidores de NTP distintos al de UNAM.		
Conocimientos requeridos:		Administración de sistema operativo.		

Ejecución	Fecha inicio
Nombre y firma Administrador del sistema de información o servidor	**Fecha término**

Observaciones / anotaciones	

(Nombre del sistema A1)			Identificador único A1	
Formato:	**7**	**Verificación anual**	**Acción concluida**	( )
Medidas de seguridad técnicas:		**Artículo 18. II. b) Instalar y mantener actualizado el software antimalware.**		
Aplicable en:		II. Sistemas operativos y servicios.		
Tiempo estimado:		Dos días hábiles.		
Importancia de la acción:		El servidor que hospede el sistema de información debe tener protecciones instaladas para mitigar la inserción de *malware* (*rootkits, backdoors o* códigos maliciosos) que pueda alterar su operación o la integridad y seguridad de los datos.		
Proceso recomendado:		**A)** En función del sistema operativo, instalar uno o varios programas para la contención de malware. *Por ejemplo*, para el caso del sistema operativo Linux existen herramientas de código abierto y uso libre como *chkrootkit, rootkit hunter, bothunter, clamAV, avast*, entre otros, que se pueden instalar desde el repositorio correspondiente a la distribución de Linux en uso. **B)** Disponer de comandos para la localización de amenazas. *Por ejemplo*, para el caso de Linux, se recomienda usar el comando *grep* para la detección de cadenas regulares de texto en las invocaciones al *shell*. **C)** Una vez instalada la solución, verificar periódicamente su actualización **D)** Llenar y firmar formato.		
Mejores prácticas, referencias:		**1.-** UNAM-CERT puede asesorar en la selección de las herramientas *anti malware* más adecuadas para el servidor donde se aloje el sistema de información. Contactar al correo seguridad.tic@unam.mx.		
Conocimientos requeridos:		Administración de sistema operativo. Instalación de aplicaciones.		
Ejecución			**Fecha inicio**	
Nombre y firma			**Fecha término**	
Administrador del sistema de información o servidor				
Observaciones / anotaciones				

(Nombre del sistema A1)			Identificador único A1	
Formato:	**8**	**Verificación anual**	**Acción concluida**	( )
Medidas de seguridad técnicas:		**Artículo 18. II. c) Instalar las actualizaciones de seguridad más recientes disponibles.**		
Aplicable en:		II. Sistemas operativos y servicios.		
Tiempo estimado:		Cuatro días hábiles.		
Importancia de la acción:		El servidor que hospede el sistema de información debe tener vigentes todas las actualizaciones de seguridad proporcionadas por el fabricante o desarrollador del sistema operativo.		
Proceso recomendado:		**A)** En función del sistema operativo, se debe revisar la vigencia y actualización de las herramientas de seguridad de la información. *Por ejemplo*, en el sistema operativo Linux ejecutar *apt-getupdate* para obtener la lista de actualizaciones, especialmente en el repositorio *security*de la respectiva distribución. **B)** Realizar un respaldo del sistema para garantizar retorno a versión anterior en caso de incompatibilidad con alguna aplicación de las actualizaciones de seguridad. **C)** Instalar las actualizaciones en el sistema operativo. **D)** Llenar y firmar formato.		
Mejores prácticas, referencias:		**1.-** Debe verificarse la actualización de seguridad del sistema operativo al menos una vez a la semana y configurar la actualización o notificación inmediata en caso de complementos de seguridad urgentes.		
Conocimientos requeridos:		Administración de sistema operativo. Instalación de aplicaciones.		
Ejecución			**Fecha inicio**	
Nombre y firma			**Fecha término**	
Administrador del sistema de información o servidor				
Observaciones / anotaciones				

(Nombre del sistema A1)			Identificador único A1	
Formato:	**9**	**Verificación anual**	**Acción concluida**	( )
Medidas de seguridad técnicas:		**Artículo 19. I. a) Aplicar un mecanismo de autenticación para las personas autorizadas con base en el principio del menor privilegio.**		
Aplicable en:		I. Bases de datos y sistemas de tratamiento.		
Tiempo estimado:		Cuatro días hábiles.		
Importancia de la acción:		Partiendo de la asignación o niveles de acceso a la información con el principio del menor privilegio, debe haber en operación en el sistema al menos un mecanismo para la validación de los usuarios autorizados.		
Proceso recomendado:		**A)** Verificar el tipo de control de acceso al sistema, esto es: a través de contraseñas, claves, identificadores, nombres de usuario, nombres de dominio, entre otros. Según sea aplicable al sistema de información en lo particular. En caso de no tener un control de acceso establecer al menos uno como: usuarios de sistema operativo, cuenta y contraseña de sistema. **B)** Revisar que los privilegios de acceso sean los adecuados en función del rol del usuario. *Por ejemplo:* el usuario de conexión a la base de datos no debe estar asignado a alguna cuenta del personal que tiene acceso al sistema. **D)** Llenar y firmar formato.		
Mejores prácticas, referencias:		**1.-** Se recomienda usar un esquema estándar de acceso a sistemas que están vinculados, por ejemplo: por medio de Directorio Activo (*Active Directory*), *LDAP* u *OpenAIM.* **2.-** Las contraseñas deben ser de 12 caracteres o más con uso de signos, letras mayúsculas y minúsculas y números.		
Conocimientos requeridos:		Administración de bases de datos. Consulta y actualización de usuarios.		
Ejecución			**Fecha inicio**	
Nombre y firma			**Fecha término**	
Administrador del sistema de información o servidor				
Observaciones / anotaciones				

(Nombre del sistema A1)			Identificador único A1	
Formato:	**10**	**Verificación anual**	**Acción concluida**	( )
Medida de seguridad técnica:		**Artículo 19. II. b) Evitar la instalación de cualquier elemento de software que implique algún riesgo para el tratamiento de datos personales.**		
Aplicable en:		II. Sistemas operativos.		
Tiempo estimado:		Dos días hábiles.		
Importancia de la acción:		Por la relevancia de los sistemas de información con datos personales se debe minimizar o erradicar el riesgo de seguridad que implica instalar aplicaciones no verificadas.		
Proceso recomendado:		**A)** Dependiendo del sistema operativo, configurar las actualizaciones solamente para versiones maduras o revisiones certificadas de las aplicaciones. *Por ejemplo*: en sistemas Linux desactivar la instalación de versiones *beta, test, debug, non-official.* **B)** De la lista de software instalado, verificar el consumo de recursos de aplicaciones *TSR (Terminal and StayResident)*. Identificar demonios que ocupen excesiva RAM o tiempo de ejecución en el procesador. *Por ejemplo*: En sistemas Windows usar el Administrador de Tareas para identificar programas de alto consumo. **C)** Desinstalar toda aquella aplicación, librería, programa, paquetería o servicio que no sea estrictamente necesario para la operación del sistema. *Por ejemplo*, si el servidor Linux no proporcionará direcciones IP, el demonio o servicio *dchpd* no debe estar instalado. **D)** Llenar y firmar formato.		
Mejores prácticas, referencias:		**1.-** En ningún caso puede instalarse software de procedencia desconocida. Se debe impedir a los usuarios en sus privilegios de acceso instalar software o inyectar código a la aplicación del sistema de información. y se debe realizar un control estricto de los puertos de comunicación (USB, Red, etc) para evitar la extracción no autorizada de datos.		
Conocimientos requeridos:		Administración de sistema operativo. Instalación de aplicaciones.		
Ejecución			**Fecha inicio**	
Nombre y firma			**Fecha término**	
Administrador del sistema de información o servidor				
Observaciones / anotaciones				

(Nombre del sistema A1)			Identificador único A1	
Formato:	**11**	**Verificación anual**	**Acción concluida**	( )
Medidas de seguridad técnicas:		**Artículo 19. III. a) Establecer las medidas físicas de seguridad que controlen el acceso a los equipos.**		
Aplicable en:		III. Equipo de cómputo.		
Tiempo estimado:		Dos días hábiles.		
Importancia de la acción:		Además de las protecciones de tipo lógico, deben implementarse medidas de seguridad para reducir el riesgo al sistema de información por accesos físicos no autorizados.		
Proceso recomendado:		**A)** Identificar las medidas físicas que restrinjan el acceso físico a equipos, tales como chapas, puertas, biométricos. **B)** En función de la ubicación del equipo de cómputo, hacer una relación de las condiciones más adecuadas para su protección que aún sean necesarias implementar. **C)** Establecer y seguir un plan de mejoramiento de la protección física de equipos. *Por ejemplo*: cámaras de video vigilancia, bitácoras, vigilantes, cuartos cerrados, racks con puerta y chapa, candados en equipos, bloqueo o desconexión física de puertos USB, alarmas y sensores, según sea lo más conveniente como mínimo para la protección de los datos. **D)** Llenar y firmar formato.		
Mejores prácticas, referencias:		**1.-** Las medidas físicas de seguridad deben revisarse regularmente y formar parte de plan de continuidad de operaciones, así como ser del conocimiento de la Comisión local de seguridad.		
Conocimientos requeridos:		Administración de bases de datos. Consulta y actualización de usuarios.		
Ejecución			**Fecha inicio**	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término**	
Observaciones / anotaciones				

(Nombre del sistema A1)			Identificador único A1	
Formato:	**12**	**Verificación anual**	**Acción concluida**	( )
Medidas de seguridad técnicas:		**Artículo 19. III. b) Restringir la salida de equipos de las instalaciones de cada área universitaria.**		
Aplicable en:		III. Equipo de cómputo.		
Tiempo estimado:		Un día hábil.		
Importancia de la acción:		Se debe tener un mecanismo de control para la entrada y salida de equipos de cómputo y eliminar extracciones no autorizadas.		
Proceso recomendado:		**A)** Diseñar una bitácora o formato para el registro de entrada y salida de equipos de cómputo y periféricos asociados como discos duros, cintas, unidades *flash*, discos ópticos, monitores, teclados, ratones y en lo general todo componente de un equipo. **B)** La bitácora de entrada y salida debe incluir el registro de número de serie e inventario UNAM. Responsable de ingreso o egreso del componente y firma autorizada del responsable del área. **C)** Incluir en el procedimiento la revisión periódica (al menos una vez al mes) de la consistencia del inventario registrado contra la bitácora de entrada y salida. **D)** Llenar y firmar formato.		
Mejores prácticas, referencias:		**1.-** Se recomienda usar un formato estándar de control de entrada y salida de bienes proporcionados por las áreas administrativas de las entidades y dependencias y conservar una copia en el área responsable del equipo de cómputo. **2.-** En la bitácora se debe incluir la razón de la entrada o salida del equipo. En el caso de baja, se deberá firmar la declaración de borrado seguro de Patrimonio Universitario.		
Conocimientos requeridos:		Gestión de Tecnología de información, control de entrada y salida de equipo y materiales.		
Ejecución			**Fecha inicio**	
Nombre y firma			**Fecha término**	
Administrador del sistema de información o servidor				
Observaciones / anotaciones				

(Nombre del sistema A1)			Identificador único A1	
Formato:	**13**	**Verificación anual**	**Acción concluida**	( )
Medidas de seguridad técnicas:		**Artículo 19. IV. a) Realizar la transmisión de datos personales a través de un canal cifrado.**		
Aplicable en:		IV. Red de datos.		
Tiempo estimado:		Tres días hábiles.		
Importancia de la acción:		La comunicación del sistema de información con otros sistemas o servicios, así como el acceso de administración para ejecución de procesos por comandos, debe estar encriptada para evitar el envío o recepción de datos susceptibles de ser interceptados en tránsito.		
Proceso recomendado:		**A)** Identificar, mediante el administrador de aplicaciones que corresponda al sistema operativo, los protocolos y aplicaciones instalados para comunicación cifrada. *Por ejemplo*: *SFTP (Secure File Transfer Protocol), SSH (Secure Shell), SCP (SecureCopy*). **B)** Instalar con el administrador de aplicaciones o comando similar los protocolos de comunicación cifrada que sean necesarios para el tipo de transacciones y accesos del sistema. *Por ejemplo*, en el caso de requerir ejecutar comandos de forma remota en un servidor Linux, instalarlo con el comando *apt-getinstallopenssh-server.* **C)** Activar los protocolos de comunicación encriptada en el servidor. *Por ejemplo*: en Linux con el comando *sudo systemctlenablessh*. **D)** Llenar y firmar formato.		
Mejores prácticas, referencias:		**1.-** Se deben mantener actualizados los protocolos de comunicación por canal cifrado al igual que las utilerías de seguridad. 2.- El protocolo de comunicación cifrada requiere puertos específicos TCP, los cuales deberán estar permitidos en la configuración del equipo activo de red.		
Conocimientos requeridos:		Administración de sistema operativo. Instalación de aplicaciones. Administración de red.		
Ejecución			**Fecha inicio**	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término**	
Observaciones / anotaciones				

(Nombre del sistema A1)			Identificador único A1	
Formato:	**14**	**Verificación anual**	**Acción concluida**	( )
Medidas de seguridad técnicas:		**Artículo 20.Aplicar el procedimiento de borrado seguro que impida la recuperación en las bases de datos y todos sus respaldos.**		
Aplicable en:		Bases de datos y sistemas de tratamiento.		
Tiempo estimado:		Tres días hábiles.		
Importancia de la acción:		Se debe verificar que el procedimiento de borrado seguro es funcional y que el dato no persiste en función del tipo de borrado (registro, tabla, base, sistema).		
Proceso recomendado:		**A)** Realizar una copia integral del sistema de información y colocarla en un servicio temporal. *Por ejemplo:* máquina virtual directorio temporal en el servidor. **B)** Ingresar a la copia del sistema de información y realizar el borrado de un registro. Verificar que el dato no persiste en la base de datos por medio de forma de consulta o comando. **C)** Realizar el mismo proceso del punto B para una tabla y finalmente para la base de datos completa. D) En caso de persistencia del dato, instalar y ejecutar herramientas para borrado seguro. *Por ejemplo*: en Linux se dispone *de shred, wipe, secure-delete, srm, sfill, sswap, sdmem,* que se pueden instalar desde el administrador de aplicaciones. **D)** Llenar y firmar este formato.		
Mejores prácticas, referencias:		**1.-** Se recomienda usar al menos un comando a nivel de sistema operativo para el borrado seguro de conformidad con el procedimiento establecido.		
Conocimientos requeridos:		Administración de sistema operativo. Instalación de aplicaciones. Gestión de archivos.		
Ejecución			**Fecha inicio**	
Nombre y firma			**Fecha término**	
Administrador del sistema de información o servidor				
Observaciones / anotaciones				

(Nombre del sistema A1)			Identificador único A1	
Formato:	**15**	**Verificación anual**	**Acción concluida**	( )
Medidas de seguridad técnicas		**Artículo 18. I. a) Utilizar los datos personales preexistentes que estén disponibles, de acuerdo con sus respectivas políticas de uso y acceso en bases de datos a cargo de otras áreas universitarias.**		
Aplicable en:		I. Bases de datos y sistemas de tratamiento.		
Tiempo estimado:		Hito.		
Importancia de la acción:		Optimizar y consolidar el uso y la protección de datos personales al hacer referencia a instancias universitarias que sean las principales responsables de su obtención, resguardo y protección.		
Proceso recomendado:		**A)** Disponer del inventario de datos del sistema de información, esto es: documento con la descripción de tablas, campos, tipo de datos, relaciones y consultas. **B)** Con la Área Universitaria que esté identificada como la instancia autoritativa en materia de datos personales, comparar el inventario de datos. *Por ejemplo*: La Dirección General de Administración Escolar es la dependencia autoritativa en materia de datos personales de estudiantes. **C)** Establecer el acuerdo por escrito para el uso de campos específicos de datos personales de la instancia autoritativa. **D)** Establecer el mecanismo de comunicación entre el sistema de información y el de la instancia autoritativa. *Por ejemplo*: *Webservices*, transferencia *SFTP.* **E)** Llenar y firmar formato.		
Mejores prácticas, referencias:		**1.-** El hacer referencia a instancias a cargo de la obtención de los datos personales y su protección se garantiza la homogeneidad de la información.		
Conocimientos requeridos:		Administración de sistema de información. Gestión de bases de datos.		
Ejecución			**Fecha inicio**	
Nombre y firma			**Fecha término**	
Administrador del sistema de información o servidor				
Observaciones / anotaciones				

(Nombre del sistema A1)			Identificador único A1	
Formato:	**16**	**Verificación anual**	**Acción concluida**	( )
Medidas de seguridad técnicas:		**Artículo 18. I. d) Permitir el acceso al código fuente de los sistemas exclusivamente a la administración del sistema y personal para el desarrollo.**		
Aplicable en:		I. Bases de datos y sistemas de tratamiento.		
Tiempo estimado:		Ocho días hábiles.		
Importancia de la acción:		Evitar el uso de códigos originales de los sistemas de información que posteriormente implique un riesgo a la seguridad de estos.		
Proceso recomendado:		**A)** Recopilar el código fuente y documentación del sistema de información en todas sus versiones disponibles. **B)** Depositar en un equipo central de desarrollo todas las versiones de código fuente y su documentación (inventario de datos, manual de administración, manual de programador). **C)** Establecer control de acceso por usuario y contraseña hacia el equipo central de desarrollo **D)** Activar bitácoras de acceso (*log*) hacia el equipo central de desarrollo. **E)** Proporcionar las credenciales de acceso al equipo central de desarrollo exclusivamente al personal a cargo de programación y mantenimiento de código y manuales. **F)** Llenar y firmar formato.		
Mejores prácticas, referencias:		**1.-** Se debe documentar todo el proceso de desarrollo y actualización de un sistema de información.		
Conocimientos requeridos:		Administración de sistema de información. Gestión de bases de datos.		
Ejecución			**Fecha inicio**	
Nombre y firma			**Fecha término**	
Administrador del sistema de información o servidor				
Observaciones / anotaciones				

(Nombre del sistema A1)			Identificador único A1	
Formato:	**17**	**Verificación anual**	**Acción concluida**	( )
Medidas de seguridad técnicas:		**Artículo 19. I. b) Establecer las medidas de seguridad en los periodos de inactividad o mantenimiento.**		
Aplicable en:		I. Bases de datos y sistemas de tratamiento.		
Tiempo estimado:		Cuatro días hábiles.		
Importancia de la acción:		Garantizar la continuidad de la operación y disponibilidad de los sistemas de información especialmente durante períodos vacacionales, contingencias o ciclos de mantenimiento.		
Proceso recomendado:		**A)** Elaborar documento con las medidas necesarias de seguridad para períodos vacacionales, contingencias y ventanas de mantenimiento, incluyendo: control de acceso físico y lógico a los equipos, ejecución de respaldos, sistemas de alta disponibilidad (redundancia). **B)** Incluir en el documento la descripción de los procedimientos en caso de contingencia por falla de servicio de red, falla de equipo de cómputo, falla lógica en sistema operativo. **C)** Incluir en el documento el directorio de responsables de cada uno de los puntos a atender: apagado seguro, apagado fortuito, apagado programado, verificación de integridad de información, activación de servicios locales o de respaldo. **D)** Llenar y firmar formato.		
Mejores prácticas, referencias:		**1.-** Las medidas de seguridad durante períodos de mantenimiento deben formar parte de un plan de continuidad de operaciones y de recuperación ante desastres (**DRP**).		
Conocimientos requeridos:		Administración de sistema de información. Administración de sistema operativo.		
Ejecución			**Fecha inicio**	
Nombre y firma			**Fecha término**	
Administrador del sistema de información o servidor				
Observaciones / anotaciones				

(Nombre del sistema A1)			Identificador único A1	
Formato:	**18**	**Verificación anual**	**Acción concluida**	( )
Medidas de seguridad técnica:		**Artículo 19. I. c) Generar respaldos y aplicar los mecanismos de control y protección para su resguardo.**		
Aplicable en:		I. Bases de datos y sistemas de tratamiento.		
Tiempo estimado:		Ocho días hábiles.		
Importancia de la acción:		Verificar que el plan de respaldos opera adecuadamente para su utilización en caso de contingencia.		
Proceso recomendado:		**A)** De acuerdo con el plan de respaldos establecido, ejecutar la secuencia de respaldos. **B)** Designar responsables de respaldos y responsables de verificación de respaldos. **C)** Completar bitácora de control de los respaldos, indicando fecha, hora, tipo de respaldo (integral, total, parcial de registros), ejecutor y revisor del respaldo, ubicación del respaldo, medio y etiqueta. **D)** Llenar y firmar formato.		
Mejores prácticas, referencias:		**1.-** La generación de respaldos, su control y protección deben formar parte de un plan de continuidad de operaciones y de recuperación ante desastres (**DRP**).		
Conocimientos requeridos:		Administración de sistema de información. Administración de sistema operativo.		
Ejecución			**Fecha inicio**	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término**	
Observaciones / anotaciones				

(Nombre del sistema A1)			Identificador único A1	
Formato:	**19**	**Verificación anual**	**Acción concluida**	( )
Medidas de seguridad técnicas:		**Artículo 19. I. d) Impedir el uso de cuentas y servicios gestionados por personas físicas para el tratamiento de los datos personales.**		
Aplicable en:		I. Bases de datos y sistemas de tratamiento.		
Tiempo estimado:		Veinte días hábiles.		
Importancia de la acción:		Debe evitarse el riesgo que implica el depender de cuentas de control personal para acceder a servicios, fuentes de información o cualquier elemento del sistema de información que ponga en riesgo su estabilidad y confiabilidad.		
Proceso recomendado:		**A)** Realizar revisión integral del sistema de información en materia de accesos, cuentas y servicios. *Por ejemplo*: En caso de consultar vía un *Webservice* a un sistema autoritativo de datos personales en la DGAE, identificar la cuenta de acceso a ese sistema. **B)** Determinar si las cuentas de acceso a servicios locales o remotos están bajo el control de la administración del sistema. *Por ejemplo*: Si la cuenta de acceso a un *Webservice* – su usuario y contraseña – está bajo el control del administrador del sistema, o si un respaldo que se realiza en un equipo remoto es con una cuenta y contraseña controlada por el administrador del sistema. **C)** Si las cuentas de acceso a servicios locales o remotos pertenecen a personas del Área Universitaria, cambiarlas por cuentas institucionales dentro del control de la instancia universitaria. *Por ejemplo*: si la identificación para acceder a un respaldo remoto es del tipo xxx@google.com, deberá cambiarse por una cuenta del tipo xxxx@unam.mx **D)** Llenar y firmar formato.		
Mejores prácticas, referencias:		**1.-** Nunca deben usarse cuentas, servicios, suscripciones, licencias o cualquier otro elemento informático cuyo control dependa de una sola persona.		
Conocimientos requeridos:		Administración de sistema de información. Gestión de bases de datos.		

Ejecución	Fecha inicio
Nombre y firma	**Fecha término**
Administrador del sistema de información o servidor	
Observaciones / anotaciones	

(Nombre del sistema A1)			Identificador único A1	
Formato:	**20**	**Verificación anual**	**Acción concluida**	( )
Medidas de seguridad técnicas:		**Artículo 19. II. a) Proteger ante manipulaciones indebidas y accesos no autorizados las bitácoras y los dispositivos donde se almacenan.**		
Aplicable en:		II. Sistemas operativos.		
Tiempo estimado:		Cuatro días hábiles.		
Importancia de la acción:		Las bitácoras son un elemento esencial para determinar acciones que atentan contra la estabilidad del sistema de información y la protección de los datos personales.		
Proceso recomendado:		**A)** Elaborar una lista de las bitácoras relacionadas con el sistema de información, tanto en medio digital como físico. *Por ejemplo*: En el equipo de cómputo las bitácoras de acceso de usuarios al sistema operativo y al sistema de información (*logs*), de forma física las bitácoras de acceso al área donde está el equipo de cómputo. **B)** Junto a la lista elaborar el cronograma de revisión de integridad y respaldo de las bitácoras. *Por ejemplo*: diario, semanal, mensual. **C)** Establecer en el documento el procedimiento de resguardo de las bitácoras. *Por ejemplo*: respaldo y protección de *logs* en el caso de equipo de cómputo o zonas seguras de almacenamiento de bitácoras en papel, digitalización de registros. **D)** Llenar y firmar formato.		
Mejores prácticas, referencias:		**1.-** Las bitácoras digitales y en papel deben resguardarse preferentemente en una zona independiente de la ubicación del sistema de información.		
Conocimientos requeridos:		Administración de sistema de información. Administración de sistema operativo.		
Ejecución			**Fecha inicio**	
Nombre y firma			**Fecha término**	
Administrador del sistema de información o servidor				
Observaciones / anotaciones				

(Nombre del sistema A1)			Identificador único A1	
Formato:	**21**	**Verificación anual**	**Acción concluida**	( )
Norma Complementaria Técnica		**Artículo 19. IV. b) Supervisar los controles de seguridad en la red de datos donde opere el sistema para tratamiento de datos personales.**		
Aplicable en:		IV. Red de datos.		
Tiempo estimado:		Cuatro días hábiles.		
Importancia de la acción:		El control de seguridad de los equipos activos de red que suministran la conectividad al sistema de información es un elemento básico para la protección de los datos.		
Proceso recomendado:		**A)** Identificar los equipos activos de red que permiten la conexión del equipo de cómputo con el sistema de información, incluyendo marca, modelo, versión de software, vigencia de mantenimiento y capacidades de protección de las comunicaciones. **B)** Determinar las reglas de seguridad físicas (acceso restringido, cuartos de telecomunicaciones) y lógicas (cuentas de acceso, puertos activos, protocolos activos) para el equipo de red. **C)** Incluir en las acciones para aseguramiento de la red de datos aquellas que sean necesarias en función de los controles actuales. Definir un plan de regularización de la seguridad en caso de ser aplicable. **D)** Mantener actualizados los equipos activos de red y con un programa de mantenimiento. **E)** Identificar y en su caso programar la instalación de equipo para seguridad perimetral de la red de datos. **D)** Llenar y firmar formato.		
Mejores prácticas, referencias:		**1.-** Las ubicaciones físicas de los equipos activos de red deben estar protegidas con cerraduras y controles de acceso, cumplir las normas de operación y no emplearse para ningún otro equipo o uso.		
Conocimientos requeridos:		Administración de redes de datos.		
Ejecución			**Fecha inicio**	
Nombre y firma			**Fecha término**	
Administrador del sistema de información o servidor				
Observaciones / anotaciones				

(Nombre del sistema A1)			Identificador único A1	
Formato:	**22**	**Verificación anual**	**Acción concluida**	( )
Medidas de seguridad técnicas:		**Artículo 19. IV. c) Proporcionar exclusivamente el acceso desde redes y servicios autorizados.**		
Aplicable en:		IV. Red de datos.		
Tiempo estimado:		Cuatro días hábiles.		
Importancia de la acción:		Es necesario reducir el mínimo necesario los puertos de comunicación para el funcionamiento del sistema de información.		
Proceso recomendado:		**A)** Revisar los puertos de comunicación (*TCP y UDP*) que requiera el sistema de información para su operación. *Por ejemplo*: para servicios *Web* los puertos 80 y 8080 son los convencionales. **B)** Activar en el sistema operativo la herramienta correspondiente para el control de puertos de comunicación. *Por ejemplo*, en Linux puede tratarse de un *firewall* a nivel de software o las herramientas que para tal efecto contenga la distribución correspondiente del sistema operativo. **C)** Dejar activos solamente los puertos necesarios para la operación del sistema. **D)** Activar el filtrado de la comunicación por direccionamiento IP en caso de ser posible para la operación del sistema. *Por ejemplo*: Permitir el acceso al puerto de *SSH* solamente a direcciones IP en una subred de la UNAM (132.248.x.y) o a un grupo de direcciones IP específicas. **E)** Llenar y firmar formato.		
Mejores prácticas, referencias:		**1.-** No se deben tener activos accesos que no son necesarios vía la red de datos.		
Conocimientos requeridos:		Administración de sistema de información. Administración de sistema operativo.		
Ejecución			**Fecha inicio**	
Nombre y firma			**Fecha término**	
Administrador del sistema de información o servidor				
Observaciones / anotaciones				

(Nombre del sistema A1)			Identificador único A1	
Formato:	**23**	**Verificación anual**	**Acción concluida**	( )
Medidas de seguridad técnicas:		**Artículo 18. I. b) Contar con entornos para desarrollo, pruebas y operación.**		
Aplicable en:		I. Bases de datos y sistemas de tratamiento.		
Tiempo estimado:		Veinte días hábiles.		
Importancia de la acción:		Para evitar riesgos innecesarios a la información, el desarrollo y actualización de los mismos deberá ser realizado siempre en una plataforma y ambientes por separado.		
Proceso recomendado:		**A)** Instalar y configurar equipos similares en características, preferentemente virtuales, a los equipos donde se instalará el sistema de información en su nueva o actualizada versión. **B)** Crear un repositorio en un equipo central de desarrollo para el resguardo de códigos, documentación, inventarios de datos y manuales de usuario, administrador y programador. **C)** Ejecutar las pruebas de nuevas versiones o actualizaciones del sistema de información en el equipo dispuesto para tal efecto. Nunca usar -equipos físicos o virtuales con el sistema actualmente en producción como las plataformas para evaluación de versiones en desarrollo. **D)** Llenar y firmar formato.		
Mejores prácticas, referencias:		**1.-** Se deben realizar respaldos de la información en los sistemas en desarrollo del mismo modo que como se realicen con el sistema en producción.		
Conocimientos requeridos:		Administración de sistema de información. Desarrollo de aplicaciones.		
Ejecución			**Fecha inicio**	
Nombre y firma			**Fecha término**	
Administrador del sistema de información o servidor				
Observaciones / anotaciones				

(Nombre del sistema A1)			Identificador único A1	
Formato:	**24**	**Verificación anual**	**Acción concluida**	( )
Medidas de seguridad técnicas:		**Artículo 18. I. f) Cumplir con las especificaciones de seguridad informática previo a la puesta en operación.**		
Aplicable en:		I. Bases de datos y sistemas de tratamiento.		
Tiempo estimado:		Veinte días hábiles.		
Importancia de la acción:		Solo los sistemas de información revisados integralmente en su seguridad y estabilidad pueden ser publicados bajo el dominio .unam.mx .		
Proceso recomendado:		A) Una vez concluido el desarrollo o actualización de un sistema de información, solicitar al área de seguridad del Área Universitaria la revisión de seguridad informática del sistema, lo que incluye: pruebas de penetración, pruebas de estabilidad, pruebas de carga y endurecimiento de la seguridad. En caso de no contar con esa área, requerirlo a UNAM CERT al correo seguridad.tic@unam.mx . **B)** Una vez recibido el reporte del área de seguridad, aplicar las medidas de corrección que incluya el reporte. Regresar al punto A. **C)** Habiendo resuelto los hallazgos y sugerencias de mejora de la seguridad señalados por el área especializada, realizar la instalación del sistema en la plataforma definitiva de cómputo, extrayéndolo del entorno de desarrollo. **D)** Llenar y firmar formato.		
Mejores prácticas, referencias:		**1.-** El equipo de UNAM CERT puede asesorar a las entidades y dependencias en la aplicación de las medidas de corrección y mitigación a partir de los resultados de la revisión de seguridad.		
Conocimientos requeridos:		Administración de aplicaciones. Administración de sistema operativo.		

Ejecución	Fecha inicio
Nombre y firma	**Fecha término**
Administrador del sistema de información o servidor	
Observaciones / anotaciones	

(Nombre del sistema A1)			Identificador único A1	
Formato:	**25**	**Verificación anual**	**Acción concluida**	( )
Medidas de seguridad técnicas:		**Artículo 18. III. a) Utilizar equipos con componentes actualizados, protegidos con garantías y soporte, y con la capacidad suficiente para atender la demanda del servicio y de los usuarios.**		
Aplicable en:		III. Equipos de cómputo.		
Tiempo estimado:		Hito.		
Importancia de la acción:		Mantener en adecuada condición de operación el equipo de cómputo incrementa la estabilidad y seguridad del sistema de información.		
Proceso recomendado:		**A)** Elaborar una lista del inventario de los equipos de cómputo, periféricos y de almacenamiento necesarios para la ejecución del sistema de información. **B)** Determinar la razón por la que el sistema de información requerirá estar localizado en un equipo físico y no en un servidor virtual. Con ello justificar una adquisición o actualización. Por ejemplo: por incompatibilidad con hipervisores, necesidades de comunicación exclusivamente locales en la entidad y dependencia o el no necesitar de un entorno de alta disponibilidad automática. **C)** Identificar en el inventario versiones, introducción en el mercado, vida útil, contratos de mantenimiento y soporte para todos y cada uno de los componentes, en el caso de emplear equipo físico. **D)** Adquirir los componentes y elementos necesarios para la actualización, vigencia de soporte y capacidad para atención a los usuarios en el equipo de cómputo físico. **E)** Llenar y firmar formato.		
Mejores prácticas, referencias:		**1.-** El mantenimiento preventivo debe contar con medidas de verificación.		
Conocimientos requeridos:		Administración de infraestructura.		
Ejecución			**Fecha inicio**	
Nombre y firma			**Fecha término**	
Administrador del sistema de información o servidor				
Observaciones / anotaciones				

(Nombre del sistema A1)			Identificador único A1	
Formato:	**26**	**Verificación anual**	**Acción concluida**	( )
Medidas de seguridad técnicas:		**Artículo 18. III. b) Definir el programa de mantenimiento preventivo.**		
Aplicable en:		III. Equipos de cómputo.		
Tiempo estimado:		Hito.		
Importancia de la acción:		Garantizar que el plan de mantenimiento de equipo se realiza en tiempo y forma.		
Proceso recomendado:		**A)** De la lista de equipo de cómputo físico necesario para la operación del sistema de información, extraer las vigencias de mantenimiento. **B)** En caso de no estar en posibilidad de aplicar el mantenimiento preventivo por el personal del Área Universitaria, cotizar pólizas de mantenimiento de acuerdo con el tipo de componente, preferentemente una sola póliza para el conjunto del equipo físico. **C)** Adquirir las pólizas de mantenimiento preventivo y observar su vigencia. La vigencia no podrá ser menor de un año. **D)** Llenar y firmar formato.		
Mejores prácticas, referencias:		**1.-** El programa de mantenimiento debe considerar los costos de contratos, refacciones, partes, actualizaciones y reemplazos.		
Conocimientos requeridos:		Administración de infraestructura.		
Ejecución			**Fecha inicio**	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término**	
Observaciones / anotaciones				

(Nombre del sistema A1)			Identificador único A1	
Formato:	**27**	**Verificación anual**	**Acción concluida**	( )
Medidas de seguridad técnicas:		**Artículo 19. III. c) Aplicar el programa de mantenimiento preventivo a los equipos.**		
Aplicable en:		III. Equipos de cómputo.		
Tiempo estimado:		Seis días hábiles.		
Importancia de la acción:		Garantizar que el plan de mantenimiento de equipo se realiza en tiempo y forma.		
Proceso recomendado:		**A)** En caso de que el personal del Área Universitaria pueda realizar el mantenimiento preventivo, definir el calendario de inactividad del sistema de información, notificar a los usuarios y aplicar el plan en caso de mantenimiento o inactividad. **B)** En caso de que sea a través de un proveedor que se proporcione el mantenimiento al equipo de cómputo, ejecutar el calendario de acciones preventivas en un período no superior a cada 3 meses hasta la conclusión del contrato o póliza respectivo. **C)** Llenar y firmar formato.		
Mejores prácticas, referencias:		**1.-** Debe actualizarse el equipo de cómputo de manera suficiente para continuar la operación del sistema y considerar en el mantenimiento preventivo sistemas paralelos de manera temporal hasta la conclusión de los trabajos.		
Conocimientos requeridos:		Administración de infraestructura.		
Ejecución			**Fecha inicio**	
Nombre y firma			**Fecha término**	
Administrador del sistema de información o servidor				
Observaciones / anotaciones				

(Nombre del sistema A1)			Identificador único A1	
Formato:	**28**	**Verificación anual**	**Acción concluida**	( )
Medidas de seguridad técnicas:		**Artículo 21.Solo se permitirá el uso de servicios de nube pública para el resguardo de archivos cifrados que contengan respaldos de la información.**		
Aplicable en:		Servicios en la nube pública.		
Tiempo estimado:		Hito.		
Importancia de la acción:		No pueden conservarse o usarse datos personales que sean tratados por la UNAM en servicios de nube pública. Estos servicios sólo se permiten para el respaldo de archivos cifrados, no en producción.		
Proceso recomendado:		**A)** Identificar los respaldos que se tengan resguardados en servicios de nube pública. **B)** Verificar el cifrado en cada uno de los respaldos que se almacenen en nube pública. El cifrado no deberá ser de menor capacidad al equivalente a AES de 128 bits.		
Mejores prácticas, referencias:		**1.-** La DGTIC proporciona el servicio de respaldos en el Centro de Datos, por lo que se sugiere utilizarlo en lugar de respaldos en la nube pública.		
Conocimientos requeridos:		Administración de respaldos. Administración de sistema operativo.		
Ejecución			**Fecha inicio**	
Nombre y firma			**Fecha término**	
Administrador del sistema de información o servidor				
Observaciones / anotaciones				

CENTRO DE ESTUDIOS MEXICANOS

UNAM-ESPAÑA

3. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

UNAM-España (Centro de Estudios Mexicanos)	
Identificador único	UNAM-España/MailChimp
(Nombre del sistema A1) *	Base de Datos MailChimp
Datos personales (sensibles o no) contenidos en el sistema*:	Nombre, apellido, correo electrónico, institución (dato optativo), país, indicación de si forma parte de la comunidad de la UNAM o no.
Responsable*:	
Nombre*:	Jorge Luis Volpi Escalante
Cargo*:	Director
Funciones*:	Coordinar la planeación y supervisión del envío de los boletines electrónicos de difusión de las actividades académicas, culturales o de información general por parte de la sede a la comunidad interesada y/o a la comunidad de la UNAM en España.
Obligaciones*:	-Supervisar que se cumplan y apliquen las políticas de protección de datos establecidas por la UNAM y la normativa española. -Establecer que, para estos fines, sólo se utilicen los datos que fueron integrados a la base de datos por los propios interesados, con la aceptación explícita de ceder dicha información personal para los fines descritos. -No difundir o compartir la información de la base de datos con terceras personas, instituciones o empresas. -Tratar la información con respeto. -Establecer mecanismos sencillos y claros para darse de baja y eliminar sus datos personales de la citada base de datos, si así lo desean. -Informar a las personas que proporcionan sus datos personales que ello se lleva a cabo a través de la plataforma MailChimp, y brindarles el enlace con la información sobre el procesamiento de sus datos a través de dicha plataforma. -Informar de todo lo anterior a las personas antes de que cedan sus datos.
	Encargados:
Nombre del encargado 1:	Diego Celorio Morayta
Cargo*:	Secretario académico
Funciones*:	Proponer contenidos y supervisar el envío de los boletines electrónicos de difusión de las actividades académicas, culturales o de información general por parte de la sede a la comunidad interesada y/o a la comunidad de la UNAM en España.
Obligaciones*:	-Utilizar para estos fines sólo los datos que fueron integrados a la base de datos por los propios interesados, mediante la aceptación de ceder dicha información personal para los fines descritos. -No difundir o compartir la información de la base de

	datos con terceras personas, instituciones o empresas. -Tratar la información con respeto. -Establecer mecanismos sencillos y claros para darse de baja y eliminar sus datos personales de la citada base de datos, si así lo desean. -Informar a las personas que proporcionan sus datos personales que ello se lleva a cabo a través de la plataforma MailChimp, y brindarles el enlace con la información sobre el procesamiento de sus datos a través de dicha plataforma. -Informar de todo lo anterior a las personas antes de que cedan sus datos.
Nombre del Encargado 2:	Adriana Suárez del Real Terrazas
Cargo*:	Secretaria técnica
Funciones*:	Elaboración y envío de los boletines electrónicos de difusión de las actividades académicas, culturales o de información general por parte de la sede a la comunidad interesada y/o a la comunidad de la UNAM en España.
Obligaciones*:	-Utilizar para estos fines sólo los datos que fueron integrados a la base de datos por los propios interesados, mediante la aceptación de ceder dicha información personal para los fines descritos. -No difundir o compartir la información de la base de datos con terceras personas, instituciones o empresas. -Tratar la información con respeto. -Establecer mecanismos sencillos y claros para darse de baja y eliminar sus datos personales de la citada base de datos, si así lo desean. -Informar a las personas que proporcionan sus datos personales que ello se lleva a cabo a través de la plataforma MailChimp, y brindarles el enlace con la información sobre el procesamiento de sus datos a través de dicha plataforma. -Informar de todo lo anterior a las personas antes de que cedan sus datos.
(Nombre del Encargado 3*)	Sandra Ortega García
Cargo*:	Suplente secretaria técnica, durante baja maternal (2022)
Funciones*:	Elaboración y envío de los boletines electrónicos de difusión de las actividades académicas, culturales o de información general por parte de la sede a la comunidad interesada y/o a la comunidad de la UNAM en España.
Obligaciones*:	-Utilizar para estos fines sólo los datos que fueron integrados a la base de datos por los propios interesados, mediante la aceptación de ceder dicha información personal para los fines descritos. -No difundir o compartir la información de la base de datos con terceras personas, instituciones o empresas. -Tratar la información con respeto. -Establecer mecanismos sencillos y claros para darse de baja y eliminar sus datos personales de la citada base de datos, si así lo desean. -Informar a las personas que proporcionan sus datos personales que ello se lleva a cabo a través de la

	plataforma MailChimp, y brindarles el enlace con la información sobre el procesamiento de sus datos a través de dicha plataforma. -Informar de todo lo anterior a las personas antes de que cedan sus datos.
	Usuarios:
(Nombre del Usuario 1*)	Diego Celorio Morayta
Cargo*:	Ídem
Funciones*:	Ídem
Obligaciones*:	Ídem
(Nombre del Usuario 2*)	Adriana Suárez del Real Terrazas
Cargo*:	Ídem
Funciones*:	Ídem
Obligaciones*:	Ídem
(Nombre del Usuario 3*)	Sandra Ortega García
Cargo*:	Ídem
Funciones*:	Ídem
Obligaciones*:	Ídem

2. ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

UNAM-España (Centro de Estudios Mexicanos)	
Identificador único¨*	UNAM-España/MailChimp
(Nombre del sistema A1*)	Base de datos MailChimp
Tipo de soporte:*	Electrónico
Descripción:*	Base de datos electrónica en la que, mediante un formulario en línea, se inscribe voluntariamente y de manera personal toda aquella persona interesada en recibir por correo electrónico información general sobre UNAM-España y las actividades que la sede lleva a cabo. Como parte del formulario, y en seguimiento a la normativa española, la persona que se inscribe debe de manifestar explícitamente que autoriza que sus datos se recaben y que sean utilizados para los fines descritos.
Características del lugar donde se resguardan los soportes:*	La base de datos se encuentra en su totalidad en la plataforma electrónica MailChimp, en línea. Los usuarios proporcionan su información directamente en esta plataforma, y desde ella se emiten también los correos electrónicos, por lo que la información no sale de ese sistema.

3. ANÁLISIS DE RIESGOS

UNAM-España (Centro de Estudios Mexicanos)		
Identificador único*	UNAM-España/MailChimp	
(Nombre del sistema A1) *	Base de Datos MailChimp	
Riesgo*	**Impacto***	**Mitigación***
Hackeo de la contraseña de acceso a la base de datos Perder la base de datos	ALTO. Se puede tener acceso a la base de datos por parte de terceros no autorizados. ALTO: se puede perder la base de datos de la comunidad interesada de las actividades de UNAM-España	Utilizar una contraseña que incorpore mayor seguridad (mayúsculas, símbolos, números, etc). Actualización periódica de la contraseña. Realizar periódicamente copias de seguridad y exportar los datos.

4. ANÁLISIS DE BRECHA

UNAM-España (Centro de Estudios Mexicanos)		
Identificador único*	UNAM-España/MailChimp	
(Nombre del sistema A1) *	Base de datos MailChimp	
Medida de seguridad actual*	**Medida de seguridad necesaria***	**Acciones para remediación***
-Sólo las personas necesarias cuentan con la contraseña de acceso.	Implementar contraseñas robustas y actualizarlas periódicamente. Reforzar el acceso con un sistema de autentificación en dos pasos. Asignar o revocar los privilegios de acceso para los usuarios teniendo como base el principio del menor privilegio Hacer copia de seguridad de la base de datos	Tener un protocolo de contraseñas seguras y actualizarlas al menos cada semestre Incluir la medida en las preferencias de seguridad de la plataforma MailChimp. Realizar periódicamente una copia de seguridad de la base de datos

5. PLAN DE TRABAJO

UNAM-España (Centro de Estudios Mexicanos)			
Identificador único*	UNAM-España/MailChimp		
(Nombre del sistema A1) *	Base de Datos MailChimp		
Actividad*	**Descripción***	**Duración***	**Cobertura***
-Control de contraseñas -Activar sistema de verificación en dos pasos - Exportar los datos de la base como copia de seguridad	Cambiar la contraseña periódicamente. Activar las preferencias de verificación en dos pasos, y las notificaciones en caso de accesos nuevos o poco frecuentes. El sistema Mailchimp permite realizar una copia de seguridad de ciertos datos que se resguardan	Duración: 1 día. Periodicidad: semestral Duración 1 día. Ya activada Duración: 1 día	Estas medidas ayudarán a brindar mayor seguridad a la información contenida en la plataforma, impidiendo el acceso por terceros no autorizados o ajenos a la institución. Igualmente, al realizar la copia de seguridad se permitirá conservar la base de datos en caso de riesgo.

6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

I. TRANSFERENCIAS DE DATOS PERSONALES

UNAM-España (Centro de Estudios Mexicanos)	
Identificador único*	UNAM-España/MailChimp
(Nombre del sistema A1)*	Base de datos MailChimp
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	No se realizan trasferencias mediante traslados en soportes físicos
Transferencias mediante el traslado de soportes electrónicos:	No se realizan trasferencias mediante traslados en soportes electrónicos
Transferencias mediante el traslado sobre redes electrónicas:	No se realizan transferencias de la base de datos mediante redes electrónicas.

1. **INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES**

Sistema (Nombre del A2):	UNAM-España/CarpetaProyectos
Datos personales contenidos en el sistema*:	Nombre, apellidos, institución de pertenencia, correo electrónico, teléfono. Adicionalmente, en muchos casos, también nacionalidad, número de pasaporte (o identificación oficial), fecha de nacimiento, dirección postal, fotografía.
	Responsable:
Nombre*:	Diego Celorio Morayta
Cargo*:	Secretario académico
Funciones*:	Recabar la información necesaria de: -Académicos, docentes, investigadores, artistas, creadores etc, de la UNAM u otras instituciones, quienes participan en actividades académicas, culturales o de movilidad organizaras por la sede o con la colaboración de la sede. -Alumnos o egresados quienes participan en convocatorias para realizan estancias de prácticas profesionales o estancias temporales en la sede. -Alumnos en movilidad estudiantil a España, cuyos datos son proporcionados por DGECI -Alumnos/candidatos a los que se apoya a petición de instancias de la UNAM para que presenten en la sede exámenes o pruebas de diferente índole. -Alumnos inscritos a cursos, diplomados o, en general, actividades de educación continua organizadas por la sede o con la colaboración de la sede.
Obligaciones*:	-Solicitar y recabar por parte de los interesados sólo la información y documentación que se requiere para las gestiones administrativas de cada caso (asignación de vuelos aéreos, gestión de hospedaje, transportes locales, inscripciones, seguros médicos, etc.) -No compartir la información personal con terceras personas, instituciones o empresas, sin la autorización de los interesados, y sólo cuando sea estrictamente necesario (por ejemplo, reserva de hospedaje, o trayectos aéreos) -Tratar la información con respeto. -Restringir el acceso a las carpetas que contienen dicha información, permitiéndolo sólo a las personas autorizadas de la sede que requieran la información para llevar a cabo las gestiones del caso.
	Encargados:
(Nombre del Encargado 1*)	Adriana Suárez del Real Terrazas
Cargo*:	Secretaria técnica
Funciones*:	Recabar la información necesaria de: -Académicos, docentes, investigadores, etc, de la UNAM u otras instituciones, quienes participan en actividades académicas, culturales o de movilidad organizaras por la sede o con la colaboración de la sede -Alumnos o egresados quienes participan en convocatorias

	para realizan estancias de prácticas profesionales en la sede. -Alumnos en movilidad estudiantil a España, cuyos datos son proporcionados por DGECI -Alumnos/candidatos a los que se apoya a petición de instancias de la UNAM para que presenten en la sede exámenes de diferente índole. -Alumnos inscritos a cursos, diplomados o, en general, actividades de Educación Continua organizadas por la sede o con la colaboración de la sede.
Obligaciones*:	-Solicitar y recabar por parte de los interesados sólo la información y documentación que se requiere para las gestiones administrativas de cada caso (asignación de vuelos aéreos, gestión de hospedaje, transportes locales, inscripciones, seguros médicos, etc.) -No compartir la información personal con terceras personas, instituciones o empresas, sin la autorización de los interesados, y sólo cuando sea estrictamente necesario (por ejemplo, reserva de hospedaje, o trayectos aéreos) -Resguardar las contraseñas que le han sido confiadas y mantenerlas en secreto. -Tratar la información con respeto.
(Nombre del Encargado 2*)	Sandra Ortega García
Cargo*:	Suplente secretaria técnica, durante baja maternal (2022)
Funciones*:	Recabar la información necesaria de: -Académicos, docentes, investigadores, etcétera, de la UNAM u otras instituciones, quienes participan en actividades académicas, culturales o de movilidad organizaras por la sede o con la colaboración de la sede -Alumnos o egresados quienes participan en convocatorias para realizan estancias de prácticas profesionales en la sede. -Alumnos en movilidad estudiantil a España, cuyos datos son proporcionados por DGECI -Alumnos/candidatos a los que se apoya a petición de instancias de la UNAM para que presenten en la sede exámenes de diferente índole. -Alumnos inscritos a cursos, diplomados o, en general, actividades de Educación Continua organizadas por la sede o con la colaboración de la sede.
Obligaciones*:	-Solicitar y recabar por parte de los interesados sólo la información y documentación que se requiere para las gestiones administrativas de cada caso (asignación de vuelos aéreos, gestión de hospedaje, transportes locales, inscripciones, seguros médicos, etc.) -No compartir la información personal con terceras personas, instituciones o empresas, sin la autorización de los interesados, y sólo cuando sea estrictamente necesario (por ejemplo, reserva de hospedaje, o trayectos aéreos) -Tratar la información con respeto. -Resguardar las contraseñas que le han sido confiadas y mantenerlas en secreto.
	Usuarios:
(Nombre del Usuario 1*)	Diego Celorio Morayta

Cargo*:	Secretario académico
Funciones*:	Ídem
Obligaciones*:	Ídem
(Nombre del Usuario 2*)	Víctor Manuel Hernández Rivera
Cargo*:	Coordinador de Relaciones y Gestión
Funciones*:	Ídem
Obligaciones*:	Ídem
(Nombre del Usuario 3*)	Adriana Suárez del Real Terrazas
Cargo*:	Ídem
Funciones*:	Ídem
Obligaciones*:	Ídem
(Nombre del Usuario 4*)	Sandra Ortega García
Cargo*:	Suplente secretaria técnica, durante baja maternal (2022)
Funciones*:	Ídem
Obligaciones*:	Ídem

2. ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

(Nombre del sistema A2*)	UNAM-España/Carpeta Proyectos
Tipo de soporte*:	Soporte electrónico
Descripción*:	Cada actividad que realiza la sede cuenta con una subcarpeta electrónica en donde se guarda toda la documentación relacionada al proyecto. Cada una de estas subcarpetas se almacena en una carpeta anual (Actividades 2021, Actividades 2022, etc.). Las carpetas de los proyectos que están en marcha se almacenan en la nube de la plataforma DropBox, y aquellos proyectos ya concluidos se archivan en un servidor local NAS, propiedad de UNAM-España.
Características del lugar donde se resguardan los soportes*:	Las carpetas electrónicas de los proyectos en curso se encuentran en la nube de la plataforma DropBox, hasta que se concluye el proyecto y son archivados en el NAS. Los proyectos archivados se encuentran en el disco duro del NAS, que se encuentra físicamente en la oficina del secretario académico de la sede. Periódicamente, se hace un respaldo del NAS en un disco duro externo, mismo que se guarda en un archivero de metal de la sede, bajo llave. Para poder acceder a ambos sistemas se requiere de sendas contraseñas, que sólo son del conocimiento del personal de la sede.

3. ANÁLISIS DE RIESGOS

UNAM-España (Centro de Estudios Mexicanos)		
Identificador único*	UNAM-España/Carpeta Proyectos	
(Nombre del sistema A2) *	Carpetas Proyectos	
Riesgo*	**Impacto***	**Mitigación***
Hackeo de la contraseña de acceso a DropBox o NAS.	ALTO Acceso a la información general de los proyectos y, por tanto, a información personal por parte de terceros no autorizados.	Utilizar una contraseña que incorpore mayor seguridad (mayúsculas, símbolos, números, etc). Actualización periódica de la contraseña.

4. ANÁLISIS DE BRECHA

UNAM-España (Centro de Estudios Mexicanos)		
Identificador único*	UNAM-España/Carpeta Proyectos	
(Nombre del sistema A2) *	Carpetas electrónicas proyectos	
Medida de seguridad actual*	**Medida de seguridad necesaria***	**Acciones para remediación***
-Sólo las personas necesarias cuentan con la contraseña de acceso. -A la carpeta de "Administración" sólo tiene acceso el administrador y no el resto de los usuarios. -Si se producen cambios en la plantilla de la sede, se da de baja el acceso de aquellas personas que ya no laboran en ella.	Realizar copias de seguridad periódicas de la información electrónica contenida en el NAS, utilizando un disco duro externo cifrado. Almacenar dicho respaldo en un lugar diferente, para que en caso de siniestro o robo no se pierda la información.	Programar respaldos de la información en un disco cifrado y almacenarlo en lugar diferente al del NAS.

5. PLAN DE TRABAJO

UNAM-España (Centro de Estudios Mexicanos)			
Identificador único*	UNAM-España/Carpeta Proyectos		
(Nombre del sistema A2)	Carpetas electrónicas proyectos		
Actividad	**Descripción**	**Duración**	**Cobertura**
-Activar sistema de verificación en dos pasos. -Realizar respaldos periódicos Actualizar componentes de equipo, dar soporte y asegurar la capacidad de de almacenamiento Definir el programa de mantenimiento preventivo	-Activar las preferencias de verificación en dos pasos, y las notificaciones en caso de accesos nuevos o poco frecuentes. -Realizar respaldos de la información en un disco duro externo Realizar mantenimiento preventivo al equipo NAS	- Duración 1 día. Ya activada -Duración 1 día. Periodicidad mensual Periodicidad Anual	-Aumentar la seguridad a la información contenida en el servidor NAS, impidiendo el acceso por terceros no autorizados o ajenos a la institución. -Se resguardará la información en un disco duro cifrado, en caso de deterioro o robo del NAS. Se mantendrá contacto con la empresa que otorga el servicio de mantenimiento para programar sesiones, anuales o semestrales

5. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

II. TRANSFERENCIAS DE DATOS PERSONALES

UNAM-España (Centro de Estudios Mexicanos)	
Identificador único*	UNAM-España/CarpetaProyectos
(Nombre del sistema A2)*	Carpetas electrónicas proyectos
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	No se realizan trasferencias mediante traslados en soportes físicos
Transferencias mediante el traslado de soportes electrónicos:	No se realizan trasferencias mediante traslados en soportes electrónicos
Transferencias mediante el traslado sobre redes electrónicas:	No se realizan trasferencias mediante traslados en soportes físicos

1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Sistema (Nombre del A3):	UNAM-España/Formularios google
Datos personales contenidos en el sistema*:	Nombre, apellidos, institución de pertenencia, correo electrónico, nacionalidad, nombre de los estudios realizados, nivel de escolaridad, sexo.
	Responsable:
Nombre*:	Diego Celorio Morayta
Cargo*:	Secretario académico
Funciones*:	Recabar la información necesaria de: -Alumnos inscritos a cursos, diplomados o, en general, actividades de educación continua organizadas por la sede o con la colaboración de la sede.
Obligaciones*:	-Solicitar y recabar por parte de los interesados sólo la información que se requiere para las inscripciones con el fin de llevar un control de la matrícula. -No compartir la información personal con terceras personas, instituciones o empresas, sin la autorización de los interesados, y sólo cuando sea estrictamente necesario (por ejemplo, cuando la UNAM o las instituciones con las que se colabora solicitan datos de comunidad beneficiada de las actividades académicas y culturales de la sede) -Tratar la información con respeto. -Restringir el acceso a los formularios que contienen dicha información, permitiéndolo sólo a las personas autorizadas de la sede que requieran la información para llevar a cabo las gestiones del caso.
	Encargados:
(Nombre del Encargado 1*)	Adriana Suárez del Real Terrazas
Cargo*:	Secretaria técnica
Funciones*:	Recabar la información necesaria de: -Alumnos inscritos a cursos, diplomados o, en general, actividades de Educación Continua organizadas por la sede o con la colaboración de la sede.
Obligaciones*:	- No compartir la información personal con terceras personas, instituciones o empresas, sin la autorización de los interesados, y sólo cuando sea estrictamente necesario (por ejemplo, cuando la UNAM o las instituciones con las que se colabora solicitan datos de comunidad beneficiada de las actividades académicas y culturales de la sede) -Tratar la información con respeto. -Restringir el acceso a los formularios que contienen dicha información, permitiéndolo sólo a las personas autorizadas de la sede que requieran la información para llevar a cabo las gestiones del caso.
(Nombre del Encargado 2*)	Sandra Ortega García
Cargo*:	Suplente secretaria técnica, durante baja maternal (2022)
Funciones*:	Recabar la información necesaria de: -Alumnos inscritos a cursos, diplomados o, en general,

	actividades de Educación Continua organizadas por la sede o con la colaboración de la sede.
Obligaciones*:	- No compartir la información personal con terceras personas, instituciones o empresas, sin la autorización de los interesados, y sólo cuando sea estrictamente necesario (por ejemplo, cuando la UNAM o las instituciones con las que se colabora solicitan datos de comunidad beneficiada de las actividades académicas y culturales de la sede) -Tratar la información con respeto. -Restringir el acceso a los formularios que contienen dicha información, permitiéndolo sólo a las personas autorizadas de la sede que requieran la información para llevar a cabo las gestiones del caso.
	Usuarios:
(Nombre del Usuario 1*)	Diego Celorio Morayta
Cargo*:	Secretario académico
Funciones*:	Ídem
Obligaciones*:	Ídem
(Nombre del Usuario 2*)	Adriana Suárez del Real Terrazas
Cargo*:	Ídem
Funciones*:	Ídem
Obligaciones*:	Ídem
(Nombre del Usuario 3*)	Sandra Ortega García
Cargo*:	Suplente secretaria técnica, durante baja maternal (2022)
Funciones*:	Ídem
Obligaciones*:	Ídem

2. ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

(Nombre del sistema A3*)	UNAM-España/formulariosgoogle
Tipo de soporte*:	Soporte electrónico
Descripción*:	Herramienta de Google que permite recabar información y gestionar las inscripciones y matriculaciones por parte de la comunidad interesada a las actividades (en su generalidad cursos, seminarios etc.) que oferta la sede.
Características del lugar donde se resguardan los soportes*:	Los formularios se diseñan y, el proceso en que se recaban los datos, se alojan en la propia plataforma de Google. Una vez que se cierra el proceso de inscripción a cursos o seminarios, los datos se almacenan en bases de datos de Excel que se resguardan en la carpeta de los proyectos en Dropbox o NAS. Para poder acceder a los formularios se accede mediante las cuentas de Gmail, cuyas contraseñas solo son del conocimiento de los usuarios de la sede.

3. ANÁLISIS DE RIESGOS

UNAM-España (Centro de Estudios Mexicanos)		
Identificador único*	UNAM-España/Formulariosgoogle	
(Nombre del sistema A3) *	Formularios Google	
Riesgo*	**Impacto***	**Mitigación***
Hackeo de la contraseña de acceso a Google y acceso a los formularios.	ALTO Acceso a la información general y datos de terceros recabados a través del formulario, posible mal uso de los mismos.	Utilizar una contraseña que incorpore mayor seguridad (mayúsculas, símbolos, números, etc.). Actualización periódica de la contraseña.

4. ANÁLISIS DE BRECHA

UNAM-España (Centro de Estudios Mexicanos)		
Identificador único*	UNAM-España/Formulariosgoogle	
(Nombre del sistema A3) *	Formularios Google	
Medida de seguridad actual*	**Medida de seguridad necesaria***	**Acciones para remediación***
-Sólo las personas necesarias cuentan con la contraseña de acceso a Google -Si se producen cambios en la plantilla de la sede, se da de baja el acceso de aquellas personas que ya no laboran en ella.	Realizar borrado seguro de datos de los formularios que se dejan de utilizar y resguardar la información estadística y o de archivo en NAS.	Programar borrado seguro de datos. Programar respaldo en Excel de datos para archivo y / o estadística. Vigilar el cierre de sesión de las cuentas de Google una vez que se termine de hacer uso del servicio.

5. PLAN DE TRABAJO

UNAM-España (Centro de Estudios Mexicanos)			
Identificador único*	UNAM-España/Formulariosgoogle		
(Nombre del sistema A2)	Formularios google		
Actividad	**Descripción**	**Duración**	**Cobertura**
- Cambio periódico de contraseña y aplicación del principio de menor privilegio - Activar sistema de verificación en dos pasos. -Realizar respaldos periódicos	- Calendarizar los cambios de contraseña de las cuentas Google -Activar las preferencias de verificación en dos pasos, y las notificaciones en caso de accesos nuevos o poco frecuentes. -Realizar respaldos de la información en un disco duro externo	- duración 1 día - Duración 1 día. Ya activada -Duración 1 día. Periodicidad mensual	- Asegurar el acceso mediante el cambio periódico de contraseña y aplicar el principio de menor privilegio - Aumentar la seguridad a la información contenida en servidor NAS, impidiendo el acceso por terceros no autorizados o ajenos a la institución. -Se resguardará la información en un disco duro cifrado, en caso de deterioro o robo del NAS.

6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

III. TRANSFERENCIAS DE DATOS PERSONALES

UNAM-España (Centro de Estudios Mexicanos)	
Identificador único*	UNAM-España/Formularios google
(Nombre del sistema A3)*	Formularios google
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	No se realizan trasferencias mediante traslados en soportes físicos
Transferencias mediante el traslado de soportes electrónicos:	No se realizan trasferencias mediante traslados en soportes electrónicos
Transferencias mediante el traslado sobre redes electrónicas:	No se realizan trasferencias mediante traslados en soportes físicos

1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

UNAM-España (Centro de Estudios Mexicanos)	
Identificador único	UNAM-España/correoelectronicoinstitucional
(Nombre del sistema A4) *	Correo electrónico institucional
Datos personales (sensibles o no) contenidos en el sistema*:	Las comunicaciones a través de los correos electrónicos del personal de la sede contienen información, en ocasiones datos personales, que forman parte del funcionamiento diario de la misma. Ésta emana y llega desde y hacia la dirección, la secretaría académica, administrativa y técnica. Los datos sensibles que pueden llegar a circular forman parte de la propia operación de la sede para el desarrollo de las actividades académicas y culturales, entre los que se encuentra: datos de identificación, datos laborales o datos académicos.
Responsable*:	
Nombre*:	Jorge Luis Volpi Escalante
Cargo*:	Director
Funciones*:	Recabar información para el desarrollo de las actividades de dirección, representación institucional, vinculación, académicas y culturales.
Obligaciones*:	-No compartir la información personal recabada con terceras personas, instituciones o empresas, sin la autorización de los interesados, y sólo cuando sea estrictamente necesario (por ejemplo, cuando la UNAM o las instituciones o empresas con las que se colabora solicitan datos de comunidad beneficiada de las actividades académicas y culturales de la sede) -Tratar la información con respeto.
	Encargados:
Nombre del encargado 1:	Diego Celorio Morayta
Cargo*:	Secretario académico
Funciones*:	Recabar información para el desarrollo de las actividades de secretaria académica, de representación institucional, de vinculación y culturales.
Obligaciones*:	-No compartir la información personal recabada con terceras personas, instituciones o empresas, sin la autorización de los interesados, y sólo cuando sea estrictamente necesario (por ejemplo, cuando la UNAM o las instituciones o empresas con las que se colabora solicitan datos de comunidad beneficiada de las actividades académicas y culturales de la sede). -Tratar la información con respeto.
Nombre del Encargado 2:	Adriana Suárez del Real Terrazas
Cargo*:	Secretaria técnica
Funciones*:	Recabar información para el desarrollo de las actividades de secretaria técnica, representación institucional, vinculación y culturales.
Obligaciones*:	-No compartir la información personal recabada con terceras personas, instituciones o empresas, sin la

	autorización de los interesados, y sólo cuando sea estrictamente necesario (por ejemplo, cuando la UNAM o las instituciones o empresas con las que se colabora solicitan datos de comunidad beneficiada de las actividades académicas y culturales de la sede) -Tratar la información con respeto.
(Nombre del Encargado 3*)	Sandra Ortega García
Cargo*:	Suplente secretaria técnica, durante baja maternal (2022)
Funciones*:	Recabar información para el desarrollo de las actividades de secretaria técnica, representación institucional, vinculación y culturales.
Obligaciones*:	-No compartir la información personal recabada con terceras personas, instituciones o empresas, sin la autorización de los interesados, y sólo cuando sea estrictamente necesario (por ejemplo, cuando la UNAM o las instituciones o empresas con las que se colabora solicitan datos de comunidad beneficiada de las actividades académicas y culturales de la sede) -Tratar la información con respeto.
(Nombre del encargado 4)	Víctor Manuel Hernández Rivera
Cargo	Coordinador de Relaciones y Gestión
Funciones	Recabar información para el desarrollo de las actividades de la coordinación de relaciones y gestión.
Obligaciones	-No compartir la información personal recabada con terceras personas, instituciones o empresas, sin la autorización de los interesados, y sólo cuando sea estrictamente necesario (por ejemplo, cuando la UNAM o las instituciones o empresas con las que se colabora solicitan datos de comunidad beneficiada de las actividades académicas y culturales de la sede) -Tratar la información con respeto.
	Usuarios:
Nombre del Usuario 1	Jorge Volpi Escalante
Cargo	Idem
Funciones	Idem
Obligaciones	Idem
(Nombre del Usuario 2*)	Diego Celorio Morayta
Cargo*:	Ídem
Funciones*:	Ídem
Obligaciones*:	Idem
(Nombre del Usuario 3*)	Adriana Suárez del Real Terrazas
Cargo*:	Ídem
Funciones*:	Ídem
Obligaciones*:	Ídem
(Nombre del Usuario 4*)	Sandra Ortega García
Cargo*:	Ídem
Funciones*:	Ídem
Obligaciones*:	Ídem
(Nombre del Usuario 5*)	Victor Manuel Hernández Rivera
Cargo*:	Idem

Funciones*:	Idem
Obligaciones*:	Idem

2. ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

UNAM-España (Centro de Estudios Mexicanos)	
Identificador único¨*	UNAM-España/Correo electrónico institucional
(Nombre del sistema A4*)	Correo electrónico institucional
Tipo de soporte:*	Electrónico
Descripción:*	Sistema de comunicación electrónica institucional que utilizan los miembros y el staff de cada una de las áreas de la sede en el que circula información del funcionamiento diario de la misma y que emana y llega hacia y desde la dirección, la secretaría académica, administrativa y técnica. La información mantiene activa la propia operación de la sede para el desarrollo de las actividades académicas, culturales, de vinculación y representación, así como administrativas y de gestión. Las comunicaciones contienen información de la UNAM y de terceras instituciones.
Características del lugar donde se resguardan los soportes:*	Los datos, archivos e información que circulan a través de las comunicaciones del correo electrónico son gestionados, y resguardados, según corresponda, en el propio correo, y luego en las carpetas de proyectos, el Dropbox o el NAS.

3. ANÁLISIS DE RIESGOS

UNAM-España (Centro de Estudios Mexicanos)		
Identificador único*	UNAM-España/Correo electrónico institucional	
(Nombre del sistema A4) *	Correo electrónico institucional	
Riesgo*	**Impacto***	**Mitigación***
- Hackeo de las contraseñas de los correos institucionales de cada una de las áreas. - Que terceros con los que se tenga comunicación puedan hacer mal uso de la información que se comparte	ALTO. Se puede tener acceso a las comunicaciones de las diferentes áreas por parte de terceros no autorizados. ALTO: Terceros pueden hacer mal uso de información que circula en los correos electrónicos.	Utilizar una contraseña que incorpore mayor seguridad (mayúsculas, símbolos, números, etc.). Actualización periódica de la contraseña.

4. ANÁLISIS DE BRECHA

UNAM-España (Centro de Estudios Mexicanos)		
Identificador único*	UNAM-España/Correo institucional	
(Nombre del sistema A4) *	Correo electrónico institucional	
Medida de seguridad actual*	**Medida de seguridad necesaria***	**Acciones para remediación***
-Sólo las personas necesarias cuentan con la contraseña de acceso a cada una de las cuentas.	Implementar contraseñas robustas y actualizarlas periódicamente. Reforzar el acceso con un sistema de autentificación en dos pasos.	Tener un protocolo de contraseñas seguras y actualizarlas al menos cada semestre. Agregar aviso de privacidad en la firma de los correos electrónicos institucionales. Vigilar el cierre de sesión desde el dispositivo del que se usa.

5. PLAN DE TRABAJO

UNAM-España (Centro de Estudios Mexicanos)			
Identificador único*	UNAM-España/Correo institucional		
(Nombre del sistema A4) *	Correo electrónico institucional		
Actividad*	**Descripción***	**Duración***	**Cobertura***
-Control de contraseñas -Activar sistema de verificación en dos pasos - Agregar Aviso de privacidad - Cierre de sesiones - Configuración de seguridad del equipo de cómputo. Instalación de antivirus actualizado -Envío de información cifrada y/o con acceso restringido.	Cambiar la contraseña periódicamente. Activar las preferencias de verificación en dos pasos, y las notificaciones en caso de accesos nuevos o poco frecuentes. Agregar un aviso de privacidad en la firma de los correos electrónicos que indique que la información contenida en los correos puede ser confidencial y se prohíbe la distribución y mal uso de la misma según la legislación vigente Procurar el cierre de sesiones de las cuentas del correo electrónico Realizar las actualizaciones del sistema correspondientes y del sistema operativo así como la	Duración: 1 día. Periodicidad: semestral Duración 1 día. Ya activada Duración: 1 día Duración: Todos los días laborales o en los que se utilice el correo electrónico Cada vez que el sistema lo solicite, actualizar el antivirus anual o semestralmente.	Estas medidas ayudarán a brindar mayor seguridad a la información contenida en los correos, impidiendo el acceso por terceros no autorizados o ajenos a la institución.

	instalación y mantenimiento de software antivirus Procurar cifrar o restringir con contraseñas el envío de documentación sensible a través del correo electrónico.		

6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS
IV. TRANSFERENCIAS DE DATOS PERSONALES

UNAM-España (Centro de Estudios Mexicanos)	
Identificador único*	UNAM-España/Correo institucional
(Nombre del sistema A4)*	Correo electrónico institucional
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	No se realizan trasferencias mediante traslados en soportes físicos
Transferencias mediante el traslado de soportes electrónicos:	No se realizan trasferencias mediante traslados en soportes electrónicos
Transferencias mediante el traslado sobre redes electrónicas:	La trasferencia, mediante correo electrónico, de documentos que contienen datos personales sensibles se procura que lleven un candado de acceso restringido.

1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

UNAM-España (Centro de Estudios Mexicanos)	
Identificador único	UNAM-España/archivo físico
(Nombre del sistema A5) *	Archivo físico
Datos personales (sensibles o no) contenidos en el sistema*:	Documentación administrativa emanada de las actividades académicas, culturales, de vinculación, y operación de la sede.
Responsable*:	
Nombre*:	Víctor Manuel Hernández Rivera
Cargo*:	Coordinador de Relaciones y Gestión
Funciones*:	Tramitar, concentrar y archivar la información y documentación administrativa emanada de las actividades académicas, culturales, de vinculación y de operación de la sede.
Obligaciones*:	-No compartir la información personal recabada con terceras personas, instituciones o empresas, sin la autorización de los interesados, y sólo cuando sea estrictamente necesario (por ejemplo, cuando la UNAM o las instituciones o empresas con las que se colabora solicitan datos de comunidad beneficiada de las actividades académicas y culturales de la sede) -Tratar la información con respeto.

2. ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

UNAM-España (Centro de Estudios Mexicanos)	
Identificador único¨*	UNAM-España/archivo físico
(Nombre del sistema A5*)	Archivo físico
Tipo de soporte:*	Físico
Descripción:*	Sistema físico de resguardo de información y documentación administrativa emanada de las actividades académicas, culturales, de vinculación y de operación de la sede.
Características del lugar donde se resguardan los soportes:*	La información y documentación se resguarda en carpetas, dentro de archiveros cerrados bajo llave, aislados, ignífugos y que se encuentran dentro de la oficina de la sede que a su vez está alojada en un edificio del Instituto Cervantes, vigilado mediante circuito cerrado, y al que se accede mediante llave y contraseña electrónica.

3. ANÁLISIS DE RIESGOS

UNAM-España (Centro de Estudios Mexicanos)		
Identificador único*	UNAM-España/archivo fisico	
(Nombre del sistema A5) *	Archivo físico	
Riesgo*	**Impacto***	**Mitigación***
- Que una persona ajena a la institución pueda acceder al edificio burlando las barreras de seguridad implementadas por el Instituto Cervantes, sede que aloja a UNAM-España y/o burlar las barreras de seguridad de los archivos	ALTO: Podrían acceder al histórico de archivos físicos administrativos de la sede	Mantener la máxima alerta de las personas que entren y salgan a la sede y mantener siempre bajo seguridad los archiveros y documentación. La información administrativa física se encuentra respaldada en archivo digital.

4. ANÁLISIS DE BRECHA

UNAM-España (Centro de Estudios Mexicanos)		
Identificador único*	UNAM-España/Archivo físico	
(Nombre del sistema A5) *	Archivo físico	
Medida de seguridad actual*	**Medida de seguridad necesaria***	**Acciones para remediación***
La documentación se mantiene resguardada bajo llave. Borrado seguro y destrucción de documentación física.	Seguir manteniendo y reforzando la seguridad en los archivos.	- Tener un protocolo en caso de que se vulneren las barreras de seguridad. - Seguir manteniendo y reforzando el respaldo periódico del archivo físico en digital.

5. PLAN DE TRABAJO

UNAM-España (Centro de Estudios Mexicanos)			
Identificador único*	UNAM-España/Archivofisico		
(Nombre del sistema A5) *	Archivo físico		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Diseño de protocolo de acciones contra la vulneración de datos del archivo físico. Política de escritorio limpio	Diseñar un protocolo de acciones en caso de que los datos personales del archivo físico sean vulnerados. Procurar que todo el staff de la sede gestione la documentación física a través de carpetas y archivos cerrados	1 semana Periódicamente	El protocolo permitirá seguir una ruta crítica en caso de que el archivo físico se vea en un escenario de vulneración. Procurar mantener bajo resguardo la información que se encuentre en soporte físico y que forme parte de la operación diaria de la oficina

6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

V. TRANSFERENCIAS DE DATOS PERSONALES

UNAM-España (Centro de Estudios Mexicanos)	
Identificador único*	UNAM-España/Archivo fisico
(Nombre del sistema A5)*	Archivo físico administrativo
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	La documentación que se transfiere se envía por mensajería, en paquete y sobre cerrado, etc.
Transferencias mediante el traslado de soportes electrónicos:	No se realizan trasferencias mediante traslados en soportes electrónicos
Transferencias mediante el traslado sobre redes electrónicas:	No se realizan transferencias mediante traslados sobre redes electrónicas.

VI. RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS

1.- Señalar las medidas de seguridad que ha implementado el área universitaria para el resguardo de los soportes físicos del sistema de manera que evite la alteración, pérdida o acceso no autorizado a los mismos.

La documentación se mantiene resguardada en carpetas y archiveros con cerradura, aislados, ignífugos y que se encuentran dentro de la oficina de la sede que a su vez está alojada en un piso del Instituto Cervantes, vigilado mediante circuito cerrado, y al que se accede mediante llave y contraseña electrónica. Las oficinas cuentan con sensor contra incendios con alarma.
Para el resguardo de la información que contienen las computadoras y el servidor se tiene instalación eléctrica del equipo de cómputo independiente de otras instalaciones, conexión de los equipos de cómputo a una toma de luz regulada, se cuenta con equipos de respaldo eléctrico (UPS, No break, planta de luz). A los equipos de cómputo se accede con contraseña de usuario.

El Servidor NAS cuenta en su interior con dos discos duros gemelos: uno de ellos almacena la información y el otro realiza automática y permanentemente un respaldo del primero. Adicionalmente, se programará un respaldo manual en un disco duro externo (cifrado), mismo que se resguardará en un lugar diferente y protegido. El NAS se encuentra físicamente en el despacho del secretario académico.

2.- Señalar en un listado las personas (nombre, cargo, funciones y obligaciones) que tienen acceso a los soportes físicos del sistema.

Las personas que tienen acceso al soporte físico del equipo de cómputo y NAS son las que laboran en la sede, detalladas en el punto I de este documento (Jorge Luis Volpi Escalante, Diego Celorio Morayta, Víctor Manuel Hernández Rivera, Adriana Suárez del Real Terrazas y Sandra Ortega García).

a. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

i. Los datos que se registran en las bitácoras:

c) Quién accede a los datos personales, fecha y hora en la que se realiza el acceso o se intenta el mismo, propósito del acceso, así como fecha y hora de salida;
d) Para soportes físicos: Número o clave del expediente utilizado, y
e) Para soportes electrónicos: Operaciones o acciones llevadas a cabo y registros utilizados de la base de datos.

6. Si las bitácoras están en soporte físico o en soporte electrónico;
7. Lugar dónde almacena las bitácoras y por cuánto tiempo;
8. La manera en que asegura la integridad de las bitácoras, y
9. Respecto del análisis de las bitácoras:

a) Quién es el responsable de analizarlas (si es el área universitaria o si es un tercero) y cada cuándo las analiza, y
b) Para el caso de que las bitácoras estén en soporte electrónico: las herramientas de análisis utilizadas.

No se realizan bitácoras de accesos y operación cotidiana, salvo para la salida y entrada de dispositivos como computadoras portátiles, o discos duros.

b. REGISTRO DE INCIDENTES:

La sede se encuentra en proceso de diseño de una bitácora de registro de incidentes, mismos que hasta la fecha no se han producido.

V. ACCESO A LAS INSTALACIONES

4. Seguridad perimetral exterior (las instalaciones del área universitaria):

La sede se encuentra albergada dentro de instalaciones del Instituto Cervantes, quién administra y realiza la supervisión de seguridad y control de acceso a las mismas. Se cuenta con circuito cerrado por fuera y dentro de las instalaciones y para acceder a las oficinas es necesario llave física y código de acceso.

5. Seguridad perimetral interior (oficina, almacén o bodega para soportes físicos, centro de datos para soportes electrónicos):

Las personas ajenas a la plantilla de la sede sólo tienen acceso al área de espera o a la sala de juntas, donde se les atiende. Los despachos están aislados tras puertas (sin cerraduras). Al estar albergados en instalaciones del Instituto Cervantes, se cuenta con personal de vigilancia, sistemas de video vigilancia y control mediante código de acceso. Para el área común donde se encuentra la sede, el personal de vigilancia se encarga de abrir y cerrar las instalaciones diariamente y de las labores de vigilancia, incluyendo monitoreo CCTV y alarma. Por último, la sede cuenta en cada oficina que la integra, archiveros con llave, mismas que resguarda cada usuario que integra la sede y su área de trabajo.

VI. ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

En este apartado se deberá establecer un mecanismo o procedimiento institucional para la actualización de la información personal contenida en el sistema, en donde se establezca la frecuencia con la que se efectúa y la forma en que se está solicitando al titular acreditar de manera idónea sus requerimientos de rectificación de datos inexactos.

Las medidas de seguridad previstas a continuación en los incisos VII al IX, sólo aplican para soportes electrónicos

VII. PERFILES DE USUARIO Y CONTRASEÑAS

En este rubro el área universitaria deberá describir el esquema de perfiles de usuario y contraseñas que tiene implementado para control de acceso mediante una red electrónica.

1. Modelo de control de acceso (alguno de los siguientes):

a) ¿Es obligatorio (etiquetas para objetos y acreditación para sujetos)?
b) ¿Es discrecional (matriz de control de acceso)?
c) ¿Está basado en roles (perfiles) o grupos?
d) ¿Está basado en reglas?

No se cuenta con información

2. Perfiles de usuario y contraseñas en el sistema operativo de red:

a) ¿Cuenta con un sistema operativo de red instalado en sus equipos?
b) ¿Proporciona dicho sistema operativo un manejo riguroso de perfiles de usuario y contraseñas?
c) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?

El único equipo de cómputo que cuenta con la conexión a un sistema operativo de red es el de la Coordinación de Relaciones y Gestión. La Red es *Team View* y accede a ella la Coordinación de

Relaciones y Asuntos Internacionales de la UNAM a solicitud expresa cuando se requiere documentación administrativa.

3. Perfiles de usuario y contraseñas manejados por el software aplicativo del sistema de tratamiento de datos personales:

a) ¿Ofrece dicho software un manejo riguroso de perfiles de usuario y contraseñas?
b) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?

No se cuenta con información

4. Administración de perfiles de usuario y contraseñas:

a) ¿Quién da de alta nuevos perfiles? El secretario académico
b) ¿Quién autoriza la creación de nuevos perfiles? El secretario académico
c) ¿Se lleva registro de la creación de nuevos perfiles? Sí

5. Acceso remoto al sistema de tratamiento de datos personales:

a) ¿Requieren los usuarios acceso remoto al equipo de cómputo que por lo general utilizan para trabajar con el sistema? Sí
b) ¿Requiere el administrador acceso remoto al equipo donde reside el sistema para realizar tareas de mantenimiento? Sí
c) ¿Cómo se evita el acceso remoto no autorizado? Mediante la solicitud de contraseña para acceder.

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

1. Señalar si realiza respaldos

a) Completos_X_, diferenciales ___ o incrementales___;
b) De forma automática _X___ o Manual ___X__, dependiendo el soporte
c) Periodicidad con que los realiza: en el NAS constante y en otros dispositivos y sistemas, cuando se requiera

2. El tipo de medios (por ejemplo: cintas magnéticas, discos duros, CD-ROM, entre otros) que utiliza para almacenar las copias de seguridad;
3. Cómo y dónde archiva esos medios, y
4. Quién es el responsable de realizar estas operaciones (el área universitaria o un tercero).

Se llevan a cabo respaldos completos de forma automática mediante el NAS y manual a través del Dropbox y archivo físico. El NAS lo hace constantemente y manualmente cada vez que termina una actividad y se transfieran los archivos del Dropbox al NAS. La documentación del archivo físico también se respalda en el NAS. Los encargados de realizar dichas operaciones son los miembros de las diferentes áreas de la sede: dirección, secretaría académica, coordinación de relaciones y gestión y secretaría técnica.

I

X. PLAN DE CONTINGENCIA

1. Presentar el plan de contingencia con el cual garantiza la continuidad de la operación del sistema o informar si no lo tiene, pero se encuentra desarrollándolo.
2. Si cuenta con plan de contingencia y lo ha implementado, deberá indicar si realiza pruebas de eficiencia de este.

3. Informar si cuenta con un sitio redundante (alterno) y señalar lo siguiente:

a) El tipo de sitio (caliente, tibio o frío);
b) Si el sitio es propio o subcontratado con un tercero;
c) Los procedimientos, el equipo y el personal que designa para poner en marcha tal sitio y
d) Tiempo que le lleva poner en marcha el sitio, según las pruebas de eficiencia.

La sede se encuentra desarrollando un plan de contingencia.

7. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

10.1. Herramientas y recursos para monitoreo de la protección de datos personales

Secretaría académica / secretaría técnica		
Identificador único*	UNAM España/Mailchimp	
(Nombre del sistema A1)*	Mailchimp	
Recurso*	**Descripción***	**Control***
Asignar o revocar los privilegios de acceso para los usuarios teniendo como base el principio del menor privilegio. Cambio periódico de contraseña Sistema de verificación en dos pasos Definir un plan y periodicidad de copia de seguridad de datos	Calendarización de cambio de contraseña de acceso a la plataforma Mailchimp. Activación del sistema de verificación en dos pasos Programar la realización de una copia de seguridad	Vigilar calendarización de cambios de contraseñas y asignación y revocación de privilegios. Revisar la calendarización y resguardo de datos. Vigilar la programación y calendarización de copia de seguridad

Secretaría académica/secretaría técnica		
Identificador único*	UNAM España/Carpeta proyectos	
(Nombre del sistema A2)*	Carpeta proyectos	
Recurso*	**Descripción***	**Control***
Cambio periódico de contraseña Copias de seguridad Actualización y mantenimiento de equipo y de sistema operativo del servidor Bloqueo y cierre de sesiones al servidor	Calendarización de cambio de contraseña de acceso a la plataforma NAS Realizar copias de seguridad periódicas de la información electrónica contenida en el NAS, utilizando un disco duro externo cifrado. Almacenar dicho respaldo en un lugar diferente, para que en caso de siniestro o robo no se pierda la información. En caso de requerirse, actualización y dar mantenimiento al equipo y sistema operativo del servidor Vigilar el bloqueo y sierre de sesiones del servidor	Revisar la calendarización Revisar la calendarización de las copias de seguridad Revisar si se producen cambios en la plantilla de la sede, se da de baja el acceso de aquellas personas que ya no laboran en ella. Calendarizar y revisar calendarización de mantenimiento de Servidor

Secretaría académica/secretaría técnica		
Identificador único*	UNAM España/Formularios google	
(Nombre del sistema A3)*	Formularios Google	
Recurso*	**Descripción***	**Control***
Cambio periódico de contraseña a plataforma Google Borrado seguro de formularios Programar un plan de respaldo de datos de formularios Bloqueo y cierre de sesión en cuentas Google	Utilizar una contraseña que incorpore mayor seguridad (mayúsculas, símbolos, números, etc.). Actualización periódica de la contraseña. Borrado de formularios una vez terminados de utilizar los datos durante los cursos. Respaldo de información que se resguarda Vigilar el cierre correcto de sesión en cada dispositivo desde el que se abra el formulario.	Revisar calendarización de cambio de contraseña Mantener sistema de verificación en pasos Revisar sistema de borrado seguro de Google Traslado de respaldo seguro a carpeta proyectos

Dirección, secretaría académica, coordinación de relaciones y gestión, secretaría técnica		
Identificador único*	UNAM España/correo institucional	
(Nombre del sistema A4)*	Correo electrónico institucional	
Recurso*	**Descripción***	**Control***
Cambio de contraseña Envío de información encriptada, restringida o cifrada Integración de aviso de privacidad en la firma	Utilizar una contraseña que incorpore mayor seguridad (mayúsculas, símbolos, números, etc.). Actualización periódica de la contraseña. Procurar enviar información sensible en mecanismos de encriptado o restricción.	Revisión de calendarización de cambio de contraseña Revisión de calendarización de integración de aviso de privacidad Revisión de aviso de privacidad en firmas del correo electrónico.

Coordinación de Relaciones y Gestión		
Identificador único*	UNAM España/archivo físico	
(Nombre del sistema A5)*	Archivo físico administrativo	
Recurso*	**Descripción***	**Control***
Mantener funcionando los sistemas de seguridad de entada y salida del edificio Mantener siempre bajo seguridad los archiveros y documentación. Respaldo del archivo físico a formato digital en archivo digital. Vigilar el mantenimiento de medidas de seguridad contra incendios	Aunque los sistemas de seguridad del edificio pertenecen al Instituto Cervantes (entidad que acoge a la sede de UNAM-España) la sede puede mantener la máxima alerta de las personas que entren y salgan a la sede Vigilar la seguridad de los archiveros Realizar respaldos periódicos del archivo físico	

10.2. Procedimiento para la revisión de las medidas de seguridad

(Denominación del área específica del Área Universitaria A)*		
Identificador único*		
(Nombre del sistema A1)*	**(Nombre del sistema A1)***	
Medida de seguridad*	**Procedimiento***	**Responsable***
Indique la medida de seguridad correspondiente al procedimiento de revisión. Agregue un renglón por cada medida.	*Indique el procedimiento para la revisión de la medida de seguridad, tales como comprobación de actualización, pruebas de penetración, revisión de estabilidad, etc.*	*Indicar:* *a) nombre del responsable del procedimiento* *b) tiempo máximo de ejecución en días.*

No se han llevado a cabo procedimientos para la revisión de las medidas de seguridad

10.3. Resultados de la evaluación y pruebas a las medidas de seguridad

(Denominación del área específica del Área Universitaria A)*		
Identificador único*		
(Nombre del sistema A1)*	**(Nombre del sistema A1)***	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***
Indique la medida de seguridad Agregue un renglón por cada medida.	*Indique el resultado de la evaluación de la medida de seguridad*	*Indicar:* *a) nombre del responsable de la evaluación* *b) fecha de conclusión.*

No se han llevado a cabo acciones de evaluación y pruebas a las medidas de seguridad

10.4. Acciones para la corrección y actualización de las medidas de seguridad

(Denominación del área específica del Área Universitaria A)*		
Identificador único*		
(Nombre del sistema A1)*	**(Nombre del sistema A1)***	
Medida de seguridad*	**Acciones***	**Responsable***
Indique la medida de seguridad (Agregue un renglón por cada medida).	*Indique las acciones aplicables para corregir o actualizar la medida de seguridad.* a) Precisar las acciones correctivas. b) Precisar las acciones preventivas.	*Indicar:* *a) nombre del responsable de las acciones* *b) fecha límite de conclusión.*

No se han llevado a cabo actividades para la corrección y actualización de las medidas de seguridad

11. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

11.1. Programa de capacitación a los responsables de tratamiento de datos personales

*(LLenar una tabla para cada sistema. Campos con * son obligatorios. Borrar instrucciones en cursivas)*

(Denominación del área específica del Área Universitaria A)*			
Identificador único*			
(Nombre del sistema A1)*	**(Nombre del sistema A1)***		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Indique actividad, tema, curso, material didáctico o recurso educativo para la capacitación. Agregar un renglón por cada elemento	*Describa el tipo de elemento, sus objetivos y forma de impartición, publicación o distribución*	*Indique duración del elemento en horas, días, meses, su fecha de inicio y de término*	*Mencione público objetivo, vigencia del elemento y frecuencia de actualización*

No se han llevado a cabo programas de capacitación a los responsables de tratamiento de datos personales

11.2. Programa de difusión de la protección a los datos personales

*(Llenar una tabla para cada sistema. Campos con * son obligatorios. Borrar instrucciones en cursivas)*

(Denominación del área específica del Área Universitaria A)*			
Identificador único*			
(Nombre del sistema A1)*	**(Nombre del sistema A1)***		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Indique actividad, tema, recursos para la difusión. Agregar un renglón por cada elemento	*Describa el tipo de elemento, sus objetivos y forma de impartición, publicación o distribución*	*Indique duración del elemento en horas, días, meses, su fecha de inicio y de término*	*Mencione público objetivo, vigencia del elemento y frecuencia de actualización*

No se han llevado a cabo programas de difusión de la protección a los datos personales

12. MEJORA CONTINUA

12.1. Actualización y mantenimiento de sistemas de información

*(Llenar una tabla para cada sistema. Campos con * son obligatorios. Borrar instrucciones en cursivas)*

(Denominación del área específica del Área Universitaria A)*			
Identificador único*			
(Nombre del sistema A1)*	**(Nombre del sistema A1)***		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Indique actividad. Agregar un renglón por cada elemento	*Describa el tipo de actividad, sus objetivos e impacto la actualización o mantenimiento del sistema de información*	*Indique duración en la ejecución de la actividad en horas, días, meses, su fecha de inicio y de término*	*Mencione los aspectos del sistema de información que son resueltos, total o parcialmente, por la actividad.*

La sede no ha llevado a cabo acciones de actualización y mantenimiento de sistemas de información

12.2. Actualización y mantenimiento de equipo de cómputo

Dirección, secretaría académica, coordinación de relaciones y gestión, secretaría técnica			
Identificador único*	Equipos de cómputo sede UNAM-España		
(Nombre del sistema A1)*			
Actividad*	**Descripción***	**Duración***	**Cobertura***
Calendarizar un programa de mantenimiento preventivo de equipo de cómputo y servidor	Programar el mantenimiento preventivo de los equipos de cómputo que contemple en caso de requerirse: - Cambio Sistema operativo -Actualizaciones de sistema -Instalación y/o actualización de antivirus y antimalware -Cambio de contraseñas de accesos a los equipos	La que estime el proveedor	Mantener el buen funcionamiento de los equipos de cómputo y proteger los sistemas que estos albergan.

12.3. Procesos para la conservación, preservación y respaldos de información

(Denominación del área específica del Área Universitaria A)*		
Identificador único*	UNAM España/carpeta proyectos	
(Nombre del sistema A2)*	Carpeta proyectos	
Proceso*	**Descripción***	**Responsable***
Proceso de respaldo de información Dropbox a NAS Proceso de respaldo de información en NAS	Al término de cada actividad académica y cultural se transfiere el archivo desde Dropbox a NAS. Servidor NAS realiza respaldos automáticos de información en un disco duro espejo.	Indicar: a) Diego Celorio, secretario académico b) Adriana Suárez del Real, secretaria técnica c) 2 días

12.4. Procesos de borrado seguro y disposición final de equipos y componentes informáticos

*(Llenar una tabla para cada sistema. Campos con * son obligatorios. Borrar instrucciones en cursivas)*

(Denominación del área específica del Área Universitaria A)*		
Identificador único*		
(Nombre del sistema A1)*	**(Nombre del sistema A1)***	
Proceso*	**Descripción***	**Responsable***
Indique el proceso en materia de borrado seguro, disposición final de equipos o componentes de cómputo. Agregue un renglón por proceso	*Describa el proceso en todas sus acciones.*	*Indicar:* *a) Nombre del responsable del proceso* *b) Tiempo máximo de ejecución en días.*

La sede no ha llevado a cabo procesos de borrado seguro salvo en momentos puntuales de duplicación de documentación física en que se utiliza una trituradora de documentos

13. PROCEDIMIENTO PARA LA CANCELACIÓN DE UN SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

(Informar y describir el procedimiento para la cancelación de un sistema de tratamiento de datos personales.)

P) DATOS DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES QUE SERÁ CANCELADO:

a) Denominación
b) Motivo de la cancelación

Q) PLAZOS Y CONDICIONES PARA EL BLOQUEO DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES:

(Señalar el periodo de bloqueo, considerando los plazos de prescripción para el ejercicio de algún derecho por parte de los titulares de conformidad con la normatividad de cada área universitaria. Asimismo, se debe señalar las condiciones y el procedimiento que se seguirá para realizar el bloqueo)

R) MEDIDAS DE SEGURIDAD PARA EL BLOQUEO Y POSTERIOR SUPRESIÓN DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES:
(Describir las medidas de seguridad aplicables al periodo de bloqueo y la supresión del sistema, considerando el nivel de protección requerido en virtud del tipo de datos personales contenidos en el sistema)

S) PROCEDIMIENTO PARA LA SUPRESIÓN DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

(Describir el procedimiento para suprimir el sistema, una vez cumplido el plazo de bloqueo)

T) MECANISMOS PARA LA SUPRESIÓN DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

(Describir las técnicas para la eliminación física del sistema)

La sede no ha llevado a cabo procedimientos para la supresión del sistema de tratamiento de datos personales

11. APROBACIÓN DEL DOCUMENTO DE SEGURIDAD

		Nombre y firma de quienes revisaron el presente documento:
Responsable del desarrollo:	Adriana Suárez del Real Terrazas Secretara técnica 915235176 adriana.suarez@cemespana.unam.mx	
Revisó:	Diego Celorio Morayta Secretario académico 915870230 dcelorio@unam.mx	
Autorizó:	Jorge Volpi Director 915870229 jvolpi@unam.mx	
Fecha de aprobación:	08/11/2022	

UNAM-REINO UNIDO

CENTRO DE ESTUDIOS MEXICANOS

1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

UNAM-Reino Unido	
Identificador único*	**Eventbrite**
(Nombre del sistema A1) *	**Eventbrite**
Datos personales (sensibles o no) contenidos en el sistema*:	Nombre completo Correo electrónico Género Ubicación geográfica
Responsable*:	
Nombre*:	Ana Elena González Treviño
Cargo*:	Directora, UNAM-Reino Unido
Funciones*:	Revisión de la traducción, estructura y diseño de la información descriptiva. Análisis de la información de la audiencia para fines estadísticos y de reportes.
Obligaciones*:	No difundir información de los datos personales. No modificar la información almacenada en el servidor. No hacer respaldos de la información de datos personales en el equipo personal.
	Encargados:
(Nombre del Encargado 1*)	Angélica Cruz Villamar
Cargo*:	Responsable TICs, UNAM-Reino Unido
Funciones*:	Recopilación de la información descriptiva del evento (Semblanzas, fotografías, artículos). Elaboración de formularios de registro para eventos en línea o presenciales. Análisis de la información de la audiencia para fines estadísticos y de reportes.
Obligaciones*:	No difundir información de los datos personales. No modificar la información almacenada en el servidor. No hacer respaldos de la información de datos personales en el equipo personal.
	Usuarios:
(Nombre del Usuario 1*)	Sara Massieu
Cargo*:	Responsable de diseño, UNAM-Reino Unido
Funciones*:	Ingresar la información descriptiva del evento (Semblanzas, fotografías, artículos). Elaboración del material de difusión e ilustrativos del portal de registro.
Obligaciones*:	No difundir información de los datos personales. No modificar la información almacenada en el servidor. No hacer respaldos de la información de datos personales en el equipo personal.

2. ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

UNAM-Reino Unido	
Identificador único¨*	Eventbrite
(Nombre del sistema A1*)	Eventbrite
Tipo de soporte:*	Soporte electrónico
Descripción:*	El registro de la información de usuarios se almacena en una base de datos.
Características del lugar donde se resguardan los soportes:*	Alojamiento en la nube privada del sistema con acceso restringido bajo usuario y contraseña. La información puede consultarse o descargada en formato PDF, XLM o CSV.

3. ANÁLISIS DE RIESGOS

UNAM-Reino Unido		
Identificador único*	Eventbrite	
(Nombre del sistema A1) *	Eventbrite	
Riesgo*	**Impacto***	**Mitigación***
Acceso no autorizado al sistema.	Acceso al sistema, consulta, modificación, robo o eliminación de la información y datos personales.	Cambio periódico de la contraseña del sistema mediante las políticas de clave secreta robusta.

ANÁLISIS DE BRECHA

UNAM-Reino Unido		
Identificador único*	Eventbrite	
(Nombre del sistema A1) *	Eventbrite	
Medida de seguridad actual*	**Medida de seguridad necesaria***	**Acciones para remediación***
Acceso al sistema mediante usuario y contraseña.	Correcta.	No es necesario.

PLAN DE TRABAJO

UNAM-Reino Unido			
Identificador único*	Eventbrite		
(Nombre del sistema A1)*	Eventbrite		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Registro de asistentes.	Los interesados a la actividad en línea o presencial se registran mediante el sistema ingresando nombre, correo electrónico y género.	El usuario cuenta con 10 minutos para ingresar los datos, de lo contrario, la sesión caduca.	El sistema solicita se acepten los Términos de servicio, las Pautas de la comunidad y la Política de privacidad de Eventbrite.

4. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

I. TRANSFERENCIAS DE DATOS PERSONALES

UNAM-Reino Unido	
Identificador único*	Eventbrite
(Nombre del sistema A1)*	Eventbrite
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	NA
Transferencias mediante el traslado de soportes electrónicos:	NA
Transferencias mediante el traslado sobre redes electrónicas:	NA

7. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

7.1 Herramientas y recursos para monitoreo de la protección de datos personales

UNAM-Reino Unido		
Identificador único*	Eventbrite	
(Nombre del sistema A1)*	Eventbrite	
Recurso*	**Descripción***	**Control***
Revisiones aleatorias.	Usuarios Administrador, Editor. Usuario y contraseña.	Responsable técnico.

7.2 Procedimiento para la revisión de las medidas de seguridad

UNAM-Reino Unido		
Identificador único*	Eventbrite	
(Nombre del sistema A1)*	Eventbrite	
Medida de seguridad*	**Procedimiento***	**Responsable***
Sistema actualizado. Acceso restringido.	Comprobante de actualización. Asignación de roles.	Responsables técnicos.

7.3 Resultados de la evaluación y pruebas a las medidas de seguridad

UNAM-Reino Unido		
Identificador único*	Eventbrite	
(Nombre del sistema A1)*	Eventbrite	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***
N/A	N/A	N/A

7.4 Acciones para la corrección y actualización de las medidas de seguridad

UNAM-Reino Unido		
Identificador único*	Eventbrite	
(Nombre del sistema A1)*	Eventbrite	
Medida de seguridad*	**Acciones***	**Responsable***
N/A	N/A	N/A

8. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

8.1 Programa de capacitación a los responsables de tratamiento de datos personales

UNAM-Reino Unido			
Identificador único*	Eventbrite		
(Nombre del sistema A1)*	Eventbrite		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Cursos de capacitación en línea.	Red de Responsables TIC UNAM	Sin fechas fijas.	Comunidad UNAM.

8.2 Programa de difusión de la protección a los datos personales

UNAM-Reino Unido			
Identificador único*	Eventbrite		
(Nombre del sistema A1)*	Eventbrite		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Cursos de capacitación en línea.	Red de Responsables TIC UNAM	Sin fechas fijas.	Comunidad UNAM.

MEJORA CONTINUA

8.3 Actualización y mantenimiento de sistemas de información

UNAM-Reino Unido			
Identificador único*	Eventbrite		
(Nombre del sistema A1)*	Eventbrite		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Actualización y mantenimiento del sistema.	Actividad interna.	Sin fecha fija.	Procedimiento de desarrollares.

8.4 Actualización y mantenimiento de equipo de cómputo

UNAM-Reino Unido			
Identificador único*	Eventbrite		
(Nombre del sistema A1)*	Eventbrite		
Actividad*	**Descripción***	**Duración***	**Cobertura***
N/A	N/A	N/A	N/A

8.5 Procesos para la conservación, preservación y respaldos de información

UNAM-Reino Unido		
Identificador único*	Eventbrite	
(Nombre del sistema A1)*	Eventbrite	
Proceso*	**Descripción***	**Responsable***
Banco de datos del sistema.	Procedimiento interno.	Responsables técnicos.

8.6 Procesos de borrado seguro y disposición final de equipos y componentes informáticos

UNAM-Reino Unido		
Identificador único*	Eventbrite	
(Nombre del sistema A1)*	Eventbrite	
Proceso*	**Descripción***	**Responsable***
N/A	N/A	N/A

MAILCHIMP

1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

UNAM-Reino Unido	
Identificador único*	**Mailchimp**
(Nombre del sistema A1) *	**Mailchimp**
Datos personales (sensibles o no) contenidos en el sistema*:	Correo electrónico Nombre completo Género Ubicación geográfica Intereses
Responsable*:	
Nombre*:	Ana Elena González Treviño
Cargo*:	Directora, UNAM-Reino Unido
Funciones*:	Revisión de la traducción, estructura y diseño del boletín. Análisis de la información de los suscriptores para fines estadísticos y de reportes.
Obligaciones*:	No difundir información de los datos personales. No modificar la información almacenada en el servidor. No hacer respaldos de la información de datos personales en el equipo personal.
	Encargados:
(Nombre del Encargado 1*)	Angélica Cruz Villamar
Cargo*:	Responsable TICs, UNAM-Reino Unido
Funciones*:	Elaboración del boletín informativo para eventos en línea o presenciales. Análisis de la información de los suscriptores para fines estadísticos y de reportes.
Obligaciones*:	No difundir información de los datos personales. No modificar la información almacenada en el servidor. No hacer respaldos de la información de datos personales en el equipo personal.

2. ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

UNAM-Reino Unido	
Identificador único*	Mailchimp
(Nombre del sistema A1*)	Mailchimp
Tipo de soporte:*	Soporte electrónico
Descripción:*	El registro de la información de los suscriptores se almacena en una base de datos.
Características del lugar donde se resguardan los soportes:*	Alojamiento en la nube privada del sistema con acceso restringido bajo usuario y contraseña. La información puede consultarse o descargada en formato CSV.

3. ANÁLISIS DE RIESGOS

UNAM-Reino Unido		
Identificador único*	Mailchimp	
(Nombre del sistema A1) *	Mailchimp	
Riesgo*	**Impacto***	**Mitigación***
Acceso no autorizado al sistema.	Acceso al sistema, consulta, modificación, robo o eliminación de la información y datos personales.	Cambio periódico de la contraseña del sistema mediante las políticas de clave secreta robusta.

4. ANÁLISIS DE BRECHA

UNAM-Reino Unido		
Identificador único*	Mailchimp	
(Nombre del sistema A1) *	Mailchimp	
Medida de seguridad actual*	**Medida de seguridad necesaria***	**Acciones para remediación***
Acceso al sistema mediante usuario y contraseña.	Correcta.	No es necesario.

PLAN DE TRABAJO

UNAM-Reino Unido			
Identificador único*	Mailchimp		
(Nombre del sistema A1)*	Mailchimp		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Suscripción al boletín.	Los interesados en recibir periódicamente el boletín se registran mediante el sistema ingresando correo electrónico, nombre, género e intereses.	El usuario debe aceptar el correo de confirmación, de lo contrario no se realiza el registro.	El sistema muestra el acceso para la consultar las políticas de privacidad del manejo de datos.

5. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

I. TRANSFERENCIAS DE DATOS PERSONALES

UNAM-Reino Unido	
Identificador único*	Mailchimp
(Nombre del sistema A1)*	Mailchimp
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	NA
Transferencias mediante el traslado de soportes electrónicos:	NA
Transferencias mediante el traslado sobre redes electrónicas:	NA

7. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

7.1 Herramientas y recursos para monitoreo de la protección de datos personales

UNAM-Reino Unido		
Identificador único*	Mailchimp	
(Nombre del sistema A1)*	Mailchimp	
Recurso*	**Descripción***	**Control***
Revisiones aleatorias.	Usuarios Administrador. Usuario y contraseña.	Responsable técnico.

7.2 Procedimiento para la revisión de las medidas de seguridad

UNAM-Reino Unido		
Identificador único*	Mailchimp	
(Nombre del sistema A1)*	Mailchimp	
Medida de seguridad*	**Procedimiento***	**Responsable***
Sistema actualizado. Acceso restringido.	Comprobante de actualización. Asignación de roles.	Responsables técnicos.

7.3 Resultados de la evaluación y pruebas a las medidas de seguridad

UNAM-Reino Unido		
Identificador único*	Mailchimp	
(Nombre del sistema A1)*	Mailchimp	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***
N/A	N/A	N/A

7.4 Acciones para la corrección y actualización de las medidas de seguridad

UNAM-Reino Unido		
Identificador único*	Mailchimp	
(Nombre del sistema A1)*	Mailchimp	
Medida de seguridad*	**Acciones***	**Responsable***
N/A	N/A	N/A

8. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

8.1 Programa de capacitación a los responsables de tratamiento de datos personales

UNAM-Reino Unido			
Identificador único*	Mailchimp		
(Nombre del sistema A1)*	Mailchimp		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Cursos de capacitación en línea.	Red de Responsables TIC UNAM	Sin fechas fijas.	Comunidad UNAM.

8.2 Programa de difusión de la protección a los datos personales

UNAM-Reino Unido			
Identificador único*	Mailchimp		
(Nombre del sistema A1)*	Mailchimp		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Cursos de capacitación en línea.	Red de Responsables TIC UNAM	Sin fechas fijas.	Comunidad UNAM.

9. MEJORA CONTINUA

9.1 Actualización y mantenimiento de sistemas de información

UNAM-Reino Unido			
Identificador único*	Mailchimp		
(Nombre del sistema A1)*	Mailchimp		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Actualización y mantenimiento del sistema.	Actividad interna.	Sin fecha fija.	Procedimiento de desarrollares.

9.2 Actualización y mantenimiento de equipo de cómputo

UNAM-Reino Unido			
Identificador único*	Mailchimp		
(Nombre del sistema A1)*	Mailchimp		
Actividad*	**Descripción***	**Duración***	**Cobertura***
N/A	N/A	N/A	N/A

9.3 Procesos para la conservación, preservación y respaldos de información

UNAM-Reino Unido		
Identificador único*	Mailchimp	
(Nombre del sistema A1)*	Mailchimp	
Proceso*	**Descripción***	**Responsable***
Banco de datos del sistema.	Procedimiento interno.	Responsables técnicos.

9.4 Procesos de borrado seguro y disposición final de equipos y componentes informáticos

UNAM-Reino Unido		
Identificador único*	Mailchimp	
(Nombre del sistema A1)*	Mailchimp	
Proceso*	**Descripción***	**Responsable***
N/A	N/A	N/A

GOOGLE FORM

1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

UNAM-Reino Unido	
Identificador único*	**Google Forms**
(Nombre del sistema A1) *	**Google Forms para pre-registro Verano Puma**
Datos personales (sensibles o no) contenidos en el sistema*:	Nombre completo Correo electrónico Fecha de nacimiento Teléfono celular Nivel escolar e institución Certificado de inglés
Responsable*:	
Nombre*:	Ana Elena González Treviño
Cargo*:	Directora, UNAM-Reino Unido
Funciones*:	Revisión del perfil del interesado. Análisis de la información de los pre-registrados para fines estadísticos y de reportes.
Obligaciones*:	No difundir información de los datos personales. No modificar la información almacenada en el servidor. No hacer respaldos de la información de datos personales en el equipo personal.
	Encargados:
(Nombre del Encargado 1*)	Angélica Cruz Villamar
Cargo*:	Responsable TICs, UNAM-Reino Unido
Funciones*:	Elaboración del formulario de pre-registro para el curso de lingüística y cultural Verano Puma. Contactar a los interesados y compartir información de la convocatoria. Análisis de la información de los pre-registrados para fines estadísticos y de reportes.
Obligaciones*:	No difundir información de los datos personales. No modificar la información almacenada en el servidor. No hacer respaldos de la información de datos personales en el equipo personal.

2. ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

UNAM-Reino Unido	
Identificador único¨*	Google Forms
(Nombre del sistema A1*)	Google Forms para pre-registro Verano Puma
Tipo de soporte:*	Soporte electrónico
Descripción:*	El registro de la información de usuarios se almacena en una base de datos.
Características del lugar donde se resguardan los soportes:*	Alojamiento en la nube privada del sistema con acceso restringido bajo usuario y contraseña. La información puede consultarse o descargada en formato PDF, XLM o CSV.

3. ANÁLISIS DE RIESGOS

UNAM-Reino Unido		
Identificador único*	Google Forms	
(Nombre del sistema A1) *	Google Forms para pre-registro Verano Puma	
Riesgo*	**Impacto***	**Mitigación***
Acceso no autorizado al sistema.	Acceso al sistema, consulta, modificación, robo o eliminación de la información y datos personales.	Cambio periódico de la contraseña del sistema mediante las políticas de clave secreta robusta.

4. ANÁLISIS DE BRECHA

UNAM-Reino Unido		
Identificador único*	Google Forms	
(Nombre del sistema A1) *	Google Forms para pre-registro Verano Puma	
Medida de seguridad actual*	**Medida de seguridad necesaria***	**Acciones para remediación***
Acceso al sistema mediante usuario y contraseña.	Correcta.	No es necesario.

PLAN DE TRABAJO

UNAM-Reino Unido			
Identificador único*	Google Forms		
(Nombre del sistema A1)*	Google Forms para pre-registro Verano Puma		
Actividad*	**Descripción***	**Duración***	**Cobertura***
El usuario realiza el pre-registro.	Los interesados al curso Verano Puma ingresan los datos solicitados mediante el formulario.	Los interesados pueden realizar la actividad durante el periodo de la convocatoria activa.	Los datos son almacenados en una base de datos con acceso restringido.

6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

I. TRANSFERENCIAS DE DATOS PERSONALES

UNAM-Reino Unido	
Identificador único*	Google Forms
(Nombre del sistema A1)*	Google Forms para pre-registro Verano Puma
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	NA
Transferencias mediante el traslado de soportes electrónicos:	NA
Transferencias mediante el traslado sobre redes electrónicas:	NA

7. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

7.1 Herramientas y recursos para monitoreo de la protección de datos personales

UNAM-Reino Unido		
Identificador único*	Google Forms	
(Nombre del sistema A1)*	Google Forms para pre-registro Verano Puma	
Recurso*	**Descripción***	**Control***
Revisiones aleatorias.	Usuarios Administrador, Editor y Lector. Usuario y contraseña.	Responsable técnico.

7.2 Procedimiento para la revisión de las medidas de seguridad

UNAM-Reino Unido		
Identificador único*	Google Forms	
(Nombre del sistema A1)*	Google Forms para pre-registro Verano Puma	
Medida de seguridad*	**Procedimiento***	**Responsable***
Sistema actualizado. Acceso restringido.	Comprobante de actualización. Asignación de roles.	Responsables técnicos.

7.3 Resultados de la evaluación y pruebas a las medidas de seguridad

UNAM-Reino Unido		
Identificador único*	Google Forms	
(Nombre del sistema A1)*	Google Forms para pre-registro Verano Puma	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***
N/A	N/A	N/A

7.4 Acciones para la corrección y actualización de las medidas de seguridad

UNAM-Reino Unido		
Identificador único*	Google Forms	
(Nombre del sistema A1)*	Google Forms para pre-registro Verano Puma	
Medida de seguridad*	**Acciones***	**Responsable***
N/A	N/A	N/A

8. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

8.1 Programa de capacitación a los responsables de tratamiento de datos personales

UNAM-Reino Unido			
Identificador único*	Google Forms		
(Nombre del sistema A1)*	Google Forms para pre-registro Verano Puma		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Cursos de capacitación en línea.	Red de Responsables TIC UNAM	Sin fechas fijas.	Comunidad UNAM.

8.2 Programa de difusión de la protección a los datos personales

UNAM-Reino Unido			
Identificador único*	Google Forms		
(Nombre del sistema A1)*	Google Forms para pre-registro Verano Puma		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Cursos de capacitación en línea.	Red de Responsables TIC UNAM	Sin fechas fijas.	Comunidad UNAM.

9. MEJORA CONTINUA

9.1 Actualización y mantenimiento de sistemas de información

UNAM-Reino Unido			
Identificador único*	Google Forms		
(Nombre del sistema A1)*	Google Forms para pre-registro Verano Puma		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Actualización y mantenimiento del sistema.	Actividad interna.	Sin fecha fija.	Procedimiento de desarrollares.

9.2 Actualización y mantenimiento de equipo de cómputo

UNAM-Reino Unido			
Identificador único*	Google Forms		
(Nombre del sistema A1)*	Google Forms para pre-registro Verano Puma		
Actividad*	**Descripción***	**Duración***	**Cobertura***
N/A	N/A	N/A	N/A

9.3 Procesos para la conservación, preservación y respaldos de información

UNAM-Reino Unido		
Identificador único*	Google Forms	
(Nombre del sistema A1)*	Google Forms para pre-registro Verano Puma	
Proceso*	**Descripción***	**Responsable***
Banco de datos del sistema.	Procedimiento interno.	Responsables técnicos.

9.4 Procesos de borrado seguro y disposición final de equipos y componentes informáticos

UNAM-Reino Unido		
Identificador único*	Google Forms	
(Nombre del sistema A1)*	Google Forms para pre-registro Verano Puma	
Proceso*	**Descripción***	**Responsable***
N/A	N/A	N/A

KING'S APPLY

1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

UNAM-Reino Unido	
Identificador único*	**King's Apply**
(Nombre del sistema A1) *	**King's Apply de King's College London**
Datos personales (sensibles o no) contenidos en el sistema*:	Nombre completo Correo electrónico Género Fecha de nacimiento País de nacimiento Nacionalidad Dirección Teléfono Datos de pasaporte Origen étnico Nivel de estudios e institución Certificado de inglés
Responsable*:	
Nombre*:	Fahema Ettoubi
Cargo*:	Academic Services, King's College London
Funciones*:	Revisión de los formularios de postulación de los estudiantes. Análisis de la información de los estudiantes para fines estadísticos y de reportes.
Obligaciones*:	No difundir información de los datos personales. No modificar la información almacenada en el servidor. No hacer respaldos de la información de datos personales en el equipo personal.

2. ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

UNAM-Reino Unido	
Identificador único¨*	King's Apply
(Nombre del sistema A1*)	King's Apply de King's College London
Tipo de soporte:*	Soporte electrónico
Descripción:*	El registro de la información de usuarios se almacena en una base de datos.
Características del lugar donde se resguardan los soportes:*	Alojamiento en la nube privada del sistema con acceso restringido bajo usuario y contraseña. La información puede consultarse o descargarse.

3. ANÁLISIS DE RIESGOS

UNAM-Reino Unido		
Identificador único*	King’s Apply	
(Nombre del sistema A1) *	King’s Apply de King’s College London	
Riesgo*	**Impacto***	**Mitigación***
Acceso no autorizado al sistema.	Acceso al sistema, consulta, modificación, robo o eliminación de la información y datos personales.	Cambio periódico de la contraseña del sistema mediante las políticas de clave secreta robusta.

4. ANÁLISIS DE BRECHA

UNAM-Reino Unido		
Identificador único*	King’s Apply	
(Nombre del sistema A1) *	King’s Apply de King’s College London	
Medida de seguridad actual*	**Medida de seguridad necesaria***	**Acciones para remediación***
Acceso al sistema mediante usuario y contraseña.	Correcta.	No es necesario.

PLAN DE TRABAJO

UNAM-Reino Unido			
Identificador único*	King’s Apply		
(Nombre del sistema A1)*	King’s Apply de King’s College London		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Inscripción de los estudiantes.	Los estudiantes envían la postulación al curso ingresando los datos solicitados.	Los interesados pueden realizar la actividad durante el periodo de la convocatoria activa.	El sistema solicita se acepten los Términos de servicio, las Pautas de la comunidad y la Política de privacidad de King’s College London.

7. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

I. TRANSFERENCIAS DE DATOS PERSONALES

UNAM-Reino Unido	
Identificador único*	King’s Apply
(Nombre del sistema A1)*	King’s Apply de King’s College London
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	NA
Transferencias mediante el traslado de soportes electrónicos:	NA
Transferencias mediante el traslado sobre redes electrónicas:	NA

7. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

7.1 Herramientas y recursos para monitoreo de la protección de datos personales

UNAM-Reino Unido		
Identificador único*	King's Apply	
(Nombre del sistema A1)*	King's Apply de King's College London	
Recurso*	**Descripción***	**Control***
Revisiones aleatorias.	Usuarios Administrador, Editor. Usuario y contraseña.	Responsable técnico.

7.2 Procedimiento para la revisión de las medidas de seguridad

UNAM-Reino Unido		
Identificador único*	King's Apply	
(Nombre del sistema A1)*	King's Apply de King's College London	
Medida de seguridad*	**Procedimiento***	**Responsable***
Sistema actualizado. Acceso restringido.	Comprobante de actualización. Asignación de roles.	Responsables técnicos.

7.3 Resultados de la evaluación y pruebas a las medidas de seguridad

UNAM-Reino Unido		
Identificador único*	King's Apply	
(Nombre del sistema A1)*	King's Apply de King's College London	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***
N/A	N/A	N/A

7.4 Acciones para la corrección y actualización de las medidas de seguridad

UNAM-Reino Unido		
Identificador único*	King's Apply	
(Nombre del sistema A1)*	King's Apply de King's College London	
Medida de seguridad*	**Acciones***	**Responsable***
N/A	N/A	N/A

8. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

8.1 Programa de capacitación a los responsables de tratamiento de datos personales

UNAM-Reino Unido			
Identificador único*	King's Apply		
(Nombre del sistema A1)*	King's Apply de King's College London		
Actividad*	**Descripción***	**Duración***	**Cobertura***
NA	NA	NA	NA

8.2 Programa de difusión de la protección a los datos personales

UNAM-Reino Unido			
Identificador único*	King's Apply		
(Nombre del sistema A1)*	King's Apply de King's College London		
Actividad*	**Descripción***	**Duración***	**Cobertura***
NA	NA	NA	NA

9. MEJORA CONTINUA

9.1 Actualización y mantenimiento de sistemas de información

UNAM-Reino Unido			
Identificador único*	King’s Apply		
(Nombre del sistema A1)*	King’s Apply de King’s College London		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Actualización y mantenimiento del sistema.	Actividad interna.	Sin fecha fija.	Procedimiento de desarrollares.

9.2 Actualización y mantenimiento de equipo de cómputo

UNAM-Reino Unido			
Identificador único*	King’s Apply		
(Nombre del sistema A1)*	King’s Apply de King’s College London		
Actividad*	**Descripción***	**Duración***	**Cobertura***
N/A	N/A	N/A	N/A

9.3 Procesos para la conservación, preservación y respaldos de información

UNAM-Reino Unido		
Identificador único*	King’s Apply	
(Nombre del sistema A1)*	King’s Apply de King’s College London	
Proceso*	**Descripción***	**Responsable***
Banco de datos del sistema.	Procedimiento interno de King’s College London.	Responsables técnicos.

9.4 Procesos de borrado seguro y disposición final de equipos y componentes informáticos

UNAM-Reino Unido		
Identificador único*	King’s Apply	
(Nombre del sistema A1)*	King’s Apply de King’s College London	
Proceso*	**Descripción***	**Responsable***
N/A	N/A	N/A

1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

UNAM-Reino Unido	
Identificador único*	**IRIS**
(Nombre del sistema A1) *	**IRIS (Sistema de Gestión de Servicio Social, FES Acatlán)**
Datos personales (sensibles o no) contenidos en el sistema*:	Número de cuenta Nombre Carrera
Responsable*:	
Nombre*:	Adriana Roque del Ángel
Cargo*:	Jefa del Departamento de Servicio Social, FES Acatlán
Funciones*:	Revisión y autorización del Alta del alumno. Revisión y autorización de Liberación del alumno. Análisis de la información de los estudiantes para fines estadísticos y de reportes.
Obligaciones*:	No difundir información de los datos personales. No modificar la información almacenada en el servidor. No hacer respaldos de la información de datos personales en el equipo personal.
	Encargados:
(Nombre del Encargado 1*)	Ana Elena González Treviño
Cargo*:	Directora, UNAM-Reino Unido
Funciones*:	Alta de alumnos. Liberación del alumno mediante Carta de finalización. Análisis de la información de los estudiantes para fines estadísticos y de reportes.
Obligaciones*:	No difundir información de los datos personales. No modificar la información almacenada en el servidor. No hacer respaldos de la información de datos personales en el equipo personal.

2. ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

UNAM-Reino Unido	
Identificador único¨*	IRIS
(Nombre del sistema A1*)	IRIS (Sistema de Gestión de Servicio Social, FES Acatlán)
Tipo de soporte:*	Soporte electrónico
Descripción:*	El registro de la información de usuarios se almacena en una base de datos.
Características del lugar donde se resguardan los soportes:*	Alojamiento en la nube privada del sistema con acceso restringido bajo usuario y contraseña. La información puede consultarse.

3. ANÁLISIS DE RIESGOS

UNAM-Reino Unido		
Identificador único*	IRIS	
(Nombre del sistema A1) *	IRIS (Sistema de Gestión de Servicio Social, FES Acatlán)	
Riesgo*	**Impacto***	**Mitigación***
Acceso no autorizado al sistema.	Acceso al sistema, consulta, modificación, robo o eliminación de la información y datos personales.	Cambio periódico de la contraseña del sistema mediante las políticas de clave secreta robusta.

4. ANÁLISIS DE BRECHA

UNAM-Reino Unido		
Identificador único*	IRIS	
(Nombre del sistema A1) *	IRIS (Sistema de Gestión de Servicio Social, FES Acatlán)	
Medida de seguridad actual*	**Medida de seguridad necesaria***	**Acciones para remediación***
Acceso al sistema mediante usuario y contraseña.	Correcta.	No es necesario.

PLAN DE TRABAJO

UNAM-Reino Unido			
Identificador único*	IRIS		
(Nombre del sistema A1)*	IRIS (Sistema de Gestión de Servicio Social, FES Acatlán)		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Alta, baja, liberación del alumno.	El responsable ingresa al sistema para la actividad.	Cualquier actividad debe realizarse en el periodo de servicio social del alumno.	Los datos son almacenados en una base de datos con acceso restringido.

8. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

I. TRANSFERENCIAS DE DATOS PERSONALES

UNAM-Reino Unido	
Identificador único*	IRIS
(Nombre del sistema A1)*	IRIS (Sistema de Gestión de Servicio Social, FES Acatlán)
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	NA
Transferencias mediante el traslado de soportes electrónicos:	NA
Transferencias mediante el traslado sobre redes electrónicas:	NA

7. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

7.1 Herramientas y recursos para monitoreo de la protección de datos personales

UNAM-Reino Unido		
Identificador único*	IRIS	
(Nombre del sistema A1)*	IRIS (Sistema de Gestión de Servicio Social, FES Acatlán)	
Recurso*	**Descripción***	**Control***
Revisiones aleatorias.	Usuarios Administrador. Usuario y contraseña.	Responsable técnico.

7.2 Procedimiento para la revisión de las medidas de seguridad

UNAM-Reino Unido		
Identificador único*	IRIS	
(Nombre del sistema A1)*	IRIS (Sistema de Gestión de Servicio Social, FES Acatlán)	
Medida de seguridad*	**Procedimiento***	**Responsable***
Sistema actualizado. Acceso restringido.	Comprobante de actualización. Asignación de roles.	Responsables técnicos.

7.3 Resultados de la evaluación y pruebas a las medidas de seguridad

UNAM-Reino Unido		
Identificador único*	IRIS	
(Nombre del sistema A1)*	IRIS (Sistema de Gestión de Servicio Social, FES Acatlán)	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***
N/A	N/A	N/A

7.4 Acciones para la corrección y actualización de las medidas de seguridad

UNAM-Reino Unido		
Identificador único*	IRIS	
(Nombre del sistema A1)*	IRIS (Sistema de Gestión de Servicio Social, FES Acatlán)	
Medida de seguridad*	**Acciones***	**Responsable***
N/A	N/A	N/A

8. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

8.1 Programa de capacitación a los responsables de tratamiento de datos personales

UNAM-Reino Unido			
Identificador único*	IRIS		
(Nombre del sistema A1)*	IRIS (Sistema de Gestión de Servicio Social, FES Acatlán)		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Cursos de capacitación en línea.	Red de Responsables TIC UNAM	Sin fechas fijas.	Comunidad UNAM.

8.2 Programa de difusión de la protección a los datos personales

UNAM-Reino Unido			
Identificador único*	IRIS		
(Nombre del sistema A1)*	IRIS (Sistema de Gestión de Servicio Social, FES Acatlán)		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Cursos de capacitación en línea.	Red de Responsables TIC UNAM	Sin fechas fijas.	Comunidad UNAM.

9. MEJORA CONTINUA

9.1 Actualización y mantenimiento de sistemas de información

UNAM-Reino Unido			
Identificador único*	IRIS		
(Nombre del sistema A1)*	IRIS (Sistema de Gestión de Servicio Social, FES Acatlán)		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Actualización y mantenimiento del sistema.	Actividad interna.	Sin fecha fija.	Procedimiento de desarrollares.

9.2 Actualización y mantenimiento de equipo de cómputo

UNAM-Reino Unido			
Identificador único*	IRIS		
(Nombre del sistema A1)*	IRIS (Sistema de Gestión de Servicio Social, FES Acatlán)		
Actividad*	**Descripción***	**Duración***	**Cobertura***
N/A	N/A	N/A	N/A

9.3 Procesos para la conservación, preservación y respaldos de información

UNAM-Reino Unido		
Identificador único*	IRIS	
(Nombre del sistema A1)*	IRIS (Sistema de Gestión de Servicio Social, FES Acatlán)	
Proceso*	**Descripción***	**Responsable***
Banco de datos del sistema.	Procedimiento interno de FES Acatlán.	Responsables técnicos.

9.4 Procesos de borrado seguro y disposición final de equipos y componentes informáticos

UNAM-Reino Unido		
Identificador único*	IRIS	
(Nombre del sistema A1)*	IRIS (Sistema de Gestión de Servicio Social, FES Acatlán)	
Proceso*	**Descripción***	**Responsable***
N/A	N/A	N/A

ZOOM

1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

UNAM-Reino Unido	
Identificador único*	**ZOOM**
(Nombre del sistema A1) *	**ZOOM (Reportes)**
Datos personales (sensibles o no) contenidos en el sistema*:	Nombre del usuario Correo electrónico
Responsable*:	
Nombre*:	Ana Elena González Treviño
Cargo*:	Directora, UNAM-Reino Unido
Funciones*:	Programación de reuniones. Análisis de la información de la audiencia para fines estadísticos y de reportes.
Obligaciones*:	No difundir información de los datos personales. No modificar la información almacenada en el servidor. No hacer respaldos de la información de datos personales en el equipo personal.
	Encargados:
(Nombre del Encargado 1*)	Angélica Cruz Villamar
Cargo*:	Responsable TICs, UNAM-Reino Unido
Funciones*:	Programación de reuniones. Análisis de la información de la audiencia para fines estadísticos y de reportes.
Obligaciones*:	No difundir información de los datos personales. No modificar la información almacenada en el servidor. No hacer respaldos de la información de datos personales en el equipo personal.

2. ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

UNAM-Reino Unido	
Identificador único*	ZOOM
(Nombre del sistema A1*)	ZOOM (Reportes)
Tipo de soporte:*	Soporte electrónico
Descripción:*	El registro de la información de usuarios se almacena en una base de datos.
Características del lugar donde se resguardan los soportes:*	Alojamiento en la nube privada del sistema con acceso restringido bajo usuario y contraseña. La información puede consultarse o descargada en CSV.

3. ANÁLISIS DE RIESGOS

UNAM-Reino Unido		
Identificador único*	ZOOM	
(Nombre del sistema A1) *	ZOOM (Reportes)	
Riesgo*	**Impacto***	**Mitigación***
Acceso no autorizado al sistema.	Acceso al sistema, consulta, modificación, robo o eliminación de la información y datos personales.	Cambio periódico de la contraseña del sistema mediante las políticas de clave secreta robusta.

4. ANÁLISIS DE BRECHA

UNAM-Reino Unido		
Identificador único*	ZOOM	
(Nombre del sistema A1) *	ZOOM (Reportes)	
Medida de seguridad actual*	**Medida de seguridad necesaria***	**Acciones para remediación***
Acceso al sistema mediante usuario y contraseña.	Correcta.	No es necesario.

PLAN DE TRABAJO

UNAM-Reino Unido			
Identificador único*	ZOOM		
(Nombre del sistema A1)*	ZOOM (Reportes)		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Asistencia de usuarios.	Los usuarios asisten a los eventos online y el sistema registra la información de los participantes en la sala.	De acuerdo a la duración del evento.	El sistema solicita se acepten los Términos de servicio, las Pautas de la comunidad y la Política de privacidad de Zoom.

9. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

I. TRANSFERENCIAS DE DATOS PERSONALES

UNAM-Reino Unido	
Identificador único*	ZOOM
(Nombre del sistema A1)*	ZOOM (Reportes)
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	NA
Transferencias mediante el traslado de soportes electrónicos:	NA
Transferencias mediante el traslado sobre redes electrónicas:	NA

7. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

7.1 Herramientas y recursos para monitoreo de la protección de datos personales

UNAM-Reino Unido		
Identificador único*	ZOOM	
(Nombre del sistema A1)*	ZOOM (Reportes)	
Recurso*	**Descripción***	**Control***
Revisiones aleatorias.	Usuarios Administrador, Editor. Usuario y contraseña.	Responsable técnico.

7.2 Procedimiento para la revisión de las medidas de seguridad

UNAM-Reino Unido		
Identificador único*	ZOOM	
(Nombre del sistema A1)*	ZOOM (Reportes)	
Medida de seguridad*	**Procedimiento***	**Responsable***
Sistema actualizado. Acceso restringido.	Comprobante de actualización. Asignación de roles.	Responsables técnicos.

7.3 Resultados de la evaluación y pruebas a las medidas de seguridad

UNAM-Reino Unido		
Identificador único*	ZOOM	
(Nombre del sistema A1)*	ZOOM (Reportes)	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***
N/A	N/A	N/A

7.4 Acciones para la corrección y actualización de las medidas de seguridad

UNAM-Reino Unido		
Identificador único*	ZOOM	
(Nombre del sistema A1)*	ZOOM (Reportes)	
Medida de seguridad*	**Acciones***	**Responsable***
N/A	N/A	N/A

8. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

8.1 Programa de capacitación a los responsables de tratamiento de datos personales

UNAM-Reino Unido			
Identificador único*	ZOOM		
(Nombre del sistema A1)*	ZOOM (Reportes)		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Cursos de capacitación en línea.	Red de Responsables TIC UNAM	Sin fechas fijas.	Comunidad UNAM.

8.2 Programa de difusión de la protección a los datos personales

UNAM-Reino Unido			
Identificador único*	ZOOM		
(Nombre del sistema A1)*	ZOOM (Reportes)		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Cursos de capacitación en línea.	Red de Responsables TIC UNAM	Sin fechas fijas.	Comunidad UNAM.

9. MEJORA CONTINUA

9.1 Actualización y mantenimiento de sistemas de información

UNAM-Reino Unido			
Identificador único*	ZOOM		
(Nombre del sistema A1)*	ZOOM (Reportes)		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Actualización y mantenimiento del sistema.	Actividad interna.	Sin fecha fija.	Procedimiento de desarrollares.

9.2 Actualización y mantenimiento de equipo de cómputo

UNAM-Reino Unido			
Identificador único*	ZOOM		
(Nombre del sistema A1)*	ZOOM (Reportes)		
Actividad*	**Descripción***	**Duración***	**Cobertura***
N/A	N/A	N/A	N/A

9.3 Procesos para la conservación, preservación y respaldos de información

UNAM-Reino Unido		
Identificador único*	ZOOM	
(Nombre del sistema A1)*	ZOOM (Reportes)	
Proceso*	**Descripción***	**Responsable***
Banco de datos del sistema.	Procedimiento interno.	Responsables técnicos.

9.4 Procesos de borrado seguro y disposición final de equipos y componentes informáticos

UNAM-Reino Unido		
Identificador único*	ZOOM	
(Nombre del sistema A1)*	ZOOM (Reportes)	
Proceso*	**Descripción***	**Responsable***
N/A	N/A	N/A

CONTACTO

1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

UNAM-Reino Unido	
Identificador único*	**Contacto**
(Nombre del sistema A1) *	**Formulario de contacto del sitio web de la sede**
Datos personales (sensibles o no) contenidos en el sistema*:	Nombre completo Correo electrónico
Responsable*:	
Nombre*:	Ana Elena González Treviño
Cargo*:	Directora, UNAM-Reino Unido
Funciones*:	Revisar y responder las preguntas/comentarios enviados por los interesados. Análisis de la información de la audiencia para fines estadísticos y de reportes.
Obligaciones*:	No difundir información de los datos personales. No modificar la información almacenada en el servidor. No hacer respaldos de la información de datos personales en el equipo personal.
	Encargados:
(Nombre del Encargado 1*)	Angélica Cruz Villamar
Cargo*:	Responsable TICs, UNAM-Reino Unido
Funciones*:	Revisar y responder las preguntas/comentarios enviados por los interesados. Mantenimiento al sistema. Análisis de la información de la audiencia para fines estadísticos y de reportes.
Obligaciones*:	No difundir información de los datos personales. No modificar la información almacenada en el servidor. No hacer respaldos de la información de datos personales en el equipo personal.

2. ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

UNAM-Reino Unido	
Identificador único¨*	Contacto
(Nombre del sistema A1*)	Formulario de contacto del sitio web de la sede
Tipo de soporte:*	Soporte electrónico
Descripción:*	El registro de la información de usuarios se almacena en una base de datos.
Características del lugar donde se resguardan los soportes:*	Alojamiento en la nube privada del sistema con acceso restringido bajo usuario y contraseña.

3. ANÁLISIS DE RIESGOS

UNAM-Reino Unido		
Identificador único*	Contacto	
(Nombre del sistema A1) *	Formulario de contacto del sitio web de la sede	
Riesgo*	**Impacto***	**Mitigación***
Acceso no autorizado al sistema.	Acceso al sistema, consulta, modificación, robo o eliminación de la información y datos personales.	Cambio periódico de la contraseña del sistema mediante las políticas de clave secreta robusta.

4. ANÁLISIS DE BRECHA

UNAM-Reino Unido		
Identificador único*	Contacto	
(Nombre del sistema A1) *	Formulario de contacto del sitio web de la sede	
Medida de seguridad actual*	**Medida de seguridad necesaria***	**Acciones para remediación***
Acceso al sistema mediante usuario y contraseña.	Correcta.	No es necesario.

PLAN DE TRABAJO

UNAM-Reino Unido			
Identificador único*	Contacto		
(Nombre del sistema A1)*	Formulario de contacto del sitio web de la sede		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Envío de formulario de contacto.	Los interesados ingresan los datos del formulario junto con las preguntas/comentarios.	El formulario esta disponible en todo momento.	Los datos son almacenados en una base de datos con acceso restringido.

10. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

I. TRANSFERENCIAS DE DATOS PERSONALES

UNAM-Reino Unido	
Identificador único*	Contacto
(Nombre del sistema A1)*	Formulario de contacto del sitio web de la sede
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	NA
Transferencias mediante el traslado de soportes electrónicos:	NA
Transferencias mediante el traslado sobre redes electrónicas:	NA

7. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

7.1 Herramientas y recursos para monitoreo de la protección de datos personales

UNAM-Reino Unido		
Identificador único*	Contacto	
(Nombre del sistema A1)*	Formulario de contacto del sitio web de la sede	
Recurso*	**Descripción***	**Control***
Revisiones aleatorias.	Usuarios Administrador, Editor. Usuario y contraseña.	Responsable técnico.

7.2 Procedimiento para la revisión de las medidas de seguridad

UNAM-Reino Unido		
Identificador único*	Contacto	
(Nombre del sistema A1)*	Formulario de contacto del sitio web de la sede	
Medida de seguridad*	**Procedimiento***	**Responsable***
Sistema actualizado. Acceso restringido.	Comprobante de actualización. Asignación de roles.	Responsables técnicos.

7.3 Resultados de la evaluación y pruebas a las medidas de seguridad

UNAM-Reino Unido		
Identificador único*	Contacto	
(Nombre del sistema A1)*	Formulario de contacto del sitio web de la sede	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***
N/A	N/A	N/A

7.4 Acciones para la corrección y actualización de las medidas de seguridad

UNAM-Reino Unido		
Identificador único*	Contacto	
(Nombre del sistema A1)*	Formulario de contacto del sitio web de la sede	
Medida de seguridad*	**Acciones***	**Responsable***
N/A	N/A	N/A

8. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

8.1 Programa de capacitación a los responsables de tratamiento de datos personales

UNAM-Reino Unido			
Identificador único*	Contacto		
(Nombre del sistema A1)*	Formulario de contacto del sitio web de la sede		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Cursos de capacitación en línea.	Red de Responsables TIC UNAM	Sin fechas fijas.	Comunidad UNAM.

8.2 Programa de difusión de la protección a los datos personales

UNAM-Reino Unido			
Identificador único*	Contacto		
(Nombre del sistema A1)*	Formulario de contacto del sitio web de la sede		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Cursos de capacitación en línea.	Red de Responsables TIC UNAM	Sin fechas fijas.	Comunidad UNAM.

9. MEJORA CONTINUA

9.1 Actualización y mantenimiento de sistemas de información

UNAM-Reino Unido			
Identificador único*	Contacto		
(Nombre del sistema A1)*	Formulario de contacto del sitio web de la sede		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Actualización y mantenimiento del sistema.	Actividad interna.	Sin fecha fija.	Procedimiento de desarrollares.

9.2 Actualización y mantenimiento de equipo de cómputo

UNAM-Reino Unido			
Identificador único*	Contacto		
(Nombre del sistema A1)*	Formulario de contacto del sitio web de la sede		
Actividad*	**Descripción***	**Duración***	**Cobertura***
N/A	N/A	N/A	N/A

9.3 Procesos para la conservación, preservación y respaldos de información

UNAM-Reino Unido		
Identificador único*	Contacto	
(Nombre del sistema A1)*	Formulario de contacto del sitio web de la sede	
Proceso*	**Descripción***	**Responsable***
Banco de datos del sistema.	Procedimiento interno.	Responsables técnicos.

9.4 Procesos de borrado seguro y disposición final de equipos y componentes informáticos

UNAM-Reino Unido		
Identificador único*	Contacto	
(Nombre del sistema A1)*	Formulario de contacto del sitio web de la sede	
Proceso*	**Descripción***	**Responsable***
N/A	N/A	N/A

ACCESO KING'S

1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

UNAM-Reino Unido	
Identificador único*	**Acceso King's**
(Nombre del sistema A1) *	**Hoja de registro para acceso a instalaciones de King's**
Datos personales (sensibles o no) contenidos en el sistema*:	Nombre completo Dependencia Firma
Responsable*:	
Nombre*:	Seguridad King's College London.
Cargo*:	Seguridad King's College London.
Funciones*:	Control de accesos. Solicitar a toda persona identificarse. Asegurar que cada visitante realice un registro de acceso.
Obligaciones*:	No difundir información de los datos personales. No modificar la información almacenada en el servidor. No hacer respaldos de la información de datos personales en el equipo personal.
	Usuarios:
(Nombre del Usuario 1*)	Ana Elena González Treviño
Cargo*:	Directora, UNAM-Reino Unido
Funciones*:	Consulta de los registros.
Obligaciones*:	No difundir información de los datos personales. No modificar la información almacenada en el servidor. No hacer respaldos de la información de datos personales en el equipo personal.

2. ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

UNAM-Reino Unido	
Identificador único¨*	Acceso King's
(Nombre del sistema A1*)	Hoja de registro para acceso a instalaciones de King's
Tipo de soporte:*	Soporte electrónico
Descripción:*	El registro de la información de usuarios se almacena en una base de datos.
Características del lugar donde se resguardan los soportes:*	Alojamiento en la nube privada del sistema con acceso restringido bajo usuario y contraseña. La información puede consultarse o descargada en formato PDF, XLM o CSV.

3. ANÁLISIS DE RIESGOS

UNAM-Reino Unido		
Identificador único*	Acceso King’s	
(Nombre del sistema A1) *	Hoja de registro para acceso a instalaciones de King’s	
Riesgo*	**Impacto***	**Mitigación***
Acceso no autorizado al sistema.	Acceso al sistema, consulta, modificación, robo o eliminación de la información y datos personales.	Cambio periódico de la contraseña del sistema mediante las políticas de clave secreta robusta.

4. ANÁLISIS DE BRECHA

UNAM-Reino Unido		
Identificador único*	Acceso King’s	
(Nombre del sistema A1) *	Hoja de registro para acceso a instalaciones de King’s	
Medida de seguridad actual*	**Medida de seguridad necesaria***	**Acciones para remediación***
Acceso al sistema mediante usuario y contraseña.	Correcta.	No es necesario.

PLAN DE TRABAJO

UNAM-Reino Unido			
Identificador único*	Acceso King's		
(Nombre del sistema A1)*	Hoja de registro para acceso a instalaciones de King's		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Registro de asistentes.	Los interesados a la actividad en línea o presencial se registran mediante el sistema ingresando nombre, correo electrónico y género.	El usuario cuenta con 10 minutos para ingresar los datos, de lo contrario, la sesión caduca.	El sistema solicita se acepten los Términos de servicio, las Pautas de la comunidad y la Política de privacidad de Eventbrite.

11. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

I. TRANSFERENCIAS DE DATOS PERSONALES

UNAM-Reino Unido	
Identificador único*	Acceso King's
(Nombre del sistema A1)*	Hoja de registro para acceso a instalaciones de King's
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	NA
Transferencias mediante el traslado de soportes electrónicos:	NA
Transferencias mediante el traslado sobre redes electrónicas:	NA

7. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

7.1 Herramientas y recursos para monitoreo de la protección de datos personales

UNAM-Reino Unido		
Identificador único*	Acceso King's	
(Nombre del sistema A1)*	Hoja de registro para acceso a instalaciones de King's	
Recurso*	**Descripción***	**Control***
Revisiones aleatorias.	IDs físicas. Stikers de Identificación para visitantes.	Seguridad privada.

7.2 Procedimiento para la revisión de las medidas de seguridad

UNAM-Reino Unido		
Identificador único*	Acceso King's	
(Nombre del sistema A1)*	Hoja de registro para acceso a instalaciones de King's	
Medida de seguridad*	**Procedimiento***	**Responsable***
Acceso controlado.	Vigilancia 24/7	Seguridad privada.

7.3 Resultados de la evaluación y pruebas a las medidas de seguridad

UNAM-Reino Unido		
Identificador único*	Acceso King's	
(Nombre del sistema A1)*	Hoja de registro para acceso a instalaciones de King's	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***
N/A	N/A	N/A

7.4 Acciones para la corrección y actualización de las medidas de seguridad

UNAM-Reino Unido		
Identificador único*	Acceso King's	
(Nombre del sistema A1)*	Hoja de registro para acceso a instalaciones de King's	
Medida de seguridad*	**Acciones***	**Responsable***
N/A	N/A	N/A

8. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

8.1 Programa de capacitación a los responsables de tratamiento de datos personales

UNAM-Reino Unido			
Identificador único*	Acceso King's		
(Nombre del sistema A1)*	Hoja de registro para acceso a instalaciones de King's		
Actividad*	**Descripción***	**Duración***	**Cobertura***
NA	NA	NA	NA

8.2 Programa de difusión de la protección a los datos personales

UNAM-Reino Unido			
Identificador único*	Acceso King's		
(Nombre del sistema A1)*	Hoja de registro para acceso a instalaciones de King's		
Actividad*	**Descripción***	**Duración***	**Cobertura***
NA	NA	NA	NA

9. MEJORA CONTINUA

9.1 Actualización y mantenimiento de sistemas de información

UNAM-Reino Unido			
Identificador único*	Acceso King's		
(Nombre del sistema A1)*	Hoja de registro para acceso a instalaciones de King's		
Actividad*	**Descripción***	**Duración***	**Cobertura***
NA	NA	NA	NA

9.2 Actualización y mantenimiento de equipo de cómputo

UNAM-Reino Unido			
Identificador único*	Acceso King's		
(Nombre del sistema A1)*	Hoja de registro para acceso a instalaciones de King's		
Actividad*	**Descripción***	**Duración***	**Cobertura***
N/A	N/A	N/A	N/A

9.3 Procesos para la conservación, preservación y respaldos de información

UNAM-Reino Unido		
Identificador único*	Acceso King's	
(Nombre del sistema A1)*	Hoja de registro para acceso a instalaciones de King's	
Proceso*	**Descripción***	**Responsable***
Banco de datos de la entidad académica.	Procedimiento interno.	Seguridad privada.

9.4 Procesos de borrado seguro y disposición final de equipos y componentes informáticos

UNAM-Reino Unido		
Identificador único*	Acceso King's	
(Nombre del sistema A1)*	Hoja de registro para acceso a instalaciones de King's	
Proceso*	**Descripción***	**Responsable***
N/A	N/A	N/A

II. RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS

3. Señalar las medidas de seguridad que ha implementado el área universitaria para el resguardo de los soportes físicos del sistema de manera que evite la alteración, pérdida o acceso no autorizado a los mismos.
NA

4. Señalar en un listado las personas (nombre, cargo, funciones y obligaciones) que tienen acceso a los soportes físicos del sistema.
NA

III. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

10. Los datos que se registran en las bitácoras:
Usuarios.
11. Si las bitácoras están en soporte físico o en soporte electrónico:
Soporte electrónico.
12. Lugar dónde almacena las bitácoras y por cuánto tiempo:
En el Administrador de Roles del sistema.
13. La manera en que asegura la integridad de las bitácoras:
Bajo el usuario Admin.
14. Respecto del análisis de las bitácoras:
Los usuarios Owner y Admin.

IV. REGISTRO DE INCIDENTES

Describir el procedimiento de atención de incidentes que tiene implementado el área universitaria y especificar si lleva registro de los incidentes relativos a soportes físicos, como lo son la pérdida o alteración no autorizada de expedientes, y para el caso de soportes electrónicos, ofrecer detalles sobre el registro de incidentes en el cual consigne los procedimientos realizados para la recuperación de los datos o para permitir la disponibilidad del proceso.

No se han registrado incidentes hasta el momento.

V. ACCESO A LAS INSTALACIONES

6. Seguridad perimetral exterior (las instalaciones del área universitaria):

King's College London, la universidad británica anfitriona de la sede, cuenta con personal de vigilancia las 24 horas en cada entrada a las instalaciones. El acceso directo a las oficinas de la sede permanece cerrado después de las 18 hrs. A partir de esta hora, la puerta alterna solo puede ser abierta con el sensor del ID.

El personal de King's es el encargado de identificar todo aquel que solicita acceso, ya sea mostrando King's ID de Staff o Student, y cuando se trata de alguien externo (invitados), se solicita el registro en la bitácora física de la entrada.

7. Seguridad perimetral interior (oficina, almacén o bodega para soportes físicos, centro de datos para soportes electrónicos):

Las oficinas de la sede tienen puertas con cerradura las cuales solo puede ser abiertas con las llaves asignas al personal.

VI. ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

La información es actualizada a petición del titular de la información mediante la modificación/cancelación del registro.

VII. PERFILES DE USUARIO Y CONTRASEÑAS

En este rubro el área universitaria deberá describir el esquema de perfiles de usuario y contraseñas que tiene implementado para control de acceso mediante una red electrónica.

1. Modelo de control de acceso (alguno de los siguientes):
Está basado en roles, existen usuarios que pueden ingresar al sistema.

2. Perfiles de usuario y contraseñas en el sistema operativo de red:
Los datos de usuario son almacenados por el aplicativo, no interviene el sistema operativo.

3. Perfiles de usuario y contraseñas manejados por el software aplicativo del sistema de tratamiento de datos personales:
El sistema almacena usuario y contraseñas en el Administrador de roles.

4. Administración de perfiles de usuario y contraseñas:
El encargado del sistema es el encargado de crear nuevos roles y su asignación de usuario. El usuario genera su contraseña. El responsable del sistema autoriza la creación de los nuevos usuarios.

5. Acceso remoto al sistema de tratamiento de datos personales:
El sistema no requiere un acceso remoto porque es un servicio web.

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

5. Señalar si realiza respaldos

a) Completos__, diferenciales ___ o incrementales___;
b) De forma automática ____ o Manual _____,
c) Periodicidad con que los realiza: __2 veces al mes__

6. El tipo de medios (por ejemplo: cintas magnéticas, discos duros, CD-ROM, entre otros) que utiliza para almacenar las copias de seguridad: __Discos duros__
7. Cómo y dónde archiva esos medios, y
8. Quién es el responsable de realizar estas operaciones (el área universitaria o un tercero).
__Responsable técnico__

IX. PLAN DE CONTINGENCIA

4. Presentar el plan de contingencia con el cual garantiza la continuidad de la operación del sistema o informar si no lo tiene, pero se encuentra desarrollándolo. _En desarrollo_
5. Si cuenta con plan de contingencia y lo ha implementado, deberá indicar si realiza pruebas de eficiencia de este. __NA__
6. Informar si cuenta con un sitio redundante (alterno): __NA__

11. APROBACIÓN DEL DOCUMENTO DE SEGURIDAD

		Nombre y firma de quienes revisaron el presente documento:
Responsable del desarrollo:	Lic. Angélica Cruz Villamar Responsable TIC, UNAM-Reino Unido acvillamar@unitedkingdom.unam.mx +44 (0) 207 848 7927	 Lic. Angélica Cruz Villamar
Revisó:	Dra. Ana Elena González Treviño Directora, UNAM-Reino Unido anaelenaglez@kcl.ac.uk +44 (0) 207 848 7031	 Dra. Ana Elena González Treviño
Autorizó:	Dra. Ana Elena González Treviño Directora, UNAM-Reino Unido anaelenaglez@kcl.ac.uk +44 (0) 207 848 7031	 Dra. Ana Elena González Treviño
Fecha de aprobación:	3 de noviembre de 2022	
Fecha de actualización:	18 de agosto de 2022 3 de noviembre de 2022	