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

ÍNDICE DE ANEXOS

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".*

1. INVENTARIO DE SISTEMAS 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*	(Asignar un identificador que asista al Área Universitaria en localizar de manera inequívoca el sistema)
(Nombre del sistema A1) *	
Datos personales (sensibles o no) contenidos en el sistema*:	(Señalar el tipo de datos personales que contiene el sistema, además de listar cada uno de los datos personales recabados)[1]
Responsable*:	
Nombre*:	
Cargo*:	
Funciones*:	(Descripción de las atribuciones con relación al tratamiento de los datos personales del sistema)
Obligaciones*:	(Descripción de las Responsabilidades en cuanto al tratamiento de los datos personales del sistema)
	Encargados[2]:
(Nombre del Encargado 1*)	
Cargo*:	
Funciones*:	(Descripción de las atribuciones con relación al tratamiento de los datos personales del sistema)
Obligaciones*:	(Descripción de las Responsabilidades en cuanto al tratamiento de los datos personales del sistema)
(Nombre del Encargado 2*)	
Cargo*:	
Funciones*:	

[1] Ejemplo de datos personales y datos personales sensibles que se pudieran recabar:

1) Datos personales en general:

a) Datos de identificación: Nombre, domicilio, teléfono particular, teléfono celular, correo electrónico, estado civil, firma, firma electrónica, RFC, CURP, cartilla militar, lugar de nacimiento, fecha de nacimiento, nacionalidad, edad, nombres de familiares, dependientes y beneficiarios, fotografía, costumbres, idioma o lengua, entre otros.

b) Datos laborales: Documentos de reclutamiento y selección, de nombramiento, de incidencia, de capacitación, puesto, domicilio de trabajo, correo electrónico institucional, teléfono institucional, actividades extracurriculares, referencias laborales, referencias personales, entre otros.

b) Datos patrimoniales: Bienes muebles e inmuebles, información fiscal, historial crediticio, ingresos y egresos, cuentas bancarias, seguros, afores, fianzas, servicios contratados, referencias personales, entre otros.

c) Datos sobre procedimientos administrativos seguidos en forma de juicio y/o procesos jurisdiccionales: Información relativa a una persona que se encuentre sujeta como parte o tercero en torno a un procedimiento administrativo seguido en forma de juicio o proceso jurisdiccional en materia laboral, civil, familiar, penal, de justicia para adolescentes, amparo o administrativa, con independencia de su etapa de trámite

d) Datos académicos: Trayectoria educativa, títulos, cédula profesional, certificados y reconocimientos, entre otros.

e) Datos de tránsito y movimientos migratorios: Información relativa al tránsito de las personas dentro y fuera del país e información migratoria de las personas, entre otros.

f) Características físicas: Color de piel, ojos y cabello, señas particulares, estatura, peso, complexión, discapacidades, entre otros.

2) Datos personales sensibles: Opiniones políticas, origen racial o étnico, creencias religiosas, creencias filosóficas y morales, afiliación sindical, estado de salud presente o futuro (historial clínico, alergias, enfermedades, información relacionada con cuestiones de carácter psicológico y/o psiquiátrico, incapacidades médicas, intervenciones quirúrgicas, vacunas, consumo de sustancias tóxicas, uso de aparatos oftalmológicos, ortopédicos, auditivos y prótesis, entre otros), preferencia sexual, información genética y cualquier otro que pueda causar.

[2] Se tienen que ingresar los datos de todos los Encargados del sistema de tratamiento de datos personales.

Obligaciones*:	
	Usuarios:
(Nombre del Usuario 1*)	
Cargo*:	
Funciones*:	
Obligaciones*:	
(Nombre del Usuario 2*)	
Cargo*:	
Funciones*:	
Obligaciones*:	
(Nombre del Usuario 3*)	
Cargo*:	
Funciones*:	
Obligaciones*:	
Sistema (Nombre del A2)*:	
Datos personales contenidos en el sistema*:	(Señalar el tipo de dato personales que contiene el sistema, además de listar cada uno de los datos personales recabados)
	Responsable:
Nombre*:	
Cargo*:	
Funciones*:	(Descripción de las atribuciones con relación al tratamiento de los datos personales del sistema)
Obligaciones*:	(Descripción de las Responsabilidades en cuanto al tratamiento de los datos personales del sistema)
	Encargados:
(Nombre del Encargado 1*)	
Cargo*:	
Funciones*:	(Descripción de las atribuciones con relación al tratamiento de los datos personales del sistema)
Obligaciones*:	(Descripción de las Responsabilidades en cuanto al tratamiento de los datos personales del sistema)
(Nombre del Encargado 2*)	
Cargo*:	
Funciones*:	
Obligaciones*:	
	Usuarios:
(Nombre del Usuario 1*)	
Cargo*:	
Funciones*:	
Obligaciones*:	
(Nombre del Usuario 2*)	
Cargo*:	

Funciones*:	
Obligaciones*:	
(Nombre del Usuario 3*)	
Cargo*:	
Funciones*:	
Obligaciones*:	

2. ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS 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¨*	(Asignar un identificador que asista al Área Universitaria en localizar de manera inequívoca el sistema)
(Nombre del sistema A1*)	
Tipo de soporte[3]:*	Precisar si el sistema se encuentra en soporte físico, electrónico, o ambos.
Descripción[4]:*	Base de datos
Características del lugar donde se resguardan los soportes[5]:*	Ejemplo: Alojamiento en la nube privada de Microsoft
(Nombre del sistema A2*)	
Tipo de soporte*:	Precisar si el sistema se encuentra en soporte físico, electrónico, o ambos.
Descripción*:	Expedientes
Características del lugar donde se resguardan los soportes*:	Ejemplo: Oficina con ventilación natural, luz natural y artificial, puerta de acceso de madera y chapa, aislada de humedad, con archiveros y libreros que permiten la conservación adecuada de los documentos.
(Nombre del sistema A3*)	

[3] En caso de que el área universitaria prevea cambiar el tipo de soporte que utiliza el sistema de tratamiento de datos personales por ejemplo de físico a electrónico o en el supuesto de que prevea en el futuro utilizar ambos tipos de soportes, deberá indicarse en este rubro.

[4] Describir el soporte en el que se encuentran los datos por ejemplo para soportes físicos podrían ser formatos, listados, documentos o expedientes, entre otros y para soportes electrónicos, hoja de cálculo o base de datos relacional, entre otros.

[5] Para describir las características del lugar donde se resguardan los soportes, se deberá considerar lo siguiente:

a) Para soportes físicos, el área universitaria deberá incluir una descripción escrita con detalles sobre las características físicas de la oficina, almacén o bodega donde resguarda dichos soportes;

b) Para soportes electrónicos, la descripción ofrecida por el área universitaria deberá incluir un diagrama de la arquitectura de seguridad en el cual sea posible apreciar el flujo de datos a través de la o las redes electrónicas que interconectan los equipos (clientes, servidores, cortafuegos, unidades de almacenamiento, entre otros) del sistema de tratamiento de datos personales. Además, deberá describir las medidas de seguridad física que ha implementado para la protección del centro de datos donde residen tales soportes.

c) En caso de que el sistema de tratamiento de datos personales ocupe ambos tipos de soportes, deberá presentar las descripciones correspondientes a cada uno, en términos de lo señalado en los incisos a) y b) anteriores.

3. ANÁLISIS DE RIESGOS

*(Llenar una tabla para cada sistema. Campos con * son obligatorios. Borrar instrucciones en cursivas)*

(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) *		
Riesgo*	**Impacto***	**Mitigación***
Describa el riesgo. Agregue un renglón para cada uno	*Describa el impacto que el riesgo implica para los datos personales*	*Describa las medidas para mitigación del riesgo y su impacto los datos personales.*

4. ANÁLISIS DE BRECHA

*(Llenar una tabla para cada sistema. Campos con * son obligatorios. Borrar instrucciones en cursivas)*

(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) *		
Medida de seguridad actual*	**Medida de seguridad necesaria***	**Acciones para remediación***
Describa la medida actual. Agregue un renglón para cada una	*Describa la medida de seguridad en su adecuado requerimiento*	*Describa las acciones para reducir la brecha entre la medida actual y la adecuada.*

5. PLAN DE TRABAJO

*(Llenar una tabla para cada sistema. Campos con * son obligatorios. Borrar instrucciones en cursivas)*

(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.*

6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

I. TRANSFERENCIAS 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)***
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:[6]	**a)** Deberá señalar si el envío se realiza a través de mensajero oficial, mensajero privado o correspondencia ordinaria,[7] **b)** Deberá precisar si utiliza un sobre o paquete sellado de manera que sea perceptible si fue abierto antes de su entrega; **c)** Deberá manifestar si el sobre o paquete enviado es entregado en mano al destinatario, previa acreditación con identificación oficial; **d)** Deberá indicar si el remitente pide al destinatario que le informe en caso de que reciba el sobre o paquete con señas de apertura; **e)** Deberá informar si el destinatario envía acuse de recibo al remitente una vez recibidos los datos personales, y **f)** Deberá señalar si el remitente registra la o las transferencias

[6] **Ejemplo de medidas de seguridad para transmisiones mediante el traslado de soportes físicos:**
a) La transmisión de datos personales mediante el traslado de soportes físicos se lleva a cabo por la vía elegida de común acuerdo entre las partes: mensajero oficial, asistente secretarial, visita personal, servicio de mensajería externo, entre otras posibles. Se define un destinatario primario y otro secundario por si el mensajero no encuentra al primero.
b) El paquete con datos personales en soportes físicos viaja debidamente sellado, de forma tal que sea perceptible cualquier violación o apertura no autorizada del mismo.
c) La entrega del paquete se realiza sólo si el destinatario acredita su identidad. Para ello, el destinatario presenta una identificación oficial con fotografía y el mensajero recaba nombre, firma y un número de referencia que aparezca en tal identificación, además de la fecha de entrega.
d) El mensajero no entrega el paquete si el destinatario no puede acreditar su identidad. En este caso, el mensajero devuelve el paquete al transmisor.
e) El transmisor verifica que el mensajero haya entregado el paquete al destinatario. Si el transmisor detecta que dicho paquete fue entregado a otra persona, da inicio al proceso de atención de un incidente.
f) Se registran estas transmisiones en el Sistema de tratamiento de datos personales.

[7] El envío por correspondencia ordinaria sólo es aceptable si los datos personales requieren de un nivel de protección básico o si los datos están disociados de sus titulares.

	en su bitácora, así como en el Sistema. **g)** Indicar si las transferencias de datos personales se formalizaron mediante algún instrumento jurídico.
Transferencias mediante el traslado de soportes electrónicos:	**a)** Deberá señalar lo previsto en el numeral 1) anterior, incisos a) al f), y **b)** Deberá precisar si los archivos electrónicos que contienen datos personales son cifrados antes de su envío y proporcionar detalles técnicos del cifrado tales como el tipo de algoritmo utilizado y la longitud de la llave (o clave)[8]. **c)** Indicar si las transferencias de datos personales se formalizaron mediante algún instrumento jurídico.
Transferencias mediante el traslado sobre redes electrónicas:	**a)** Deberá señalar la información prevista en el inciso b) del numeral 2) anterior; **b)** Deberá precisar si utiliza un canal de comunicación dedicado o una red privada virtual especificando detalles técnicos relativos al cifrado de dicho canal como la longitud de llave (o clave); en su caso, deberá precisar si para dicho canal utiliza una red pública (como Internet) especificando el protocolo de transferencias protegidas utilizado; **c)** Deberá manifestar si el remitente y/o el destinatario cuentan con dispositivos que faciliten la detección de intrusiones en el canal de comunicaciones. **d)** Deberá informar si el destinatario envía acuse de recibo al remitente una vez recibidos los datos personales y **e)** Deberá señalar si el remitente registra la o las transferencias en su bitácora, así como en el Sistema de tratamiento de datos personales. **f)** Indicar si las transferencias de datos personales se formalizaron mediante algún instrumento jurídico.
(Nombre del sistema A2)	
(Nombre del sistema A3)	

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.[9]
2. Señalar en un listado las personas (nombre, cargo, funciones y obligaciones) que tienen acceso a los soportes físicos del sistema.[10]

III. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

1. Los datos que se registran en las bitácoras:[11]

[8] Se recomiendan los siguientes bits de longitud considerando el nivel de protección que requieren los datos personales: nivel de protección bajo, 128 bits de longitud; nivel de protección medio, 512 bits de longitud; y nivel de protección alto, 1024 bits. Estos parámetros pueden variar de acuerdo con el avance o desarrollo en tecnologías de cifrado.
[9] Por ejemplo, se espera que precise si los formatos impresos, documentos, listados o expedientes están foliados, cosidos o engargolados, si los muebles o la estantería donde residen cuentan con cerradura, si existen mecanismos para regular la temperatura y la humedad, si existen sistemas de tratamiento de datos personales de detección y/o supresión de incendios, si cuenta con mecanismos para regular y mantener el suministro continuo de energía eléctrica, entre otras posibles medidas.
[10] En caso de ser muchas personas, se sugiere agregar el listado como Anexo al Documento de seguridad.
[11] Las áreas de informática y seguridad de la información han designado una persona que se encarga de realizar un análisis de las bitácoras generadas. Las siguientes características aplican al caso:

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;[12]

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, 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

a) Se cuenta con la ayuda de una herramienta informática adquirida para tal propósito.

b) Cada semana se llevan a cabo análisis de bitácoras, pero no de todas ellas. Depende de la bitácora y de las amenazas detectadas en el entorno.

Ejemplo de medidas de seguridad aplicables a bitácoras para sistema de tratamiento de datos personales en soportes físicos: El responsable del sistema procurará un estricto control y registro de:

a) Las autorizaciones emitidas para facultar el acceso a un funcionario universitario a fin de que éste, en el ejercicio de sus funciones, pueda interactuar con uno o más de los sistemas de tratamiento de datos personales a su cargo.

b) La asignación, actualización y reemplazo de las llaves que entrega a los autorizados para que éstos puedan abrir el mecanismo de apertura de la puerta en la zona de acceso restringido. Las acciones que los autorizados llevan a cabo en el área de resguardo. Para ello, designa a un Encargado quien anota lo siguiente: Quién solicita el acceso, cuándo se lleva a cabo (fecha y hora de entrada y salida), la razón que lo motiva y número del expediente utilizado.

c) El préstamo de expedientes es asistido por un sistema de tratamiento de datos personales de cómputo que utiliza códigos de barras en los gafetes del personal autorizado y en los expedientes.

d) El sistema de tratamiento de datos personales de préstamo de expedientes genera una bitácora electrónica que se respalda diariamente en un servidor dentro del centro de cómputo que administra el área de informática. Su integridad se garantiza copiando dicha bitácora en un CD-R diariamente.

e) El Encargado del sistema de tratamiento de datos personales es la persona designada para analizar la bitácora cada mes mediante una herramienta adquirida para tal fin.

Ejemplo de medidas de seguridad aplicables a bitácoras para sistema de tratamiento de datos personales en soportes electrónicos:

I. El responsable del sistema de tratamiento de datos personales -en coordinación con las áreas de informática y seguridad de la información- lleva un estricto control y registro de:

a) Las bitácoras de eventos ocurridos a nivel *sistema de tratamiento de datos personales operativo* en los equipos (servidores, cortafuegos, almacenamiento masivo) que habilitan la operación del sistema de tratamiento de datos personales. Entre otras, se generan bitácoras para desempeño del servidor: intentos de acceso (exitosos y fallidos); accesos denegados a usuarios y terminales; uso de herramientas para administración del servidor, y fecha y hora de los eventos anteriores.

b) Las bitácoras de eventos generados a nivel *software aplicativo* del sistema de tratamiento de datos personales. Entre otras, se generan bitácoras para mensajes de error; apertura, modificación y cierre de archivos; violaciones de seguridad detectadas por el software aplicativo, y fecha y hora de estos eventos.

c) Las bitácoras de eventos relativos a las actividades de usuarios (capturistas, Encargados, el propio responsable y el administrador del servidor) en su interacción con el sistema de tratamiento de datos personales. Entre otras, se generan bitácoras para: archivos servicios y recursos utilizados; intentos de acceso (exitosos y fallidos); comandos y operaciones iniciadas, y fecha y hora de dichos eventos.

d) El conjunto de bitácoras permite registrar, entre otros, los siguientes datos: Quién accede a los datos personales, desde dónde y con qué; accesos (intentos exitosos y fallidos) y salidas; propósito del acceso (sólo para modificaciones en el software aplicativo); operaciones llevadas a cabo; datos personales (registros y campos) utilizados de la base de datos, y fecha y hora de estos eventos.

e) Las bitácoras arriba mencionadas están todas en soportes electrónicos y se almacenan al menos por dos años en CD-R. Se tiene una copia en el centro de datos y otra se lleva a una bóveda bancaria subcontratada también para los respaldos.

II. La integridad de las bitácoras se garantiza copiándolas en un servidor del centro de datos el cual las graba en CD-R. Algunas se copian cada hora, otras a diario. La integridad de las copias se garantiza además con "resúmenes" creados por un algoritmo "digestor". Se cuenta con una herramienta de software que automatiza estas operaciones.

III. Se pueden realizar análisis focalizados a mayor profundidad en caso de presentarse un incidente que así lo requiera.

[12] En caso de tener las bitácoras en soportes físicos, debe señalar si en el futuro planea incorporarlas a soportes electrónicos.

permitir la disponibilidad del proceso.

1. Los datos que registra:
   a) La persona que resolvió el incidente;
   b) La metodología aplicada;[13]
   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 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?

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.

[13] **Ejemplo de procedimiento en caso de presentarse un incidente:**
- **a)** El Encargado elabora y entrega un informe al responsable a más tardar al día siguiente de haber ocurrido el incidente. Dicho informe precisa los soportes físicos o electrónicos afectados y, en su caso, los recuperados.
- **b)** El incidente se registra en una hoja de cálculo anotando quién resolvió el incidente y los soportes dañados y recuperados. Dicha hoja está protegida con una contraseña de acceso. Su integridad se garantiza generando y almacenando un resumen creado por un algoritmo digestor en un servidor del centro de datos y respaldándola en un CD-R después de registrar un incidente.
- **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.

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

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?

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 los almacena?

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 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

1. Señalar si realiza respaldos
   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) que utiliza para almacenar las copias de seguridad;[14]
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

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);[15]
   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)[16], 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

[14] Es deseable que precise si para almacenar dichos medios cuenta con al menos dos lugares distintos que cumplan con las condiciones de seguridad especificadas en el articulado del Capítulo V de los Lineamientos, conforme a la fracción III del Trigésimo primero de los Lineamientos; o bien, si utiliza un espacio externo seguro para guardar de manera sistemática dichos respaldos, según la fracción VIII del Trigésimo séptimo de tales Lineamientos.

[15] El tipo de sitio caliente, tibio o frío se refiere a la infraestructura, el equipo y el software disponibles en el sitio alterno; por lo que a mayor disponibilidad de dichos elementos resulta una menor demora para restablecer las operaciones de uno o más sistema de tratamiento de datos personales. Ejemplos de lo anterior son, en cuanto a **infraestructura:** aire acondicionado, cableado, suministro de energía eléctrica y enlaces de comunicaciones; en cuanto al **equipo**: servidores, almacenamiento y periféricos, y por lo que se refiere al **software:** sistema de tratamiento de datos personales operativos, manejadores de bases de datos y aplicaciones. Por lo tanto:
i) En un **sitio alterno caliente** se mantienen disponibles en todo momento la infraestructura, el equipo y el software; lo único que hace falta para iniciar operaciones son los datos y el personal. Este tipo de sitios alternos es el más costoso, pero supone tan solo unas cuantas horas para restaurar operaciones.
ii) El **sitio alterno tibio** cuenta con infraestructura no configurada y equipos equivalentes que pueden estar disponibles en pocas horas, pero no contienen software ni datos. Este tipo de sitios alternos es el punto medio en costo y tiempo para restaurar operaciones.
iii) 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.

[16] Se debe seguir el modelo del sistema de tratamiento de datos personales A1 –incisos I al IX- para señalar las medidas de seguridad aplicables a cada uno de los sistema de tratamiento de datos personales que posea el área universitaria.

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

7.1. Herramientas y recursos para monitoreo de la protección 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*	*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)

7.2. Procedimiento para la revisión de las medidas de seguridad

*(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)***	
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*	*Indicar:* *a) nombre del responsable del procedimiento*

	penetración, revisión de estabilidad, etc.	*b) tiempo máximo de ejecución en días.*

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

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

8. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

8.1. Programa de capacitación a los responsables de seguridad 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*

8.2. 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*

9. MEJORA CONTINUA

9.1. 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.*

9.2. Actualización y mantenimiento de equipo de cómputo

*(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 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.*

9.3. Procesos para la conservación, preservación y respaldos 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)***	
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.*

9.4. 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.*

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.)[17]

[17] La cancelación da lugar al bloqueo de los datos, esto es, el periodo en el que la autoridad conservará los datos para efectos de responsabilidades, el cual será equivalente al plazo de prescripción de las acciones derivadas de la relación jurídica que funda el tratamiento en términos de la normatividad de aplicable y, cumplido este plazo, deberá procederse a la supresión del dato que implica el borrado físico del mismo.
Bajo este contexto, la cancelación no supone automáticamente la supresión o borrado físico de los datos, sino que se debe determinar un período o fase previa de bloqueo de los datos, en el cual no se podrá disponer de tales datos en la misma medida en que la podría hacerse por el área universitaria de estar en operación el 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:[18]

(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)

La cancelación de sistema de tratamiento de datos personales debe considerar lo establecido en los Lineamientos Generales para la Organización, Administración y Conservación de los Archivos de la Universidad Nacional Autónoma de México, así como el Catálogo de disposición documental de la Universidad del año respectivo, a fin de atender al valor documental de la información contenida en el mismo.

[18] Es el periodo por el que se conservará para efectos de responsabilidades, tomando en cuenta el plazo de su prescripción conforme la normatividad aplicable.

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 funcionario o empleado universitario que elaboró el documento de seguridad)	
Revisó:	(Señalar nombre, puesto, teléfono y correo electrónico del funcionario o empleado universitario que revisó el documento de seguridad)	
Autorizó:	(Señalar nombre, puesto, teléfono y correo electrónico del funcionario o empleado universitario que autorizó el documento de seguridad)	
Fecha de aprobación:	(Incluir la fecha de liberación del documento)	
Fecha de actualización:	(Incluir la primer versión e ir agregando las subsiguientes del documento)	

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.

Núm. formato	Etapa	Duración estimada	Medidas de seguridad técnicas y proceso recomendado para su cumplimiento
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.

Núm. formato	Etapa	Duración estimada	Medidas de seguridad técnicas y proceso recomendado para su cumplimiento
			- 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.** **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

Núm. formato	Etapa	Duración estimada	Medidas de seguridad técnicas y proceso recomendado para su cumplimiento
			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.* **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

Núm. formato	Etapa	Duración estimada	Medidas de seguridad técnicas y proceso recomendado para su cumplimiento
			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.** **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

Núm. formato	Etapa	Duración estimada	Medidas de seguridad técnicas y proceso recomendado para su cumplimiento
			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.

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				

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 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	