Documento de seguridad de datos personales de la Secretaría de Desarrollo Institucional

Agosto 2022

Secretaría de
Desarrollo Institucional

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 Secretaría de Desarrollo Institucional (en adelante SDI) de la Universidad Nacional Autónoma de México, 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 la SDI, el tipo de datos personales que contiene cada uno, los responsables, encargados, usuarios de cada sistema y las medidas de seguridad concretas implementadas.

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 en el *Diario Oficial de la Federación* 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 sea 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.

La SDI, con la finalidad de establecer y mantener las medidas de seguridad de carácter administrativo, físico y técnico para la protección de los datos personales y en cumplimiento a las disposiciones legales antes descritas, emite el presente *Documento de Seguridad*, en observancia de los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad en el tratamiento de los datos personales, con la intención de brindar homogeneidad en la organización y procesos para la protección de los datos personales de esta Secretaría.

El cimiento del presente *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 mismo considera el tamaño y estructura de la propia UNAM, objetivos, clasificación de la información, requerimientos de seguridad y procesos que se precisan en razón de los activos que posee esta 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”.

OBJETIVO

El presente *Documento de Seguridad* tiene como propósito describir pormenorizadamente los procesos de control interno del universo de datos personales en posesión de la SDI, el tipo de datos personales que contienen los archivos, los responsables, las obligaciones, el análisis de riesgos, el análisis de brecha y los mecanismos de monitoreo y revisión de las medidas de seguridad, el ciclo de vida de los datos personales, entre otros.

TÉRMINOS Y DEFINICIONES

Activo: Todo elemento de valor para la Universidad involucrado en el tratamiento de datos personales, entre ellos, las bases de datos, el conocimiento de los procesos, el personal, el hardware, el software, los archivos o los documentos en papel.

Aviso de privacidad: Documento a disposición del titular de forma física, electrónica o en cualquier formato generado por el responsable, a partir del momento en el cual se recaben sus datos personales, con el objeto de informarle los propósitos del tratamiento de éstos.

Bases de datos: Conjunto ordenado de datos personales referentes a una persona física identificada o identificable, condicionados a criterios determinados, con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización.

Borrado seguro: Procedimiento para la eliminación en un dispositivo o medio de almacenamiento, conocido o por conocer, que impide la recuperación de los datos personales.

Ciclo vital del documento: Las tres fases por las que atraviesan los documentos de archivo, sea cual sea su soporte, desde su recepción o generación hasta su conservación permanente o baja documental, a saber: archivo de trámite, archivo de concentración y archivo histórico.

Confidencialidad: Es el principio de seguridad de la información que consiste en que la información no pueda estar disponible o divulgarse a personas o procesos no autorizados por el área universitaria respectiva.

Control de seguridad en la red: Configuración de equipo activo de telecomunicaciones y software para proteger la transmisión de datos personales.

Disociación: El procedimiento mediante el cual los datos personales no pueden asociarse al titular ni permitir, por su estructura, contenido o grado de desagregación, la identificación de este.

Disponibilidad: Es el principio de seguridad de la información que consiste en ser accesible y utilizable a solicitud de personas o procesos autorizados por el área universitaria respectiva.

Documento de seguridad: Instrumento que describe y da cuenta de manera general sobre las medidas de seguridad técnicas, físicas y administrativas adoptadas por el responsable para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que posee.

Encargado: La persona física o jurídica distinta a las áreas, entidades o dependencias universitarias, que realizan el tratamiento de los datos personales a nombre de la Universidad, suscribiendo para tal

efecto los instrumentos consensuales, correspondientes acordes con la Legislación Universitaria aplicable.

Integridad: Es el principio de seguridad de la información consistente en garantizar la exactitud y la completitud de la información y los sistemas, de manera que éstos no puedan ser modificados sin autorización, ya sea accidental o intencionadamente.

Ley General: Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

Lineamientos: Lineamientos para la Protección de Datos Personales en Posesión de la Universidad Nacional Autónoma de México.

Medidas de seguridad: Conjunto de acciones, actividades, controles o mecanismos técnicos, administrativos y físicos que permitan proteger los datos personales.

Medidas de seguridad administrativas: Políticas y procedimientos para la gestión, soporte y revisión de la seguridad de la información a nivel organizacional; la identificación, clasificación y borrado seguro de la información, así como la sensibilización y capacitación del personal, en materia de protección de datos personales.

Medidas de seguridad físicas: Conjunto de acciones y mecanismos para proteger el entorno físico de los datos personales y de los recursos involucrados en su tratamiento, los cuales pueden ser desde medidas preventivas, cotidianas y correctivas para tener un control de acceso, preservación, conservación de las instalaciones, recursos o bienes en los cuales se resguarda información e incluso a la información misma, asegurando así su disponibilidad e integridad. De manera enunciativa más no limitativa, se deben considerar las siguientes actividades:

- Prevenir el acceso no autorizado al perímetro de la organización, sus instalaciones físicas, áreas críticas, recursos e información;
- Prevenir el daño o interferencia a las instalaciones físicas, áreas críticas de la organización, recursos e información;
- Proteger los recursos móviles, portátiles y cualquier soporte físico o electrónico que pueda salir de la organización, y
- Proveer a los equipos que contienen o almacenan datos personales de un mantenimiento eficaz, que asegure su disponibilidad e integridad.

Medidas de seguridad técnicas: Conjunto de acciones y mecanismos para proteger los datos personales que se encuentren en formato digital, así como los sistemas informáticos que les den tratamiento. De manera enunciativa más no limitativa, se deben considerar las siguientes actividades:

- Asegurar que el acceso a las bases de datos o a la información, así como a los recursos, sea por usuarios identificados y autorizados;
- Generar un esquema de privilegios para que el usuario realice las actividades que requiere con motivo de sus funciones;
- Revisar la configuración de seguridad en la adquisición, operación, desarrollo y mantenimiento del software y hardware, y
- Gestionar las comunicaciones, operaciones y medios de almacenamiento de los recursos informáticos en el tratamiento de datos personales.

Principio del menor privilegio: Otorgamiento de los permisos necesarios y suficientes a un usuario autorizado para acceder a un sistema de información para el desempeño de sus actividades.

Red de datos: Conjunto de componentes electrónicos activos y medios de comunicación conocidos o por conocer tales como fibra óptica, enlaces inalámbricos, cable, entre otros, que permiten el intercambio de paquetes de datos entre dispositivos electrónicos para el procesamiento de información.

Responsable: Las áreas universitarias que manejan, resguardan y/o deciden sobre el tratamiento de datos personales.

Responsable de seguridad de datos personales: Encargado de las acciones relacionadas con las medidas de seguridad para el tratamiento de los datos personales designado por cada área universitaria.

Seguridad de la información: La preservación de la confidencialidad, integridad y disponibilidad de la información, que puede abarcar además otras propiedades, como la autenticidad, la responsabilidad, la fiabilidad y el no repudio.

Servicios de nube privada: Modelo de servicio de tecnología de información proporcionados bajo demanda a las áreas universitarias, en infraestructura propiedad de la Universidad y que incluye cómputo, almacenamiento, plataforma, seguridad y respaldos.

Servicios de nube pública: Modelo de servicio de tecnología de información adquirida bajo demanda a terceros, operada en infraestructura ajena a la Universidad.

Sistema de Gestión de Seguridad de Datos Personales: Conjunto de elementos y actividades interrelacionadas para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el tratamiento y la seguridad de los datos personales.

Sistemas para el tratamiento: Conjunto de elementos mutuamente relacionados o que interactúan para realizar la obtención, uso, registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de datos personales, en medios físicos o electrónicos.

Soporte: Medio, ya sea electrónico o físico, en el que se registra y guarda información, como lo es: el papel, así como los audiovisuales, fotográficos, fílmicos, digitales, electrónicos, sonoros y visuales, entre otros, y los que produzca el avance de la tecnología.

Soportes electrónicos: Son los medios de almacenamiento accesibles sólo a través del uso de algún dispositivo electrónico conocido o por conocer, que procese su contenido para examinar, modificar o almacenar los datos, tales como: cintas magnéticas de audio, vídeo y datos, fichas de microfilm, discos ópticos (CDs, DVDs y Blue-rays), discos magneto ópticos, discos magnéticos (flexibles y duros) y demás medios para almacenamiento masivo no volátil.

Soportes físicos: Son los medios de almacenamiento accesibles de forma directa y sin intervención de algún dispositivo para examinar, modificar o almacenar los datos, tales como: documentos, oficios, formularios impresos, escritos autógrafos, documentos de máquina de escribir, fotografías, placas radiológicas, carpetas, expedientes, entre otros.

Supresión: La erradicación del registro de los datos personales conforme a la normativa archivística aplicable, que resulte en la eliminación, borrado o destrucción de los datos personales bajo las medidas de seguridad previamente establecidas por el responsable.

Transferencia: Toda comunicación de datos personales dentro o fuera del territorio mexicano, realizada a persona distinta del titular, del responsable o del encargado.

Tratamiento: Cualquier operación o conjunto de operaciones efectuadas mediante procedimientos manuales o automatizados aplicados a los datos personales, relacionadas con la obtención, uso, registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de datos personales.

Vulneración de seguridad: En cualquier fase del tratamiento de datos, se considera la pérdida o destrucción no autorizada; el robo, extravío o copia no autorizada; el uso, acceso o tratamiento no autorizado, o el daño, la alteración o modificación no autorizada.

ABREVIATURAS

SDI: Secretaría de Desarrollo Institucional de la UNAM.

ALCANCE

Aplica a todas las áreas que integran la SDI que recaban para sus funciones y tienen en su poder datos personales y datos personales sensibles.

El documento se desglosa por cada una de las áreas de la SDI, que tienen a su cargo o utilizan sistemas que inciden en el tratamiento de datos personales, conforme al siguiente orden:

Coordinación de Enlace y Seguimiento:

Coordinador de Diseño, Identidad y Comunicación:
- Solicitud de difusión (1)
- Gestión de eventos virtuales (2)

Departamento de Gestión Institucional:
- Bitácora del responsable Sanitario de la SDI / Comité de Seguimiento COVID-19 (3)

Departamento de TIC:
- Gestión de correo electrónico institucional (4)
- Solicitud de servicios TIC (5)

Secretaría Técnica:

Departamento de la Red de Educación Continua:
- Control de registros para la emisión de constancias – SIGECO (6)

Departamento de Proceso Editorial:
- Reconocimiento de los Derechos Patrimoniales (7)

Unidad Administrativa:

Departamento de Bienes y Suministros y Servicios Generales:
- Sistema Institucional de Compras SIC (8)
- Sistema de Videovigilancia (9)

Departamento de Personal:
- Sistema Integral de Personal/FORMA UNICA ELECTRONICA (FUE) (10)
- Sistema Integral de Personal/Honorarios (11)

Departamento de Presupuesto:
- Sistema Integral de Administración Financiera (SIAF) (12)
- Sistema Factura Digital UNAM (13)

COORDINACIÓN DE ENLACE Y SEGUIMIENTO:
COORDINADOR DE DISEÑO, IDENTIDAD Y COMUNICACIÓN
(1)

1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Coordinación de Enlace y Seguimiento	
Identificador único*	**(SDI-CEYS-1)**
(Nombre del sistema A1) *	**Solicitud de difusión**
Datos personales (sensibles o no) contenidos en el sistema*	**1. Datos personales en general:** **a) Datos de identificación:** Nombre completo y correo electrónico. 2. **No se recaban datos personales sensibles**.
Responsable*:	
Nombre*	Rubén Muñiz Arzate
Cargo*	Coordinador de Enlace y Seguimiento
Funciones*	• Generar propuestas para coadyuvar a la difusión de logros de la Universidad y de la Secretaría de Desarrollo Institucional, en diversos medios. • Colaborar en la integración de estudios de identidad y valores universitarios, con otras áreas responsables de la Secretaría de Desarrollo Institucional.
Obligaciones*	• Conocer, proteger su integridad, resguardar y conservar la privacidad de los datos que se manejan y mantener la secrecía de la información. • Hacer uso de los datos únicamente en el ejercicio de sus funciones y para los fines que han sido recabados.
	Encargados:
(Nombre del Encargado 1*)	Félix Luciano Miramontes Hernández
Cargo*:	Coordinador de Diseño, Identidad y Comunicación
Funciones*:	• Recibir y revisar las solicitudes para difundir información en los canales institucionales de la Secretaría de Desarrollo institucional. • Dar seguimiento a las solicitudes de difusión. • Publicar y vigilar la correcta difusión en las redes sociales institucionales de la información solicitada.

Obligaciones*:	• Conocer, proteger su integridad, resguardar y conservar la privacidad de los datos que se manejan y mantener la secrecía de la información. • Mantener la confidencialidad de los datos personales contenidos en la solicitud. • Hacer uso de los datos únicamente en el ejercicio de sus funciones y para los fines para los que han sido recabados. • Eliminar la información una vez que la solicitud haya sido procesada.
(Nombre del Encargado 2*)	Linda Ma. del C. Rey Hernández
Cargo*:	Jefa del departamento de TIC
Funciones*:	• Recibir y revisar las solicitudes para difundir información en los canales institucionales de la SDI. • Dar seguimiento a las solicitudes de difusión de los usuarios. • Publicar y vigilar la correcta difusión de la información solicitada en la página web institucional.
Obligaciones*:	• Conocer, proteger su integridad, resguardar y conservar la privacidad de los datos que se manejan y mantener la secrecía de la información. • Mantener la confidencialidad de los datos personales contenidos en la solicitud. • Hacer uso de los datos únicamente en el ejercicio de sus funciones y para los fines para los que han sido recabados. • Eliminar la información una vez que la solicitud haya sido procesada

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

Coordinación de Enlace y Seguimiento	
Identificador único*	**(SDI-CEYS-1)**
(Nombre del sistema A1) *	**Solicitud de difusión**
Tipo de soporte: *	Soporte electrónico.
Descripción: *	Nube privada.
Características del lugar donde se resguardan los soportes: *	Alojamiento en nube privada.

3. ANÁLISIS DE RIESGOS

Eliminado: Seis renglones en los que se especifica el riesgo, once con el impacto y veinticuatro con la mitigación, correspondientes al análisis de riesgos. Fundamento legal: artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública. En virtud de tratarse de información reservada.

Coordinación de Enlace y Seguimiento		
Identificador único¨*	**(SDI-CEYS-1)**	
(Nombre del sistema A1*)	**Solicitud de difusión**	
Riesgo*	**Impacto***	**Mitigación***
Comentario	Comentario	Comentario
Comentario	Comentario	Comentario
Comentario	Comentario	Comentario

4. ANÁLISIS DE BRECHA

Eliminado: Once renglones en los que se especifican las medias de seguridad actuales, doce con las medidas de seguridad necesarias y once con las acciones para remediación, correspondientes al análisis de brecha.
Fundamento legal: artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública. En virtud de tratarse de información reservada.

Coordinación de Enlace y Seguimiento		
Identificador único¨*	**(SDI-CEYS-1)**	
(Nombre del sistema A1*)	**Solicitud de difusión**	
Medida de seguridad actual*	**Medida de seguridad necesaria***	**Acciones para remediación***
Comentario	Comentario	Comentario
Comentario	Comentario	Comentario
Comentario	Comentario	Comentario
Comentario	Comentario	Comentario

5. PLAN DE TRABAJO

Eliminado: Cuatro renglones en los que se especifican las actividades, dieciséis con la descripción, quince con la duración y diecisiete con la cobertura, correspondientes al plan de trabajo. Fundamento legal: artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública. En virtud de tratarse de información reservada.

Coordinación de Enlace y Seguimiento			
Identificador único¨*	**(SDI-CEYS-1)**		
(Nombre del sistema A1*)	**Solicitud de difusión**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Comentario	Comentario	Comentario	Comentario
Comentario	Comentario	Comentario	Comentario

6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

I. TRANSFERENCIAS DE DATOS PERSONALES

Coordinación de Enlace y Seguimiento	
Identificador único¨*	**(SDI-CEYS-1)**
(Nombre del sistema A1*)	**Solicitud de difusión**
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	No se realiza transferencia mediante soportes físicos
Transferencias mediante el traslado de soportes electrónicos:	No se realiza transferencia mediante soportes electrónicos
Transferencias mediante el traslado sobre redes electrónicas:	No se realiza transferencia mediante redes electrónicas

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

No se realiza resguardo de datos personales en soportes físicos.

III. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

No se cuenta con bitácora para acceso y operación cotidiana.

IV. REGISTRO DE INCIDENTES

No contamos con un procedimiento de atención de incidentes.

V. ACCESO A LAS INSTALACIONES

Aunque no se realiza resguardo de datos personales en soportes físicos, la Coordinación de las Comisiones Locales de Seguridad de la Torre de Rectoría es la encargada de la seguridad de las instalaciones de las diversas dependencias que convivimos en este edificio, por lo que la vigilancia y revisión de acceso y salida está a cargo de dicha Coordinación.

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

No se realiza actualización de datos personales dado que se elimina una vez atendida la solicitud.

VII. PERFILES DE USUARIO Y CONTRASEÑAS

El formulario de registro de actividad no requiere identificación de los usuarios.

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

No se almacenan datos personales.

IX. PLAN DE CONTINGENCIA

No se tiene un plan de contingencia.

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

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

Coordinación de Enlace y Seguimiento		
Identificador único¨*	**(SDI-CEYS-1)**	
(Nombre del sistema A1*)	**Solicitud de difusión**	
Recurso*	**Descripción***	**Control***
N/A	N/A	N/A

7.2 Procedimiento para la revisión de las medidas de seguridad

Coordinación de Enlace y Seguimiento		
Identificador único¨*	**(SDI-CEYS-1)**	
(Nombre del sistema A1*)	**Solicitud de difusión**	
Medida de seguridad*	**Procedimiento***	**Responsable***
N/A	N/A	N/A

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

Coordinación de Enlace y Seguimiento		
Identificador único¨*	**(SDI-CEYS-1)**	
(Nombre del sistema A1*)	**Solicitud de difusión**	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***
N/A	N/A	N/A

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

Coordinación de Enlace y Seguimiento		
Identificador único¨*	**(SDI-CEYS-1)**	
(Nombre del sistema A1*)	**Solicitud de difusión**	
Medida de seguridad*	**Acciones***	**Responsible***

N/A	N/A	N/A

8 PROGRAMA ESPECÍFICO DE CAPACITACIÓN

8.1 Programa de capacitación a los responsables de seguridad de datos personales

Coordinación de Enlace y Seguimiento	
Identificador único¨*	**(SDI-CEYS-1)**
(Nombre del sistema A1*)	**Solicitud de difusión**

Actividad*	**Descripción***	**Duración***	**Cobertura***
La SDI solicitará a la Unidad de Transparencia de la UNAM programar un curso enfocado a la capacitación del personal involucrado en la captación, manejo, resguardo y seguridad de datos personales. De igual forma, se buscarán cursos relacionados que impartan otras instancias como el INAI.	Cursos relacionados con la protección y seguridad de datos personales	Capacitación por lo menos una vez al año.	Deberan asistir por lo menos dos personas de cada área que maneje datos personales en la SDI.

8.2 Programa de difusión de la protección a los datos personales

Coordinación de Enlace y Seguimiento	
Identificador único¨*	**(SDI-CEYS-1)**
(Nombre del sistema A1*)	**Solicitud de difusión**

Actividad*	Descripción*	Duración*	Cobertura*
Difusión de protección de datos personales	El 25 de febrero de 2019, la UNAM difundió en la Gaceta UNAM los Lineamientos para la protección de datos personal en posesión de la UNAM.	Permanente	Institucional

9 MEJORA CONTINUA

9.1 Actualización y mantenimiento de sistemas de información

Coordinación de Enlace y Seguimiento			
Identificador único¨*	**(SDI-CEYS-1)**		
(Nombre del sistema A1*)	**Solicitud de difusión**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Registro de solicitudes de difusión.	Recibir y atender las solicitudes de difusión de información en los canales institucionales de la SDI.	Permanente	Se trata de atender de manera oportuna las solicitudes cada usuario o solicitante.

9.2 Actualización y mantenimiento de equipo de cómputo

Coordinación de Enlace y Seguimiento	
Identificador único¨*	**(SDI-CEYS-1)**
(Nombre del sistema A1*)	**Solicitud de difusión**

Actividad*	Descripción*	Duración*	Cobertura*
Identificar los requerimientos de cada equipo derivado de las actualizaciones de cada plataforma de difusión o redes sociales.	Actualizar los equipos de cómputo para una mejor funcionalidad.	Permanente	Se trata de atender de manera oportuna las solicitudes del usuario.

9.3 Procesos para la conservación, preservación y respaldos de información

Coordinación de Enlace y Seguimiento		
Identificador único¨*	**(SDI-CEYS-1)**	
(Nombre del sistema A1*)	**Solicitud de difusión**	
Proceso*	**Descripción***	**Responsable***
NA	NA	NA

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

Coordinación de Enlace y Seguimiento		
Identificador único¨*	**(SDI-CEYS-1)**	
(Nombre del sistema A1*)	**Solicitud de difusión**	
Proceso	**Descripción***	**Responsable***
Procesos de borrado seguro y disposición final de equipos y componentes informáticos.	Procesos de borrado seguro y disposición final de equipos y componentes informáticos.	Jefa de Departamento de TIC´s.

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

Este sistema no comprende el tratamiento de datos personales.

COORDINACIÓN DE ENLACE Y SEGUIMIENTO:
COORDINADOR DE DISEÑO, IDENTIDAD Y COMUNICACIÓN
(2)

1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Coordinación de Enlace y Seguimiento	
Identificador único*	**(SDI-CEYS-2)**
(Nombre del sistema A1) *	**Gestión de eventos virtuales**
Datos personales (sensibles o no) contenidos en el sistema*	**1. Datos personales en general:** a) **Datos de identificación:** Nombre, correo electrónico (opcional). **Si se graba la sesión:** imagen de perfil o imagen/video en sesión. **Si el asistente solicita constancia:** Nombre, apellidos, correo electrónico, Clave Única de Registro de Población (CURP). Datos laborales: Institución de procedencia. **2. No se recaban datos sensibles.**
Responsable*:	
Nombre*	Rubén Muñiz Arzate
Cargo*	Coordinador de Enlace y Seguimiento.
Funciones*	• Proponer estrategias que permitan impulsar la calidad, innovación e incorporación de nuevas tecnologías, para fortalecer el desarrollo de las Tecnologías de Información y Comunicación (TIC) en la UNAM. • Verificar, en apego a los protocolos y políticas de seguridad de la UNAM, los planes de seguridad para la protección y preservación de la información y de datos personales que se encuentren en posesión de sistemas informáticos desarrollados y/o administrados por la Secretaría de Desarrollo Institucional (SDI). • Supervisar el buen funcionamiento de los servicios de cómputo proporcionados al personal de la SDI. • Diagnosticar y orientar en la gestión de infraestructura tecnológica y de soluciones de cómputo y de telecomunicaciones, para cumplir con los objetivos del Plan de Desarrollo de la UNAM, en materia de TIC.
Obligaciones*	• Conocer, proteger su integridad, resguardar y conservar la privacidad de los datos que se manejan y mantener la secrecía de la información. • Hacer uso de los datos únicamente en el ejercicio de sus funciones y para los fines para los que han sido recabados.

	Encargados:
(Nombre del Encargado 1*)	Linda Ma. del C. Rey Hernández
Cargo*:	Jefa del Departamento de Tecnologías de Información y Comunicación.
Funciones*:	• Administrar y configurar la cuenta de videoconferencia institucional asignada a la Secretaría de Desarrollo Institucional. • Crear, gestionar y monitorear las sesiones procurando la seguridad durante la sesión. • Habilitar sala de espera para evitar ingresos no autorizados. • En los eventos que lo requieran, habilitar y configurar el registro de los participantes y ponentes asignando los permisos correspondientes sobre la sesión. • Informar al organizador del evento las estadísticas y registro de participantes para que pueda expedir constancias a quien cumpla con los requisitos previamente acordados con el público. • Realizar grabaciones y/o transmisiones del evento. • Enviar al organizador la liga de descarga de la grabación de la sesión si es que se realizó.
Obligaciones*:	• Conocer, proteger su integridad, resguardar y conservar la privacidad de los datos que se manejan y mantener la secrecía de la información. • No difundir la información de datos personales contenida en los registros o grabaciones de las sesiones. • Hacer uso de los datos únicamente en el ejercicio de sus funciones y para los fines para los que han sido recabados. • Eliminar la información cuando se haya entregado al organizador. Realizar estadísticas sobre solicitudes al DTIC sin incluir datos personales. • No compartir y resguardar las claves de acceso a la cuenta de la plataforma asignada a la SDI.
	Usuarios:
(Nombre del Usuario 1*)	Organizador o coanfitrión del evento
Cargo*:	Personal de Coordinaciones y Direcciones adscritas a la SDI
Funciones*:	• Solicitar la creación de la sesión de videoconferencia de acuerdo con los requerimientos del evento. • Si se habilita el registro, solicitar los datos generados automáticamente por la plataforma para la creación de constancias a través del Sistema Generador de Constancias (SIGECO) administrado por la Coordinación de Universidad Abierta, Innovación Educativa y Educación a Distancia (CUAIEED).
Obligaciones*:	• Conocer, proteger su integridad, resguardar y conservar la privacidad de los datos que se manejan y mantener la secrecía de la información. • No difundir la información de datos personales contenida en los registros o grabaciones de las sesiones. • Hacer uso de los datos únicamente en el ejercicio de sus funciones y para los fines para los que han sido recabados.

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

Coordinación de Enlace y Seguimiento	
Identificador único¨*	**(SDI-CEYS-2)**
(Nombre del sistema A1*)	**Gestión de eventos virtuales.**
Tipo de soporte: *	Soporte electrónico.
Descripción: *	Nube privada y servidor de correo institucional.
Características del lugar donde se resguardan los soportes: *	Alojamiento en nube privada. Grabaciones locales y correo electrónico institucional alojado en el Centro de Datos de la UNAM para el envío de los enlaces de descarga y archivos de registros.

3. ANÁLISIS DE RIESGOS

Eliminado: Siete renglones en los que se especifican los riesgos, trece con el impacto y veintiuno con la mitigación, correspondientes al análisis de riesgos. Fundamento legal: artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública. En virtud de tratarse de información reservada.

Coordinación de Enlace y Seguimiento		
Identificador único¨*	**(SDI-CEYS-2)**	
(Nombre del sistema A1*)	**Gestión de eventos virtuales.**	
Riesgo*	**Impacto***	**Mitigación***
Comentario	Comentario	Comentario
Comentario	Comentario	Comentario
Comentario	Comentario	Comentario

Eliminado: Un renglón en el que se especifica un riesgo, cuatro con el impacto y trece con la mitigación, correspondientes al análisis de riesgos. Fundamento legal: artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública. En virtud de tratarse de información reservada.

		Comentario
Comentario	Comentario	Comentario

4. ANÁLISIS DE BRECHA

Eliminado: Trece renglones en los que se especifican las medias de seguridad actuales, trece con las medidas de seguridad necesarias y dieciséis con las acciones para remediación, correspondientes al análisis de brecha. Fundamento legal: artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública. En virtud de tratarse de información reservada.

Coordinación de Enlace y Seguimiento		
Identificador único¨*	**(SDI-CEYS-2)**	
(Nombre del sistema A1*)	**Gestión de eventos virtuales.**	
Medida de seguridad actual*	**Medida de seguridad necesaria***	**Acciones para remediación***
Comentario	Comentario	Comentario
Comentario	Comentario	Comentario
Comentario	Comentario	Comentario
Comentario	Comentario	Comentario
Comentario	Comentario	Comentario

5. PLAN DE TRABAJO

Eliminado: Diez renglones en los que se especifican las actividades, treinta y cinco con la descripción, veintiséis con la duración y trece con la cobertura, correspondientes al plan de trabajo. Fundamento legal: artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública. En virtud de tratarse de información reservada.

Coordinación de Enlace y Seguimiento			
Identificador único¨*	**(SDI-CEYS-2)**		
(Nombre del sistema A1*)	**Gestión de eventos virtuales.**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Comentario	Comentario	Comentario	Comentario
Comentario	Comentario	Comentario	Comentario
Comentario	Comentario	Comentario	Comentario

6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

I. TRANSFERENCIAS DE DATOS PERSONALES

Coordinación de Enlace y Seguimiento	
Identificador único¨*	**(SDI-CEYS-2)**
(Nombre del sistema A1*)	**Gestión de eventos virtuales.**
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	No aplica.
Transferencias mediante el traslado de soportes electrónicos:	No aplica.
Transferencias mediante el traslado sobre redes electrónicas:	Las estadísticas de uso y registro de las sesiones, se almacena en la nube privada y los archivos generados son enviados a través del correo electrónico institucional administrado en Centro de Datos UNAM. La información se envía cifrada mediante protocolo SSL/TLS a través de correo electrónico o directamente desde la plataforma.

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

La gestión de eventos virtuales, no realiza tratamiento de datos personales con soportes físicos, ya que se realiza a través de soporte electrónico utilizando la cuenta de plataforma institucional y correo electrónico institucional.

III. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

El administrador de la plataforma UNAM es quien tiene acceso a las bitácoras. Únicamente cuando se envía por correo se pude visualizar la bitácora de envío de información.

IV. REGISTRO DE INCIDENTES:

No contamos con un procedimiento de atención de incidentes.

V. ACCESO A LAS INSTALACIONES

La Coordinación de las Comisiones Locales de Seguridad de la Torre de Rectoría son los encargados de la seguridad de las Instalaciones de las diversas Dependencias que convivimos en este edificio, por lo que la vigilancia y revisión de acceso y salida está a cargo de dicha Coordinación.

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

La plataforma no permite la edición de la información. Cuando se descarga y se envía al usuario final se envía con contraseña.

VII. PERFILES DE USUARIO Y CONTRASEÑAS

El acceso a la plataforma está restringido a un solo usuario de la cuenta quien tiene el perfil para generar y descargar los registros y estadísticas. Las grabaciones pueden ser compartidas con el usuario final a través de una contraseña que únicamente permite visualizar o descargar la grabación según lo requiera cada evento.

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

La información no se respalda.

IX. PLAN DE CONTINGENCIA

No contamos con un plan de contingencia propio, solo nos apegamos al soporte de la plataforma.

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

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

Coordinación de Enlace y Seguimiento		
Identificador único	(SDI-CEYS-2)	
Nombre del sistema	**Gestión de eventos virtuales.**	
Recurso*	**Descripción***	**Control***
N/A	N/A	N/A

7.2 Procedimiento para la revisión de las medidas de seguridad

Coordinación de Enlace y Seguimiento		
Identificador único	(SDI-CEYS-2)	
Nombre del sistema	**Gestión de eventos virtuales**.	
Medida de seguridad*	**Procedimiento***	**Responsable***
N/A	N/A	N/A

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

Coordinación de Enlace y Seguimiento		
Identificador único	(SDI-CEYS-2)	
Nombre del sistema	**Gestión de eventos virtuales.**	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***
N/A	N/A	N/A

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

Coordinación de Enlace y Seguimiento		
Identificador único	(SDI-CEYS-2)	
(Nombre del sistema A1)*	**Gestión de eventos virtuales**.	
Medida de seguridad*	**Acciones***	**Responsable***
N/A	N/A	N/A

8 PROGRAMA ESPECÍFICO DE CAPACITACIÓN

8.1 Programa de capacitación a los responsables de seguridad de datos personales

Coordinación de Enlace y Seguimiento			
Identificador único	(SDI-CEYS-2)		
Nombre del sistema	**Gestión de eventos virtuales.**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
La SDI solicitará a la Unidad de Transparencia de la UNAM programar un curso enfocado a la capacitación del personal involucrado en la captación, manejo, resguardo y seguridad de datos personales. De igual forma, se buscarán cursos relacionados que impartan otras instancias como el INAI.	Cursos relacionados con la protección y seguridad de datos personales	Capacitación por lo menos una vez al año.	Deberan asistir por lo menos dos personas de cada área que maneje datos personales en la SDI.

8.2 Programa de difusión de la protección a los datos personales

Coordinación de Enlace y Seguimiento			
Identificador único	(SDI-CEYS-2)		
Nombre del sistema	**Gestión de eventos virtuales**.		
Actividad*	**Descripción***	**Duración***	**Cobertura***

Difusión de protección de datos personales	El 25 de febrero de 2019, la UNAM difundió en la Gaceta UNAM los Lineamientos para la protección de datos personal en posesión de la UNAM.	Permanente	Institucional

9 MEJORA CONTINUA

9.1 Actualización y mantenimiento de sistemas de información

Coordinación de Enlace y Seguimiento			
Identificador único*	(SDI-CEYS-2)		
Nombre del sistema	**Gestión de eventos virtuales**.		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Actualización de software	Mantener actualizado el sistema en los equipos.	Permanente	Usuarios

9.2 Actualización y mantenimiento de equipo de cómputo

Coordinación de Enlace y Seguimiento			
Identificador único	(SDI-CEYS-2)		
Nombre del sistema	**Gestión de eventos virtuales**.		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Mantenimiento preventivo	Realizar el mantenimiento preventivo del equipo de trabajo tanto a nivel hardware como software para mantenerlo funcional.	2 veces al año	Equipos de la oficina de la SDI.

9.3 Procesos para la conservación, preservación y respaldos de información

Coordinación de Enlace y Seguimiento		
Identificador único	(SDI-CEYS-2)	
Nombre del sistema	**Gestión de eventos virtuales.**	
Proceso*	**Descripción***	**Responsable***
N/A	N/A	N/A

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

Coordinación de Enlace y Seguimiento	
Identificador único	(SDI-CEYS-2)
Nombre del sistema	**Gestión de eventos virtuales**.

Proceso	Descripción*	Responsable*
Procesos de borrado seguro y disposición final de equipos y componentes informáticos.	Procesos de borrado seguro y disposición final de equipos y componentes informáticos. Formato de bajo nivel realizado en los discos de equipos que se transfieren o se dan de baja.	Jefa del Departamento de TIC.

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

Este proceso se es realizado por el Administrador central (DGTIC) de la plataforma, que son los que tienen un sistema de tratamiento de datos personales.

COORDINACIÓN DE ENLACE Y SEGUIMIENTO
DEPARTAMENTO DE GESTIÓN INSTITUCIONAL
(3)

1. **INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES**

Coordinación de Enlace y Seguimiento	
Identificador único*	**(SDI-CEYS-3)**
(Nombre del sistema A1) *	**Bitácora del responsable Sanitario de la SDI / Comité de Seguimiento COVID-19**
Datos personales (sensibles o no) contenidos en el sistema*	**1. Datos personales en general:** **a) Datos de identificación:** Nombre, correo electrónico, RFC. **b) Datos laborales:** Número de Trabajador, Nombramiento, correo electrónico institucional. 2**. Datos personales sensibles:** Estado de salud del personal de la SDI, sospechoso o confirmado de COVID-19 y esquema de vacunación de COVID-19.
Responsable*:	
Nombre*	Rubén Muñiz Arzate
Cargo*	Coordinador de Enlace y Seguimiento
Funciones*	• Difundir las medidas implementadas por la Universidad para la protección de la salud de la comunidad, en apego a los Lineamientos generales para el regreso a las actividades universitarias en el marco de la pandemia de COVID-19. • Recibir a través del correo institucional, la notificación por parte del personal de la SDI, sospechoso o confirmado de la enfermedad COVID-19. • Establecer comunicación con el personal de la SDI, que se reporten como sospechosos o confirmados de COVID-19. • En los casos confirmados de COVID 19, promover el cumplimiento del Protocolo para el regreso a las actividades universitarias en el marco de la pandemia de COVID–19, de la Secretaría de Desarrollo Institucional (SDI). • Mantener actualizada la Bitácora del responsable Sanitario en la plataforma del Comité de Seguimiento Covid-19, que incluye: – El personal de la SDI que pertenecen a la población en probable situación de vulnerabilidad, de acuerdo con los criterios de vulnerabilidad que emite el Comité de Expertos o las autoridades de salud.

	– Registro de personal sospechosas o confirmadas de COVID-19. – Registro de personal con esquema de vacunación de la SDI.
Obligaciones*	• Conocer, proteger su integridad, resguardar y conservar la privacidad de los datos que se manejan y mantener la secrecía de la información. • Hacer uso de los datos únicamente en el ejercicio de sus funciones y para los fines para los que han sido recabados.
	Encargados:
(Nombre del Encargado 1*)	Emma Patricia Camacho Bustamante
Cargo*:	Jefa del Departamento de Gestión Institucional
Funciones*:	• Mantener informados al personal de la SDI, sobre la evolución de la pandemia a través de mensajes, utilizando todos los medios a la disposición. • Supervisar que en las instalaciones de la SDI se cumplan las condiciones y procedimientos señalados en los Lineamientos generales para el regreso a las actividades universitarias en el marco de la pandemia de COVID-19. • Informar al Comité de Seguimiento de cualquier incidencia en la SDI relacionada con el funcionamiento de estos Lineamientos o la emergencia sanitaria. • Promover los principios rectores de los Lineamientos generales para el regreso a las actividades universitarias en el marco de la pandemia de COVID-19, con especial énfasis en la "No Discriminación" para las personas que hayan tenido COVID-19 o hayan convivido con algún familiar que lo tenga o haya tenido.
Obligaciones*:	• Seguimiento cronológico del estado del personal de la SDI que se reportaron como sospechosas o confirmadas por COVID-19, atendiendo la normatividad en el uso de datos personales. • Conocer, proteger su integridad, resguardar y conservar la privacidad de los datos que se manejan y mantener la secrecía de la información. • Hacer uso de los datos únicamente en el ejercicio de sus funciones y para los fines para los que han sido recabados.
	Usuarios:
(Nombre del Usuario 1*)	Sara Angélica Hernández Bautista
Cargo*:	Jefa de la Unidad Administrativa
Funciones*:	• Estar informada del personal de la SDI que se reportan como sospechosos o confirmados de COVID-19. • Identificar, con la ayuda de los funcionarios de cada área, al personal a su cargo en posible situación de vulnerabilidad de acuerdo con los criterios que emita el Comité de Expertos o las autoridades de salud.

	• Autorizar, de ser posible, el ingreso de trabajadores en horarios escalonados para evitar los horarios pico en el transporte público. • Establecer horarios escalonados para los trabajadores en área de alimentos, comedores o vestidores para reducir el riesgo de exposición.
Obligaciones*:	• Hacer uso de los datos únicamente en el ejercicio de sus funciones y para los fines para los que han sido recabados.

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

Coordinación de Enlace y Seguimiento	
Identificador único¨*	**(SDI-CEYS-3)**
(Nombre del sistema A1*)	**Comité de Seguimiento COVID-19 / Bitácora del responsable Sanitario de la SDI**
Tipo de soporte: *	Soporte electrónico
Descripción: *	Soporte electrónico: • Disco magnético HD. • Nube privada.
Características del lugar donde se resguardan los soportes: *	Disco magnético HD de la computadora asignada al Departamento de Gestión Institucional Nube privada asociada a la cuenta de correo institucional del Departamento de Gestión Institucional. Plataforma del Comité de Seguimiento COVID-19, en servidor administrado por la Secretaría Administrativa de la UNAM.

3. ANÁLISIS DE RIESGOS

Eliminado: Once renglones en los que se especifican los riesgos, veintiuno con el impacto y veinticinco con la mitigación, correspondientes al análisis de riesgos. Fundamento legal: artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública. En virtud de tratarse de información reservada.

Coordinación de Enlace y Seguimiento		
Identificador único¨*	**(SDI-CEYS-3)**	
(Nombre del sistema A1*)	**Comité de Seguimiento COVID-19 / Bitácora del responsable Sanitario de la SDI**	
Riesgo*	**Impacto***	**Mitigación***
Comentario	Comentario	Comentario
Comentario	Comentario	Comentario
Comentario	Comentario	Comentario
Comentario	Comentario	Comentario

		Comentario [redacted]

Eliminado: Cuatro renglones en los que se especifica la mitigación, correspondientes al análisis de riesgos. Fundamento legal: artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública. En virtud de tratarse de información reservada.

4. ANÁLISIS DE BRECHA

Eliminado: Diecisiete renglones en los que se especifican las medias de seguridad actuales, trece con las medidas de seguridad necesarias y
doce con las acciones para remediación,
correspondientes al análisis de brecha. Fundamento legal: artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública. En virtud de tratarse de información reservada.

Coordinación de Enlace y Seguimiento		
Identificador único¨*	**(SDI-CEYS-3)**	
(Nombre del sistema A1*)	**Comité de Seguimiento COVID-19 / Bitácora del responsable Sanitario de la SDI**	
Medida de seguridad actual*	**Medida de seguridad necesaria***	**Acciones para remediación***
Comentario	Comentario	Comentario
Comentario	Comentario	Comentario
Comentario	Comentario	Comentario

5. PLAN DE TRABAJO

Eliminado: Cuatro renglones en los que se especifican las actividades, trece con la descripción, uno con la duración y tres con la cobertura, correspondientes al plan de trabajo. Fundamento legal: artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública. En virtud de tratarse de información reservada.

Coordinación de Enlace y Seguimiento			
Identificador único¨*	**(SDI-CEYS-3)**		
(Nombre del sistema A1*)	**Comité de Seguimiento COVID-19 / Bitácora del responsable Sanitario de la SDI**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Comentario	Comentario	Comentario	Comentario

6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

I. TRANSFERENCIAS DE DATOS PERSONALES

Coordinación de Enlace y Seguimiento	
Identificador único¨*	**(SDI-CEYS-3)**
(Nombre del sistema A1*)	**Comité de Seguimiento COVID-19 / Bitácora del responsable Sanitario de la SDI**
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	No aplica
Transferencias mediante el traslado de soportes electrónicos:	No aplica
Transferencias mediante el traslado sobre redes electrónicas:	La transferencia de la información es cifrada mediante protocolos SSL/TLS en la red interna.

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

La Bitácora del responsable Sanitario de la SDI no realiza tratamiento de datos personales con soportes físicos, ya que se encuentra en electrónico a través del mismo sistema.

III. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

La Bitácora del responsable Sanitario de la SDI cuenta con una opción de Consulta, la cual permite visualizar el reporte de los casos sospechosos o confirmados, así como el esquema de vacunación del personal de la SDI.

V. REGISTRO DE INCIDENTES

No contamos con un procedimiento de atención de incidentes.

V. ACCESO A LAS INSTALACIONES

La Coordinación de las Comisiones Locales de Seguridad de la Torre de Rectoría son los encargados de la seguridad de las Instalaciones de las diversas Dependencias que convivimos en este Edificio, por lo que la vigilancia y revisión de acceso y salida está a cargo de dicha Coordinación.

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

La Secretaría Administrativa de la UNAM, es la encargada realizar las actualizaciones y/o notificaciones de los posibles cambios realizados a la Plataforma.

VII. PERFILES DE USUARIO Y CONTRASEÑAS

La Plataforma del Comité de Seguimiento COVID-19 de la UNAM está diseñado para que cada responsable Sanitario tenga un usuario y contraseña, para ingresar a la Bitácora de responsable Sanitario de su dependencia, para la actualización. Los usuarios y contraseñas son autorizados por el Comité de Seguimiento.

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

Esta actividad es garantizada por el Comité de Seguimiento a través de la Secretaría Administrativa de la UNAM.

IX. PLAN DE CONTINGENCIA

Esta actividad es garantizada por el Comité de Seguimiento a través de la Secretaría Administrativa de la UNAM.

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

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

Coordinación de Enlace y Seguimiento	
Identificador único	**(SDI-CEYS-3)**
Nombre del sistema	**Comité de Seguimiento COVID-19 / Bitácora del responsable Sanitario de la SDI**

Recurso*	Descripción*	Control*
N/A	N/A	N/A

7.2 Procedimiento para la revisión de las medidas de seguridad

Coordinación de Enlace y Seguimiento		
Identificador único	**(SDI-CEYS-3)**	
Nombre del sistema	**Comité de Seguimiento COVID-19 / Bitácora del responsable Sanitario de la SDI**	
Medida de seguridad*	**Procedimiento***	**Responsable***
N/A	N/A	N/A

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

Coordinación de Enlace y Seguimiento		
Identificador único	**(SDI-CEYS-3)**	
Nombre del sistema	**Comité de Seguimiento COVID-19 / Bitácora del responsable Sanitario de la SDI**	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***
N/A	N/A	N/A

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

Coordinación de Enlace y Seguimiento	
Identificador único	**(SDI-CEYS-3)**

(Nombre del sistema A1)*	Comité de Seguimiento COVID-19 / Bitácora del responsable Sanitario de la SDI	
Medida de seguridad*	**Acciones***	**Responsable***
N/A	N/A	N/A

8 PROGRAMA ESPECÍFICO DE CAPACITACIÓN

8.1 Programa de capacitación a los responsables de seguridad de datos personales

Coordinación de Enlace y Seguimiento			
Identificador único	**(SDI-CEYS-3)**		
Nombre del sistema	**Comité de Seguimiento COVID-19 / Bitácora del responsable Sanitario de la SDI**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
La SDI solicitará a la Unidad de Transparencia de la UNAM programar un curso enfocado a la capacitación del personal involucrado en la captación, manejo, resguardo y seguridad de datos personales. De igual forma, se buscarán cursos relacionados que impartan otras instancias como el INAI.	Cursos relacionados con la protección y seguridad de datos personales	Capacitación por lo menos una vez al año.	Deberan asistir por lo menos dos personas de cada área que maneje datos personales en la SDI.

8.2 Programa de difusión de la protección a los datos personales

Coordinación de Enlace y Seguimiento			
Identificador único	**(SDI-CEYS-3)**		
Nombre del sistema	**Comité de Seguimiento COVID-19 / Bitácora del responsable Sanitario de la SDI**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Difusión de protección de datos personales	El 25 de febrero de 2019, la UNAM difundió en la Gaceta UNAM los Lineamientos para la protección de datos personal en posesión de la UNAM.	Permanente	Institucional

9 MEJORA CONTINUA

9.1 Actualización y mantenimiento de sistemas de información

Coordinación de Enlace y Seguimiento			
Identificador único*	**(SDI-CEYS-3)**		
Nombre del sistema	**Comité de Seguimiento COVID-19 / Bitácora del responsable Sanitario de la SDI**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Registro de casos sospechosos, confirmados y esquema de vacunación.	Alimentar la bitácora del responsable Sanitario de la SDI.	Hasta que las autoridades lo consideren pertinente.	Contribuir a mantener actualizados los datos para el Comité de Seguimiento COVD-19 de la UNAM.

9.2 Actualización y mantenimiento de equipo de cómputo

Coordinación de Enlace y Seguimiento			
Identificador único	**(SDI-CEYS-3)**		
Nombre del sistema	**Comité de Seguimiento COVID-19 / Bitácora del responsable Sanitario de la SDI**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Identificar los requerimientos técnicos, para ingresar a la Bitácora del responsable Sanitario del Comité de Seguimiento COVID-19.	Proporcionar a las áreas de trabajo los equipos de cómputo para una mejor funcionalidad.	Permanente	Se trata de mantener actualizada la Bitácora sobre el Seguimiento Covid-19.

9.3 Procesos para la conservación, preservación y respaldos de información

Coordinación de Enlace y Seguimiento		
Identificador único	**(SDI-CEYS-3)**	
Nombre del sistema	**Comité de Seguimiento COVID-19 / Bitácora del responsable Sanitario de la SDI**	
Proceso*	**Descripción***	**Responsable***
N/A	N/A	Esta actividad la realiza la Secretaría Administrativa de la UNAM.

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

Coordinación de Enlace y Seguimiento		
Identificador único	**(SDI-CEYS-3)**	
Nombre del sistema	**Comité de Seguimiento COVID-19 / Bitácora del responsable Sanitario de la SDI**	
Proceso	**Descripción***	**Responsable***
Procesos de borrado seguro y disposición final de equipos y componentes informáticos.	Procesos de borrado seguro y disposición final de equipos y componentes informáticos.	Jefa de Departamento de Gestión Institucional

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

Las personas que cuenten con usuario y contraseña en la Bitácora del responsable Sanitario del Comité de Seguimiento COVID-19, no tiene injerencia en el procedimiento para la cancelación del sistema de tratamiento de datos personales, debido a que esta actividad depende de la Secretaría Administrativa de la UNAM.

COORDINACIÓN DE ENLACE Y SEGUIMIENTO:
DEPARTAMENTO DE TIC
(4)

1. **INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES**

Coordinación de Enlace y Seguimiento	
Identificador único*	**(SDI-CEYS-4)**
(Nombre del sistema A1) *	**Gestión de correo electrónico institucional.**
Datos personales (sensibles o no) contenidos en el sistema*	**1. Datos personales en general:** a) **Datos de identificación:** Nombre, correo electrónico y RFC. b) **Datos laborales:** Nombramiento, área de adscripción, número de trabajador. 2. **No se recaban datos sensibles**.
Responsable*:	
Nombre*	Rubén Muñiz Arzate
Cargo*	Coordinador de Enlace y Seguimiento
Funciones*	• Proponer estrategias que permitan impulsar la calidad, innovación e incorporación de nuevas tecnologías, para fortalecer el desarrollo de las Tecnologías de Información y Comunicación (TIC) en la UNAM. • Verificar, en apego a los protocolos y políticas de seguridad de la UNAM, los planes de seguridad para la protección y preservación de la información y de datos personales que se encuentren en posesión de sistemas informáticos desarrollados y/o administrados por la Secretaría de Desarrollo Institucional (SDI). • Supervisar el buen funcionamiento de los servicios de cómputo proporcionados al personal de la SDI. • Designar, por parte de la SDI, al usuario con acceso del Sistema de Servicios de TIC (GTIC) de la Dirección General de Cómputo y de Tecnologías de Información y Comunicación (DGTIC).
Obligaciones*	• Conocer, proteger su integridad, resguardar y conservar la privacidad de los datos que se manejan y mantener la secrecía de la información. • Hacer uso de los datos únicamente en el ejercicio de sus funciones y para los fines para los que han sido recabados.
	Encargados:

(Nombre del Encargado 1*)	Linda Ma. del C. Rey Hernández
Cargo*:	Jefa del Departamento de Tecnologías de Información y Comunicación.
Funciones*:	• Recibir y revisar las solicitudes para asignar una cuenta de correo institucional al personal de la SDI que lo requiera. • Dar trámite a la creación de cuenta de correo electrónico institucional en el Sistema de Servicios de TIC (GTIC) de la Dirección General de Cómputo y de Tecnologías de Información y Comunicación (DGTIC). • Llevar a cabo el seguimiento de la solicitud en el Sistema GTIC y dar atención al ticket de servicio asignado. • Si la asignación de la cuenta de correo es favorable, informar al solicitante que se generó su correo institucional y que sus datos de acceso se recibirán en el correo alterno que proporcionó.
Obligaciones*:	• Conocer, proteger su integridad, resguardar y conservar la privacidad de los datos que se manejan y mantener la secrecía de la información. • No difundir la información de datos personales contenida en la solicitud. • Hacer uso de los datos únicamente en el ejercicio de sus funciones y para los fines para los que han sido recabados. • Eliminar la información cuando la solicitud sea aprobada por la DGTIC a través del GTIC. • No compartir y resguardar las claves de acceso al sistema GTIC.

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

Coordinación de Enlace y Seguimiento	
Identificador único¨*	**(SDI-CEYS-4)**
(Nombre del sistema A1*)	**Gestión de correo electrónico institucional.**
Tipo de soporte: *	Soporte electrónico.
Descripción: *	Nube privada.
Características del lugar donde se resguardan los soportes: *	Alojamiento en nube privada.

3. ANÁLISIS DE RIESGOS

Eliminado: Seis renglones en los que se especifican los riesgos, doce con el impacto y veintiséis con la mitigación, correspondientes al análisis de riesgos. Fundamento legal: artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública. En virtud de tratarse de información reservada.

Coordinación de Enlace y Seguimiento		
Identificador único¨*	**(SDI-CEYS-4)**	
(Nombre del sistema A1*)	**Gestión de correo electrónico institucional.**	
Riesgo*	**Impacto***	**Mitigación***
Comentario	Comentario	Comentario
Comentario	Comentario	Comentario
Comentario	Comentario	Comentario

4. ANÁLISIS DE BRECHA

Eliminado: Once renglones en los que se especifican las medias de seguridad actuales, doce con las medidas de seguridad necesarias y doce con las acciones para remediación, correspondientes al análisis de brecha. Fundamento legal: artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública. En virtud de tratarse de información reservada.

Coordinación de Enlace y Seguimiento		
Identificador único¨*	**(SDI-CEYS-4)**	
(Nombre del sistema A1*)	**Gestión de correo electrónico institucional.**	
Medida de seguridad actual*	**Medida de seguridad necesaria***	**Acciones para remediación***
Comentario	Comentario	Comentario
Comentario	Comentario	Comentario
Comentario	Comentario	Comentario
Comentario	Comentario	Comentario

5. PLAN DE TRABAJO

Eliminado: Seis renglones en los que se especifican las actividades, treinta y cinco con la descripción, veinticuatro con la duración y dieciocho con la cobertura, correspondientes al plan de trabajo. Fundamento legal: artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública. En virtud de tratarse de información reservada.

Coordinación de Enlace y Seguimiento			
Identificador único¨*	**(SDI-CEYS-4)**		
(Nombre del sistema A1*)	**Gestión de correo electrónico institucional.**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Comentario	Comentario	Comentario	Comentario
Comentario	Comentario	Comentario	Comentario
Comentario	Comentario	Comentario	Comentario

6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

I. TRANSFERENCIAS DE DATOS PERSONALES

Coordinación de Enlace y Seguimiento	
Identificador único¨*	**(SDI-CEYS-4)**
(Nombre del sistema A1*)	**Gestión de correo electrónico institucional.**
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	No aplica.
Transferencias mediante el traslado de soportes electrónicos:	No aplica.
Transferencias mediante el traslado sobre redes electrónicas:	El formulario se almacena en nube privada y la información se envía cifrada mediante protocolo SSL/TLS al Sistema de Servicios de TIC (GTIC) de la Dirección General de Cómputo y de Tecnologías de Información y Comunicación (DGTIC). El sistema GTIC envía correo de recepción y queda grabado como ticket durante el proceso y como histórico en su bitácora.

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

El proceso de Gestión de correo electrónico institucional no realiza tratamiento de datos personales con soportes físicos, ya que se realiza a través de soporte electrónico utilizando formularios en nube privada y se transfiere al Sistema de Servicios de TIC (GTIC) de la Dirección General de Cómputo y de Tecnologías de Información y Comunicación (DGTIC).

III. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

En el formulario donde se recaban los datos personales se pude visualizar la bitácora de envío de información y la actividad en la cuenta. Una vez atendido el proceso se elimina la respuesta y no se resguarda información.

VI. REGISTRO DE INCIDENTES:

No contamos con un procedimiento de atención de incidentes.

V. ACCESO A LAS INSTALACIONES

La Coordinación de las Comisiones Locales de Seguridad de la Torre de Rectoría son los encargados de la seguridad de las Instalaciones de las diversas Dependencias que convivimos en este edificio, por lo que la vigilancia y revisión de acceso y salida está a cargo de dicha Coordinación.

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

En el formulario que se maneja internamente no se puede modificar la información. Una vez cargado en el GTIC solo los administradores de dicho sistema pueden realizar actualizaciones.

VII. PERFILES DE USUARIO Y CONTRASEÑAS

El formulario en el que se recaba la solicitud no requiere la identificación del usuario para enviar la solicitud. En el GTIC únicamente el Responsable de TIC de la SDI tiene acceso para realizar las solicitudes y dar seguimiento.

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

El formulario de solicitud no se respalda. La información contenida en el GTIC es responsabilidad de la DGTIC.

IX. PLAN DE CONTINGENCIA

Esta actividad es garantizada por el GTIC de la DGTIC.

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

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

Coordinación de Enlace y Seguimiento		
Identificador único	(SDI-CEYS-4)	
Nombre del sistema	**Gestión de correo electrónico institucional.**	
Recurso*	**Descripción***	**Control***
N/A	N/A	N/A

7.2 Procedimiento para la revisión de las medidas de seguridad

Coordinación de Enlace y Seguimiento		
Identificador único	(SDI-CEYS-4)	
Nombre del sistema	**Gestión de correo electrónico institucional.**	
Medida de seguridad*	**Procedimiento***	**Responsable***
N/A	N/A	N/A

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

Coordinación de Enlace y Seguimiento		
Identificador único	(SDI-CEYS-4)	
Nombre del sistema	**Gestión de correo electrónico institucional.**	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***
N/A	N/A	N/A

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

Coordinación de Enlace y Seguimiento		
Identificador único	(SDI-CEYS-4)	
(Nombre del sistema A1)*	**Gestión de correo electrónico institucional.**	
Medida de seguridad*	**Acciones***	**Responsable***
N/A	N/A	N/A

8. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

8.1 Programa de capacitación a los responsables de seguridad de datos personales

Coordinación de Enlace y Seguimiento			
Identificador único	(SDI-CEYS-4)		
Nombre del sistema	**Gestión de correo electrónico institucional.**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
La SDI solicitará a la Unidad de Transparencia de la UNAM programar un curso enfocado a la capacitación del personal involucrado en la captación, manejo, resguardo y seguridad de datos personales. De igual forma, se buscarán cursos relacionados que impartan otras instancias como el INAI.	Cursos relacionados con la protección y seguridad de datos personales	Capacitación por lo menos una vez al año.	Deberan asistir por lo menos dos personas de cada área que maneje datos personales en la SDI.

8.2 Programa de difusión de la protección a los datos personales

Coordinación de Enlace y Seguimiento			
Identificador único	(SDI-CEYS-4)		
Nombre del sistema	**Gestión de correo electrónico institucional.**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Difusión de protección de datos personales	El 25 de febrero de 2019, la UNAM difundió en la	Permanente	Institucional

	Gaceta UNAM los Lineamientos para la protección de datos personal en posesión de la UNAM.		

9. MEJORA CONTINUA

9.1 Actualización y mantenimiento de sistemas de información

Coordinación de Enlace y Seguimiento			
Identificador único*	(SDI-CEYS-4)		
Nombre del sistema	**Gestión de correo electrónico institucional.**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Creación de sistema interno para gestión de solicitudes	Desarrollar un sistema interno que permita la gestión de solicitudes de servicio que permita un mejor control sobre los datos personales que se requieren para la atención al usuario.	Cuarto trimestre 2022	Coordinaciones, Direcciones y Seminarios Universitarios adscritos a la SDI.

9.2 Actualización y mantenimiento de equipo de cómputo

Coordinación de Enlace y Seguimiento			
Identificador único	(SDI-CEYS-4)		
Nombre del sistema	**Gestión de correo electrónico institucional.**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Mantenimiento preventivo	Realizar el mantenimiento preventivo del equipo de trabajo tanto a nivel hardware como software para mantenerlo funcional.	2 veces al año	Equipos de la oficina de la SDI.

9.3 Procesos para la conservación, preservación y respaldos de información

Coordinación de Enlace y Seguimiento		
Identificador único	(SDI-CEYS-4)	
Nombre del sistema	**Gestión de correo electrónico institucional.**	
Proceso*	**Descripción***	**Responsable***
N/A	N/A	N/A

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

Coordinación de Enlace y Seguimiento		
Identificador único	(SDI-CEYS-4)	
Nombre del sistema	**Gestión de correo electrónico institucional.**	
Proceso	**Descripción***	**Responsable***
Procesos de borrado seguro y disposición final de equipos y componentes informáticos.	Procesos de borrado seguro y disposición final de equipos y componentes informáticos. Formato de bajo nivel realizado en los discos de equipos que se transfieren o se dan de baja.	Jefa del Departamento de TIC.

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

Este proceso se administra en un sistema UNAM, que son los que tienen el sistema de tratamiento de datos personales.

COORDINACIÓN DE ENLACE Y SEGUIMIENTO
DEPARTAMENTO DE TIC
(5)

1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Coordinación de Enlace y Seguimiento	
Identificador único*	**(SDI-CEYS-5)**
(Nombre del sistema A1) *	**Solicitud de servicios TIC.**
Datos personales (sensibles o no) contenidos en el sistema*	**1. Datos personales en general:** a) **Datos de identificación:** Nombre y correo electrónico. b) **Datos laborales:** Correo electrónico institucional. 2. **No se recaban datos sensibles**.
Responsable*:	
Nombre*	Rubén Muñiz Arzate
Cargo*	Coordinador de Enlace y Seguimiento
Funciones*	• Proponer estrategias que permitan impulsar la calidad, innovación e incorporación de nuevas tecnologías, para fortalecer el desarrollo de las Tecnologías de Información y Comunicación (TIC) en la UNAM. • Verificar, en apego a los protocolos y políticas de seguridad de la UNAM, los planes de seguridad para la protección y preservación de la información y de datos personales que se encuentren en posesión de sistemas informáticos desarrollados y/o administrados por la Secretaría de Desarrollo Institucional (SDI). • Supervisar el buen funcionamiento de los servicios de cómputo proporcionados al personal de la SDI. • Designar, por parte de la SDI, al usuario con acceso del Sistema de Servicios de TIC (GTIC) de la Dirección General de Cómputo y de Tecnologías de Información y Comunicación (DGTIC). • Diagnosticar y orientar en la gestión de infraestructura tecnológica y de soluciones de cómputo y de telecomunicaciones, para cumplir con los objetivos del Plan de Desarrollo de la UNAM, en materia de TIC.
Obligaciones*	• Conocer, proteger su integridad, resguardar y conservar la privacidad de los datos que se manejan y mantener la secrecía de la información. • Hacer uso de los datos únicamente en el ejercicio de sus funciones y para los fines para los que han sido recabados.

	Encargados:
(Nombre del Encargado 1*)	Linda Ma. del C. Rey Hernández
Cargo*:	Jefa del Departamento de Tecnologías de Información y Comunicación.
Funciones*:	• Recibir y revisar las solicitudes que ingresan al Departamento de Tecnologías de Información y Comunicación (DTIC) de la SDI. • Gestionar y dar seguimiento a los servicios de TIC que así lo requieran en el Sistema de Servicios de TIC (GTIC) de la Dirección General de Cómputo y de Tecnologías de Información y Comunicación (DGTIC), por ejemplo, alta de dominio, servicios de DNS, creación de cuentas institucionales, licenciamiento de software institucional, solicitud de alojamiento web o infraestructura virtual. • Realizar las solicitudes de servicios TIC que se atienden directamente en el DTIC, como la difusión de eventos, actualización de páginas web administradas en el departamento, soporte técnico, gestión de salas de videoconferencia, asesorías en TIC. • Informar al solicitante el estado de su solicitud o si ya se ha concluido.
Obligaciones*:	• Conocer, proteger su integridad, resguardar y conservar la privacidad de los datos que se manejan y mantener la secrecía de la información. • No difundir la información de datos personales contenida en la solicitud. • Hacer uso de los datos únicamente en el ejercicio de sus funciones y para los fines para los que han sido recabados. • Eliminar la información al finalizar el año. Realizar estadísticas sobre solicitudes al DTIC sin incluir datos personales. • No compartir y resguardar las claves de acceso al sistema GTIC.

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

Coordinación de Enlace y Seguimiento	
Identificador único¨*	**(SDI-CEYS-5)**
(Nombre del sistema A1*)	**Solicitud de servicios TIC.**
Tipo de soporte: *	Soporte electrónico.
Descripción: *	Nube privada y servidor de correo institucional.

Características del lugar donde se resguardan los soportes: *	Alojamiento en nube privada y correo electrónico institucional alojado localmente en el Centro de Datos de la UNAM.

3. ANÁLISIS DE RIESGOS

Eliminado: Siete renglones en los que se especifican los riesgos, once con el impacto y veintitrés con la mitigación, correspondientes al análisis de riesgos. Fundamento legal: artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública. En virtud de tratarse de información reservada.

Coordinación de Enlace y Seguimiento		
Identificador único¨*	**(SDI-CEYS-5)**	
(Nombre del sistema A1*)	**Solicitud de servicios TIC.**	
Riesgo*	**Impacto***	**Mitigación***
Comentario	Comentario	Comentario
Comentario	Comentario	Comentario
Comentario	Comentario	Comentario

Eliminado: Un renglón en los que se especifican los riesgos, cuatro con el impacto y once con la mitigación, correspondientes al análisis de riesgos. Fundamento legal: artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública. En virtud de tratarse de información reservada.

		Comentario
Comentario	Comentario	Comentario

4. ANÁLISIS DE BRECHA

Eliminado: Trece renglones en los que se especifican las medias de seguridad actuales, trece con las medidas de seguridad necesarias y diecisiete con las acciones para remediación, correspondientes al análisis de brecha. Fundamento legal: artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública. En virtud de tratarse de información reservada.

Coordinación de Enlace y Seguimiento		
Identificador único¨*	**(SDI-CEYS-5)**	
(Nombre del sistema A1*)	**Solicitud de servicios TIC.**	
Medida de seguridad actual*	**Medida de seguridad necesaria***	**Acciones para remediación***
Comentario	Comentario	Comentario
Comentario	Comentario	Comentario
Comentario	Comentario	Comentario
Comentario	Comentario	Comentario
Comentario	Comentario	Comentario

5. PLAN DE TRABAJO

Eliminado: Seis renglones en los que se especifican las actividades, treinta y cuatro con la descripción, veinticinco con la duración y dieciocho con la cobertura, correspondientes al plan de trabajo. Fundamento legal: artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública. En virtud de tratarse de información reservada.

Coordinación de Enlace y Seguimiento			
Identificador único¨*	**(SDI-CEYS-5)**		
(Nombre del sistema A1*)	**Solicitud de servicios TIC.**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Comentario	Comentario	Comentario	Comentario
Comentario	Comentario	Comentario	Comentario
Comentario	Comentario	Comentario	Comentario

6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

I. TRANSFERENCIAS DE DATOS PERSONALES

Coordinación de Enlace y Seguimiento	
Identificador único¨*	**(SDI-CEYS-5)**
(Nombre del sistema A1*)	**Solicitud de servicios TIC.**
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	No aplica.
Transferencias mediante el traslado de soportes electrónicos:	No aplica.
Transferencias mediante el traslado sobre redes electrónicas:	El formulario se almacena en nube privada y en correo electrónico institucional administrado en Centro de Datos UNAM. La información se envía cifrada mediante protocolo SSL/TLS al Sistema de Servicios de TIC (GTIC) de la Dirección General de Cómputo y de Tecnologías de Información y Comunicación (DGTIC). El sistema GTIC envía correo de recepción y queda grabado como ticket durante el proceso y como histórico en su bitácora.

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

La gestión de solicitudes de servicios TIC, no realiza tratamiento de datos personales con soportes físicos, ya que se realiza a través de soporte electrónico utilizando formularios en nube privada y, en algunos casos, se transfiere al Sistema de Servicios de TIC (GTIC) de la Dirección General de Cómputo y de Tecnologías de Información y Comunicación (DGTIC).

III. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

En el formulario donde se recaban los datos personales se pude visualizar la bitácora de envío de información y la actividad en la cuenta. Una vez atendido el proceso se elimina la respuesta y no se resguarda información.

IV. REGISTRO DE INCIDENTES:

No contamos con un procedimiento de atención de incidentes.

V. ACCESO A LAS INSTALACIONES

La Coordinación de las Comisiones Locales de Seguridad de la Torre de Rectoría son los encargados de la seguridad de las Instalaciones de las diversas Dependencias que convivimos en este edificio, por lo que la vigilancia y revisión de acceso y salida está a cargo de dicha Coordinación.

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

En el formulario que se maneja internamente no se puede modificar la información. Una vez cargado en el GTIC solo los administradores de dicho sistema pueden realizar actualizaciones.

VII. PERFILES DE USUARIO Y CONTRASEÑAS

El formulario en el que se recaba la solicitud no requiere la identificación del usuario para enviar la solicitud. En el GTIC únicamente el Responsable de TIC de la SDI tiene acceso para realizar las solicitudes y dar seguimiento.

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

El formulario de solicitud no se respalda. La información contenida en el GTIC es responsabilidad de la DGTIC.

IX. PLAN DE CONTINGENCIA

Esta actividad es garantizada por el GTIC de la DGTIC.

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

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

Coordinación de Enlace y Seguimiento		
Identificador único	(SDI-CEYS-5)	
Nombre del sistema	**Solicitud de servicios TIC.**	
Recurso*	**Descripción***	**Control***
N/A	N/A	N/A

7.2 Procedimiento para la revisión de las medidas de seguridad

Coordinación de Enlace y Seguimiento		
Identificador único	(SDI-CEYS-5)	
Nombre del sistema	**Solicitud de servicios TIC.**	
Medida de seguridad*	**Procedimiento***	**Responsable***
N/A	N/A	N/A

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

Coordinación de Enlace y Seguimiento		
Identificador único	(SDI-CEYS-5)	
Nombre del sistema	**Solicitud de servicios TIC.**	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***
N/A	N/A	N/A

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

Coordinación de Enlace y Seguimiento		
Identificador único	(SDI-CEYS-5)	
(Nombre del sistema A1)*	**Solicitud de servicios TIC.**	
Medida de seguridad*	**Acciones***	**Responsable***
N/A	N/A	N/A

8 PROGRAMA ESPECÍFICO DE CAPACITACIÓN

8.1 Programa de capacitación a los responsables de seguridad de datos personales

Coordinación de Enlace y Seguimiento			
Identificador único	(SDI-CEYS-5)		
Nombre del sistema	**Solicitud de servicios TIC.**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
La SDI solicitará a la Unidad de Transparencia de la UNAM programar un curso enfocado a la capacitación del personal involucrado en la captación, manejo, resguardo y seguridad de datos personales. De igual forma, se buscarán cursos relacionados que impartan otras instancias como el INAI.	Cursos relacionados con la protección y seguridad de datos personales	Capacitación por lo menos una vez al año.	Deberan asistir por lo menos dos personas de cada área que maneje datos personales en la SDI.

8.2 Programa de difusión de la protección a los datos personales

Coordinación de Enlace y Seguimiento			
Identificador único	(SDI-CEYS-5)		
Nombre del sistema	**Solicitud de servicios TIC.**		
Actividad*	**Descripción***	**Duración***	**Cobertura***

Difusión de protección de datos personales	El 25 de febrero de 2019, la UNAM difundió en la Gaceta UNAM los Lineamientos para la protección de datos personal en posesión de la UNAM.	Permanente	Institucional

9 MEJORA CONTINUA

9.1 Actualización y mantenimiento de sistemas de información

Coordinación de Enlace y Seguimiento			
Identificador único*	(SDI-CEYS-5)		
Nombre del sistema	**Solicitud de servicios TIC.**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Creación de sistema interno para gestión de solicitudes	Desarrollar un sistema interno que permita la gestión de solicitudes de servicio que permita un mejor control sobre los datos personales que se requieren para la atención al usuario.	Cuarto trimestre 2022	Coordinaciones, Direcciones y Seminarios Universitarios adscritos a la SDI.

9.2 Actualización y mantenimiento de equipo de cómputo

Coordinación de Enlace y Seguimiento			
Identificador único	(SDI-CEYS-5)		
Nombre del sistema	**Solicitud de servicios TIC.**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Mantenimiento preventivo	Realizar el mantenimiento preventivo del equipo de trabajo tanto a nivel hardware como software para mantenerlo funcional.	2 veces al año	Equipos de la oficina de la SDI.

9.3 Procesos para la conservación, preservación y respaldos de información

Coordinación de Enlace y Seguimiento		
Identificador único	(SDI-CEYS-5)	
Nombre del sistema	**Solicitud de servicios TIC.**	
Proceso*	**Descripción***	**Responsable***
N/A	N/A	N/A

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

Coordinación de Enlace y Seguimiento		
Identificador único	(SDI-CEYS-5)	
Nombre del sistema	**Solicitud de servicios TIC.**	
Proceso	**Descripción***	**Responsable***
Procesos de borrado seguro y disposición final de equipos y componentes informáticos.	Procesos de borrado seguro y disposición final de equipos y componentes informáticos. Formato de bajo nivel realizado en los discos de equipos que se transfieren o se dan de baja.	Jefa del Departamento de TIC.

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

Este proceso es administrado por la DGTIC, que son los que tienen un sistema de tratamiento de datos personales.

SECRETARÍA TÉCNICA
DEPARTAMENTO DE LA RED DE EDUCACIÓN CONTINUA
(6)

1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Secretaría Técnica de la Secretaría de Desarrollo Institucional	
Identificador único*	**(SDI – ST – REDEC - 6)**
(Nombre del sistema A1) *	**Control de registros para la emisión de constancias - SIGECO**
Datos personales (sensibles o no) contenidos en el sistema*	**1. Datos personales en general:** **a) Datos de identificación:** Nombre completo, correo electrónico, CURP, fecha de nacimiento, nacionalidad. **b) Datos laborales:** Nombramiento, puesto, correo electrónico institucional, teléfono institucional. **c) Datos académicos:** Trayectoria educativa. **2. Datos personales sensibles:** No se solicitan.
Responsable*:	
Nombre*	**Dr. José Alfredo Delgado Guzmán**
Cargo*	Secretario Técnico
Funciones*	• Coordinar, organizar y definir actividades académicas, de formación y capacitación para los integrantes del Comité Editorial de la SDI, los Seminarios Universitarios, la Red de Educación Continua (REDEC) y público en general en el ámbito nacional e internacional laboral. • Promover la evaluación y análisis de los proyectos del Comité Editorial, los Seminarios Universitarios y la Red de Educación Continua.
Obligaciones*	• Conocer, proteger su integridad, resguardar y conservar la privacidad de los datos que se manejan y mantener la secrecía de la información. • Hacer uso de los datos únicamente en el ejercicio de sus funciones y para los fines para los que han sido recabados.
	Encargados:
(Nombre del Encargado 1*)	**Lic. David Méndez Aguilar**
Cargo*:	**Jefa del Departamento de la Red de Educación Continua de la UNAM**

Funciones*:	• Integrar la información estadística de las actividades de Educación Continua producidas por las entidades y dependencias de la REDEC para su análisis y evaluación. • Apoyar en la planeación, coordinación y ejecución de actividades académicas de capacitación y formación para los integrantes de la REDEC.
Obligaciones*:	• Conocer, proteger su integridad, resguardar y conservar la privacidad de los datos que se manejan y mantener la secrecía de la información. • Hacer uso de los datos únicamente en el ejercicio de sus funciones y para los fines para los que han sido recabados.
	Usuarios:
(Nombre del Usuario 1*)	Dirección de Desarrollo de Sistemas para la Educación de la Coordinación de Universidad Abierta, Innovación Educativa y Educación a Distancia (CUAIEED)
Cargo*:	No aplica
Funciones*:	No aplica
Obligaciones*:	No aplica

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

Secretaría Técnica de la Secretaría de Desarrollo Institucional	
Identificador único¨*	**(SDI – ST – REDEC - 6)**
(Nombre del sistema A1*)	**Control de registros para la emisión de constancias - SIGECO**
Tipo de soporte: *	Soporte electrónico
Descripción: *	Hojas de cálculo Excel
Características del lugar donde se resguardan los soportes: *	Archivos almacenados en el equipo designado para actividades REDEC

3. ANÁLISIS DE RIESGOS

Eliminado: Cinco renglones en los que se especifican los riesgos, diez con el impacto y diecinueve con la mitigación, correspondientes al análisis de riesgos. Fundamento legal: artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública. En virtud de tratarse de información reservada.

Secretaría Técnica de la Secretaría de Desarrollo Institucional		
Identificador único¨*	**(SDI – ST – REDEC - 6)**	
(Nombre del sistema A1*)	**Control de registros para la emisión de constancias – SIGECO**	
Riesgo*	**Impacto***	**Mitigación***
Comentario	Comentario	Comentario
Comentario	Comentario	Comentario

Eliminado: Cuatro renglones en los que se especifican los riesgos, quince con el impacto y treinta con la mitigación, correspondientes al análisis de riesgos. Fundamento legal: artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública. En virtud de tratarse de información reservada.

		Comentario
Comentario	Comentario	Comentario
Comentario	Comentario	Comentario
Comentario	Comentario	Comentario

Eliminado: Un renglón en el que se especifica las medias de seguridad actuales, cinco con las medidas de seguridad necesarias y dieciséis con las acciones para remediación, correspondientes al análisis de brecha. Fundamento legal: artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública. En virtud de tratarse de información reservada.

		Comentario
	Comentario	Comentario

4. ANÁLISIS DE BRECHA

Eliminado: Veintisiete renglones en los que se especifican las medias de seguridad actuales, cinco con las medidas de seguridad necesarias y ocho con las acciones para remediación, correspondientes al análisis de brecha. Fundamento legal: artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública. En virtud de tratarse de información reservada.

Secretaría Técnica de la Secretaría de Desarrollo Institucional		
Identificador único¨*	**(SDI – ST – REDEC - 6)**	
(Nombre del sistema A1*)	**Control de registros para la emisión de constancias – SIGECO**	
Medida de seguridad actual*	**Medida de seguridad necesaria***	**Acciones para remediación***
Comentario [redacted]	Comentario [redacted]	Comentario [redacted]

5. PLAN DE TRABAJO

Eliminado: Nueve renglones en los que se especifican las actividades, veintinueve con la descripción, cuatro con la duración y once con la cobertura, correspondientes al plan de trabajo. Fundamento legal: artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública. En virtud de tratarse de información reservada.

Secretaría Técnica de la Secretaría de Desarrollo Institucional			
Identificador único¨*	**(SDI – ST – REDEC-6)**		
(Nombre del sistema A1*)	**Control de registros para la emisión de constancias – SIGECO**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Comentario	Comentario	Comentario	Comentario
Comentario	Comentario	Comentario	Comentario
Comentario	Comentario	Comentario	Comentario
Comentario	Comentario	Comentario	Comentario

Eliminado: Un renglón en el que se especifican las actividades, ocho con la descripción, uno con la duración y tres con la cobertura, correspondientes al plan de trabajo. Fundamento legal: artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública. En virtud de tratarse de información reservada.

	Comentario		
Comentario	Comentario	Comentario	Comentario

6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

I. TRANSFERENCIAS DE DATOS PERSONALES

Secretaría Técnica de la Secretaría de Desarrollo Institucional	
Identificador único¨*	**(SDI – ST – REDEC - 6)**
(Nombre del sistema A1*)	**Control de registros para la emisión de constancias – SIGECO**
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	No se realiza traslado en soporte físico.
Transferencias mediante el traslado de soportes electrónicos:	No se realiza traslado en soporte electrónico.
Transferencias mediante el traslado sobre redes electrónicas:	El formulario se almacena en en equipo de cómputo designado y en correo electrónico institucional administrado por el Centro de Datos de la UNAM. En algunos casos, la información se envía cifrada mediante protocolos SSL/TLS al Sistema de Constancias (SIGECO) administrado por la CUAIEED.

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

El Sistema de Gestión de Constancias (SIGECO), no realiza tratamiento de datos personales con soportes físicos, ya que se encuentra a través de soporte electrónico a través del mismo sistema, el cual esta albergado en los servidores de la CUAIEED.

III. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

El Sistema de Gestión de Constancias (SIGECO) cuenta con una opción de Consulta, la cual permite visualizar los datos que se ingresaron para la emisión de las constancias; así como la fecha y hora en que se emitieron.

IV. REGISTRO DE INCIDENTES:

Se desconoce si se cuenta con este registro, debido a que el sistema es administrado por la CUAIEED.

V. ACCESO A LAS INSTALACIONES

La Coordinación de las Comisiones Locales de Seguridad de la Torre de Rectoría son los encargados de la seguridad de las Instalaciones de las diversas dependencias que convivimos en este edificio, por lo que la vigilancia y revisión de acceso y salida está a cargo de dicha Coordinación.

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

La Coordinación de Universidad Abierta, Innovación Educativa y Educación a Distancia (CUAIEED), es la encargada de realizar las actualizaciones y/o notificaciones de los posibles cambios realizados al sistema.

VII. PERFILES DE USUARIO Y CONTRASEÑAS

El Sistema de Gestión de Constancias (SIGECO) fue diseñado para que cada persona responsable tenga un usuario y contraseña y pueda tener acceso al sistema para cargar la información confidencial y pueda realizar la emisión de constancias correspondientes. Los usuarios y contraseñas son autorizados por el administrador del SIGECO, adscrito a la CUAIEED.

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

El respaldo de la información recopilada por la Jefatura de Departamento de la Red de Educación Continua, se realiza mediante hojas de cálculo almacenadas en nube privada.

En cuanto al proceso de recuperación de datos, es responsabilidad del administrador del SIGECO y se desconoce el procedimiento.

IX. PLAN DE CONTINGENCIA

Se desconoce el procedimiento ya que es responsabilidad de la CUIAEED.

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

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

Secretaría Técnica de la Secretaría de Desarrollo Institucional		
Identificador único	(SDI – ST – REDEC - 6)	
Nombre del sistema	**Control de registros para la emisión de constancias - SIGECO**	
Recurso*	**Descripción***	**Control***
N/A	N/A	N/A

7.2 Procedimiento para la revisión de las medidas de seguridad

Secretaría Técnica de la Secretaría de Desarrollo Institucional		
Identificador único	(SDI – ST – REDEC - 6)	
Nombre del sistema	**Control de registros para la emisión de constancias - SIGECO**	
Medida de seguridad*	**Procedimiento***	**Responsable***
N/A	N/A	N/A

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

Secretaría Técnica de la Secretaría de Desarrollo Institucional		
Identificador único	(SDI – ST – REDEC - 6)	
Nombre del sistema	**Control de registros para la emisión de constancias - SIGECO**	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***
N/A	N/A	N/A

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

Secretaría Técnica de la Secretaría de Desarrollo Institucional		
Identificador único	(SDI – ST – REDEC - 6)	
Nombre del sistema	**Control de registros para la emisión de constancias - SIGECO**	
Medida de seguridad*	**Acciones***	**Responsable***
N/A	N/A	a) N/A

8 PROGRAMA ESPECÍFICO DE CAPACITACIÓN

8.1 Programa de capacitación a los responsables de seguridad de datos personales

Secretaría Técnica de la Secretaría de Desarrollo Institucional			
Identificador único	(SDI – ST – REDEC - 6)		
Nombre del sistema	**Control de registros para la emisión de constancias - SIGECO**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
La SDI solicitará a la Unidad de Transparencia de la UNAM programar un curso enfocado a la capacitación del personal involucrado en la captación, manejo, resguardo y seguridad de datos personales. De igual forma, se buscarán cursos relacionados que impartan otras instancias como el INAI.	Cursos relacionados con la protección y seguridad de datos personales	Capacitación por lo menos una vez al año.	Deberan asistir por lo menos dos personas de cada área que maneje datos personales en la SDI.

8.2 Programa de difusión de la protección a los datos personales

Secretaría Técnica de la Secretaría de Desarrollo Institucional			
Identificador único	(SDI – ST – REDEC - 6)		
Nombre del sistema	**Control de registros para la emisión de constancias - SIGECO**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Difusión de protección de datos personales	El 25 de febrero de 2019, la UNAM difundió en la Gaceta UNAM los Lineamientos para la protección de datos personal en posesión de la UNAM	Permanente	Institucional

9 MEJORA CONTINUA

9.1 Actualización y mantenimiento de sistemas de información

Secretaría Técnica de la Secretaría de Desarrollo Institucional			
Identificador único*	(SDI – ST – REDEC - 6)		
Nombre del sistema	**Control de registros para la emisión de constancias - SIGECO**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
N/A	N/A	N/A	N/A

9.2 Actualización y mantenimiento de equipo de cómputo

Secretaría Técnica de la Secretaría de Desarrollo Institucional	
Identificador único	(SDI – ST – REDEC - 6)

Nombre del sistema	Control de registros para la emisión de constancias - SIGECO		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Mantenimiento preventivo	Realizar el mantenimiento preventivo del equipo de cómputo tanto a nivel hardwere como software para su funcionamiento óptimo.	2 veces por año	Equipos de la oficina de la SDI

9.3 Procesos para la conservación, preservación y respaldos de información

Secretaría Técnica de la Secretaría de Desarrollo Institucional		
Identificador único	(SDI – ST – REDEC - 6)	
Nombre del sistema	**Control de registros para la emisión de constancias - SIGECO**	
Proceso*	**Descripción***	**Responsable***
N/A	N/A	Esta actividad la realiza la Coordinación de Universidad Abierta, Innovación Educativa y Educación a Distancia (CUAIEED)

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

Secretaría Técnica de la Secretaría de Desarrollo Institucional	
Identificador único	(SDI – ST – REDEC - 6)

Nombre del sistema	Control de registros para la emisión de constancias - SIGECO	
Proceso	**Descripción***	**Responsable***
Procesos de borrado seguro y disposición final de equipos y componentes informáticos.	Procesos de borrado seguro y disposición final de equipos y componentes informáticos.	Jefa de Departamento de TIC de la SDI

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

Las personas que cuenten con usuario y contraseña al Sistema de Gestión de Constancias (SIGECO, no tiene injerencia en la cancelación de tratamiento de datos personales o del sistema, debido a que esta actividad depende de la Coordinación de Universidad Abierta, Innovación Educativa y Educación a Distancia (CUAIEED)

SECRETARÍA TÉCNICA
DEPARTAMENTO DE PROCESO EDITORIAL
(7)

1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Secretaría Técnica de la Secretaría de Desarrollo Institucional	
Identificador único*	**SDI-ST-PE-7**
(Nombre del sistema A1) *	**Reconocimiento de los Derechos Patrimoniales**
Datos personales (sensibles o no) contenidos en el sistema*	**1. Datos personales en general:** **a) Datos de identificación:** Nombre, domicilio, teléfono particular, teléfono celular, correo electrónico, firma, RFC, lugar de nacimiento, fecha de nacimiento y nacionalidad. **b) Datos laborales:** Nombramiento y dependencia académica de adscripción. **2. No se recaban datos personales sensibles.**
Responsable*:	
Nombre*	**Dr. José Alfredo Delgado Guzmán**
Cargo*	**Secretario Técnico**
Funciones*	• Coadyuvar en la planeación, programación, divulgación, difusión y evaluación de los proyectos, de las actividades editoriales, de educación continua y de investigación generados de los Seminarios Universitarios a cargo de la SDI. • Contribuir a la generación, distribución y difusión de productos y proyectos innovadores en materia editorial, investigación, formación y capacitación.
Obligaciones*	• Conocer, proteger su integridad, resguardar y conservar la privacidad de los datos que se manejan y mantener la secrecía de la información. • Hacer uso de los datos únicamente en el ejercicio de sus funciones y para los fines por los que han sido recabados.
	Encargado:

(Nombre del Encargado 1*)	**Adriana Núñez Macías**
Cargo*:	**Jefa del Departamento de Proceso Editorial**
Funciones*:	• Procesar las obras presentadas al Comité Editorial de la SDI y garantizar el cumplimiento de los requisitos de integridad académica señalados en el Reglamento del Comité Editorial y Normatividad Universitaria en materia editorial. • Coordinar el proceso y producción editorial desde la creación, dictaminación, edición, publicación, sesión de derechos y registros nacionales e internacionales especializados de las obras a cargo de la SDI.
Obligaciones*:	• Conocer, proteger su integridad, resguardar y conservar la privacidad de los datos que se manejan y mantener la secrecía de la información. • Hacer uso de los datos únicamente en el ejercicio de sus funciones y para los fines para los que han sido recabados.
	Usuarios:
(Nombre del Usuario 1*)	Dirección de Propiedad Intelectual de la Dirección General de Asuntos Jurídicos de la UNAM.
Cargo*:	No aplica
Funciones*:	No aplica
Obligaciones*:	No aplica

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

Secretaría Técnica de la Secretaría de Desarrollo Institucional	
Identificador único¨*	**SDI-ST-PE-7**
(Nombre del sistema A1*)	**Reconocimiento de los Derechos Patrimoniales**
Tipo de soporte: *	Soporte físico: expedientes.
Descripción: *	Expedientes individuales con información de cada libro publicado.

Características del lugar donde se resguardan los soportes: *	Los expedientes se ubican en una oficina con ventilación natural, luz natural y artificial, puerta de acceso de vidrio y chapa, aislada de humedad, con archiveros y libreros que permiten la conservación de los documentos.

3. ANÁLISIS DE RIESGOS

Eliminado: Ocho renglones en los que se especifican los riesgos, nueve con el impacto y veintiún con la mitigación, correspondientes al análisis de riesgos. Fundamento legal: artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública. En virtud de tratarse de información reservada.

Secretaría Técnica de la Secretaría de Desarrollo Institucional		
Identificador único¨*	**SDI-ST-PE-7**	
(Nombre del sistema A1*)	**Reconocimiento de los Derechos Patrimoniales**	
Riesgo*	**Impacto***	**Mitigación***
Comentario	Comentario	Comentario
Comentario	Comentario	Comentario
Comentario	Comentario	Comentario
Comentario	Comentario	Comentario
Comentario	Comentario	Comentario

SIN TEXTO

4. ANÁLISIS DE BRECHA

Eliminado: Siete renglones en los que se especifican las medias de seguridad actuales, doce con las medidas de seguridad necesarias y ocho con las acciones para remediación, correspondientes al análisis de brecha. Fundamento legal: artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública. En virtud de tratarse de información reservada.

Secretaría Técnica de la Secretaría de Desarrollo Institucional		
Identificador único¨*	**SDI-ST-PE-7**	
(Nombre del sistema A1*)	**Reconocimiento de los Derechos Patrimoniales**	
Medida de seguridad actual*	**Medida de seguridad necesaria***	**Acciones para remediación***
[redacted] Comentario	[redacted] Comentario	[redacted] Comentario

5. PLAN DE TRABAJO

Eliminado: Cinco renglones en los que se especifican las actividades, diecisiete con la descripción, dos con la duración y dos con la cobertura, correspondientes al plan de trabajo. Fundamento legal: artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública. En virtud de tratarse de información reservada.

Secretaria Técnica de la Secretaría de Desarrollo Institucional			
Identificador único¨*	**SDI-ST-PE-7**		
(Nombre del sistema A1*)	**Reconocimiento de los Derechos Patrimoniales**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Comentario	Comentario	Comentario Comentario	Comentario

6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

I. TRANSFERENCIAS DE DATOS PERSONALES

Secretaria Técnica de la Secretaría de Desarrollo Institucional	
Identificador único¨*	**SDI-ST-PE-7**
(Nombre del sistema A1*)	**Reconocimiento de los Derechos Patrimoniales**
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	Envío de la información con mensajero en sobre sellado y clasificado como confidencial. Se solicita el acuse de recibido del destinatario que recibe los datos personales.
Transferencias mediante el traslado de soportes electrónicos:	No aplica
Transferencias mediante el traslado sobre redes electrónicas:	No aplica.

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

El soporte físico de los datos personales se resguarda en expedientes y en archiveros bajo llave.

III. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

Se dispone de los correos electrónicos del proceso con las fechas de inicio y termino del proceso, la operación cotidiana lo realiza una sola persona.

IV. REGISTRO DE INCIDENTES:

No contamos con un procedimiento de atención de incidentes

V. ACCESO A LAS INSTALACIONES

La Coordinación de las Comisiones Locales de Seguridad de la Torre de Rectoría son los encargados de la seguridad de las Instalaciones de las diversas Dependencias que convivimos en este Edificio, por lo que la vigilancia y revisión de acceso y salida está a cargo de dicha Coordinación.

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

Al tratarse de expedientes físicos en caso de cambio de algún dato personal se incorpora el comprobante actualizado en formato físico.

VII. PERFILES DE USUARIO Y CONTRASEÑAS

No aplica.

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

Se realiza un respaldo en PDF, en caso de recuperación de datos se solicita la información al usuario.

IX. PLAN DE CONTINGENCIA

Se desconoce el procedimiento, ya que es responsabilidad de la Dirección General de Asuntos Jurídicos.

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

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

Secretaría Técnica de la Secretaría de Desarrollo Institucional		
Identificador único	(SDI-ST-PE-7)	
Nombre del sistema	Reconocimiento de los Derechos Patrimoniales	
Recurso*	**Descripción***	**Control***
N/A	N/A	N/A

7.2 Procedimiento para la revisión de las medidas de seguridad

Secretaría Técnica de la Secretaría de Desarrollo Institucional		
Identificador único	(SDI-ST-PE-7)	
Nombre del sistema	Reconocimiento de los Derechos Patrimoniales	
Medida de seguridad*	**Procedimiento***	**Responsable***
Mantenimiento de cerraduras y control de accesos al sitio en donde se ubican los expedientes físicos.	Revisión técnica de las cerraduras y Registro de visitas.	Área de bienes y suministros. Vigilancia privada

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

Secretaría Técnica de la Secretaría de Desarrollo Institucional		
Identificador único	(SDI-ST-PE-7)	
Nombre del sistema	Reconocimiento de los Derechos Patrimoniales	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***
N/A	N/A	N/A

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

Secretaría Técnica de la Secretaría de Desarrollo Institucional		
Identificador único	(SDI-ST-PE-7)	
(Nombre del sistema A1)*	Reconocimiento de los Derechos Patrimoniales	
Medida de seguridad*	**Acciones***	**Responsable***

Los expedientes físicos son administrados por una sola persona.	Prohibir el acceso a los expedientes.	Lic. Adriana Núñez Macías.

VIII. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

8.1 Programa de capacitación a los responsables de seguridad de datos personales

Unidad Administrativa de la Secretaría de Desarrollo Institucional			
Identificador único	(SDI-ST-PE-7)		
Nombre del sistema	Reconocimiento de los Derechos Patrimoniales		
Actividad*	**Descripción***	**Duración***	**Cobertura***
La SDI solicitará a la Unidad de Transparencia de la UNAM programar un curso enfocado a la capacitación del personal involucrado en la captación, manejo, resguardo y seguridad de datos personales. De igual forma, se buscarán cursos relacionados que impartan otras instancias como el INAI.	Cursos relacionados con la protección y seguridad de datos personales	Capacitación por lo menos una vez al año.	Deberan asistir por lo menos dos personas de cada área que maneje datos personales en la SDI.

8.2 Programa de difusión de la protección a los datos personales

Unidad Administrativa de la Secretaría de Desarrollo Institucional			
Identificador único	(SDI-ST-PE-7)		
Nombre del sistema	Reconocimiento de los Derechos Patrimoniales		
Actividad*	**Descripción***	**Duración***	**Cobertura***

Difusión de protección de datos personales	El 25 de febrero de 2019, la UNAM difundió en la Gaceta UNAM los Lineamientos para la protección de datos personal en posesión de la UNAM	Permanente	Institucional

IX. MEJORA CONTINUA

9.1 Actualización y mantenimiento de sistemas de información

Secretaría Técnica de la Secretaría de Desarrollo Institucional			
Identificador único*	(SDI-ST-PE-7)		
Nombre del sistema	Reconocimiento de los Derechos Patrimoniales		
Actividad*	**Descripción***	**Duración***	**Cobertura***
.N/A	N/A	N/A	N/A

9.2 Actualización y mantenimiento de equipo de cómputo

Secretaría Técnica de la Secretaría de Desarrollo Institucional			
Identificador único	(SDI-ST-PE-7)		
Nombre del sistema	Reconocimiento de los Derechos Patrimoniales		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Mantenimiento preventivo	Realizar el mantenimiento preventivo del equipo de cómputo tanto a nivel de hardware y software para mantenerlo funcional.	2 veces al año.	Equipos de la oficina de la SDI.

9.3 Procesos para la conservación, preservación y respaldos de información

Secretaría Técnica de la Secretaría de Desarrollo Institucional		
Identificador único	(SDI-ST-PE-7)	
Nombre del sistema	Reconocimiento de los Derechos Patrimoniales	
Proceso*	**Descripción***	**Responsable***
Conformación de los expedientes físicos.	Se resguardan los datos en archiveros bajo llave, libres de húmeda.	Lic. Adriana Núñez Macías

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

Secretaría Técnica de la Secretaría de Desarrollo Institucional		
Identificador único	(SDI-ST-PE-7)	
Nombre del sistema	**Reconocimiento de los Derechos Patrimoniales**	
Proceso	**Descripción***	**Responsable***
Procesos de borrado seguro y disposición final de equipos y componentes informáticos.	Procesos de borrado seguro y disposición final de equipos y componentes informáticos.	Jefa de Departamento de TIC, de la SDI.

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

La cancelación de datos personas se hace mediante oficio por parte del interesado de la SDI.

UNIDAD ADMINISTRATIVA
DEPARTAMENTO DE BIENES Y SUMINISTROS Y SERVICIOS GENERALES
(8)

1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Unidad Administrativa de la Secretaría de Desarrollo Institucional	
Identificador único	(SDI-UA-8)
Nombre del sistema	**Sistema Institucional de Compras SIC**
Datos personales (sensibles o no) contenidos en el sistema*:	**1) Datos personales en general:** a) **Datos de identificación**: Nombre, domicilio, teléfono particular o celular, correo electrónico, RFC. b) **Datos laborales:** Nombre, teléfono y correo electrónico. **2) No se recaban datos personales sensibles**.
Responsable:	
Nombre 1:	Mtra. Sara Angélica Hernández Bautista
Cargo:	Jefa de Unidad Administrativa
Funciones:	• Establecer criterios y lineamientos para el aprovisionamiento de bienes, materiales y la prestación de servicios, que se requieran para el desempeño de las actividades de la SDI.
Obligaciones:	• Conocer, proteger su integridad, resguardar y conservar la privacidad de los datos que se manejan y mantener la secrecía de la información. • Hacer uso de los datos únicamente en el ejercicio de sus funciones y para los fines para los que han sido recabados.
	Encargados:
Nombre del Encargado 1	L.C. César Munive Dorantes
Cargo:	Jefe del Departamento de Bienes y Suministros y Servicios Generales
Funciones:	• Verificar y determinar, en coordinación con la Unidad Administrativa, el mecanismo de compra de material y equipo que requieran las diversas áreas de la SDI, conforme a la normatividad universitaria en la materia y darles trámite administrativo en el Sistema Institucional de Compras (SIC).
Obligaciones:	• Conocer, proteger su integridad, resguardar y conservar la privacidad de los datos que se manejan y mantener la secrecía de la información. • Hacer uso de los datos únicamente en el ejercicio de sus funciones y para los fines para los que han sido recabados.
Nombre del Encargado 2	Lic. Daniela Martínez Dávila
Cargo:	Asistente de Procesos
Funciones:	• Realizar la captura y seguimiento de las compras que determinen en conjunto la Unidad Administrativa y la Jefatura del

	Departamento de Bienes y Suministros y Servicios Generales, en el Sistema Institucional de Compras (SIC).
Obligaciones:	• Conocer, proteger su integridad, resguardar y conservar la privacidad de los datos que se manejan y mantener la secrecía de la información. • Hacer uso de los datos únicamente en el ejercicio de sus funciones y para los fines para los que han sido recabados.
Nombre del Encargado 3	L.C. José Isaac Pérez Hernández
Cargo:	Jefe del Departamento de Presupuesto y Contabilidad
Funciones:	• Realizar la recepción, visto bueno y autorización de toda aquella documentación que se encuentra en trámite de aquellas partidas presupuestales que tienen carácter centralizado, conforme al calendario programado.
Obligaciones:	• Conocer, proteger su integridad, resguardar y conservar la privacidad de los datos que se manejan y mantener la secrecía de la información. • Hacer uso de los datos únicamente en el ejercicio de sus funciones y para los fines para los que han sido recabados.
Nombre del Encargado 4	Lic. Iván de Jesús Gutiérrez Rojas
Cargo:	Asistente de Procesos
Funciones:	• Realizar la captura y seguimiento de los códigos presupuestales de los trámites de pago a proveedor que determine la Jefatura del Presupuesto y Contabilidad, en el Sistema Institucional de Compras (SIC). • Administrar los roles de cada responsable en el Sistema Institucional de Compras (SIC).
Obligaciones:	• Conocer, proteger su integridad, resguardar y conservar la privacidad de los datos que se manejan y mantener la secrecía de la información. • Hacer uso de los datos únicamente en el ejercicio de sus funciones y para los fines para los que han sido recabados.
Nombre del Encargado 5	Lic. David Adrián Jiménez Figueroa
Cargo:	Asistente de Procesos
Funciones:	• Realizar la captura y seguimiento de los códigos presupuestales de los trámites de pago a proveedor que determine la Jefatura del Presupuesto y Contabilidad, en el Sistema Institucional de Compras (SIC).
Obligaciones:	• Conocer, proteger su integridad, resguardar y conservar la privacidad de los datos que se manejan y mantener la secrecía de la información. • Hacer uso de los datos únicamente en el ejercicio de sus funciones y para los fines para los que han sido recabados.
	Usuarios:
Nombre del Usuario:	Dra. Patricia Dolores Dávila Aranda
Cargo:	Secretaria de Desarrollo Institucional
Funciones:	• Autoriza los procesos mediante su firma electrónica.

Obligaciones:	• Conocer, proteger su integridad, resguardar y conservar la privacidad de los datos que se manejan y mantener la secrecía de la información. • Hacer uso de los datos únicamente en el ejercicio de sus funciones y para los fines para los que han sido recabados.

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

Unidad Administrativa de la Secretaría de Desarrollo Institucional	
Identificador único	(SDI-UA-8)
Nombre del sistema	**Sistema Institucional de Compras SIC**
Tipo de soporte:	Sistema electrónico.
Descripción:	Nube privada.
Características del lugar donde se resguardan los soportes:	Servidores de la Dirección General de Proveeduría de la UNAM, en el cual tenemos acceso a través de la dirección https://www.sic.unam.mx

3. ANÁLISIS DE RIESGOS

Eliminado: Dos renglones en los que se especifican los riesgos, cinco con el impacto y catorce con la mitigación, correspondientes al análisis de riesgos. Fundamento legal: artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública. En virtud de tratarse de información reservada.

Unidad Administrativa de la Secretaría de Desarrollo Institucional		
Identificador único	(SDI-UA-8)	
Nombre del sistema	**Sistema Institucional de Compras SIC**	
Riesgo	**Impacto***	**Mitigación***
Comentario	Comentario	Comentario
Comentario	Comentario	Comentario

4. ANÁLISIS DE BRECHA

Eliminado: Cuatro renglones en los que se especifican las medias de seguridad actuales, ocho con las medidas de seguridad necesarias y tres con las acciones para remediación, correspondientes al análisis de brecha. Fundamento legal: artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública. En virtud de tratarse de información reservada.

Unidad Administrativa de la Secretaría de Desarrollo Institucional		
Identificador único*	(SDI-UA-8)	
Nombre del sistema	**Sistema Institucional de Compras SIC**	
Medida de seguridad actual*	**Medida de seguridad necesaria***	**Acciones para remediación***
Comentario	Comentario	Comentario

5. PLAN DE TRABAJO

Eliminado: Siete renglones en los que se especifican las actividades, doce con la descripción, ocho con la duración y cinco con la cobertura, correspondientes al plan de trabajo. Fundamento legal: artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública. En virtud de tratarse de información reservada.

Unidad Administrativa de la Secretaría de Desarrollo Institucional			
Identificador único*	(SDI-UA-8)		
Nombre del sistema	**Sistema Institucional de Compras SIC**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Comentario	Comentario	Comentario	Comentario

6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

I. TRANSFERENCIAS DE DATOS PERSONALES

Unidad Administrativa de la Secretaría de Desarrollo Institucional	
Identificador único	(SDI-UA-8)
Nombre del sistema	**Sistema Institucional de Compras SIC**
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	No se realiza traslado de soporte físico
Transferencias mediante el traslado de soportes electrónicos:	No se realiza traslado de soporte electrónico
Transferencias mediante el traslado sobre redes electrónicas:	• Carga de información de proveedores y solicitantes en el Sistema Institucional de Compras (SIC); • En el Sistema Institucional de Compras (SIC) a través de la liga de internet https://www.sic.unam.mx, se registran las adquisiciones de las diversas áreas, se debe contar con una contraseña para el acceso a la aplicación; • La Dirección General de Proveeduría es la encargada de proporcionar la seguridad del sistema y debe detectar las intrusiones en el canal de comunicaciones. • La Dirección General de Proveeduría asigna un número de Solicitud de Compra a cada operación registrada. • El Sistema Institucional de Compras (SIC) tiene habilitada una opción para ver los registros históricos al generar cada operación.

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

El Sistema Institucional de Compras (SIC) no realiza tratamiento de datos personales con soportes físicos, ya que se encuentra a través de soporte electrónico a través de internet.

III. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

El Sistema Institucional de Compras (SIC) genera un histórico por cada operación a través de soporte electrónico, se almacenan y resguardan en los servidores de la Dirección General de Proveeduría y se pueden consultar todas las operaciones registradas en el sistema, desde su implementación y uso de cada Dependencia Universitaria.

IV. REGISTRO DE INCIDENTES:

No contamos con un procedimiento de atención de incidentes, debido a que no se ha dado ningún caso.

V. ACCESO A LAS INSTALACIONES

La Coordinación de las Comisiones Locales de Seguridad de la Torre de Rectoría son los encargados de la seguridad de las Instalaciones de las diversas Dependencias que convivimos en este Edificio, por lo que la vigilancia y revisión de acceso y salida está a cargo de dicha Coordinación.

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

Los usuarios son los encargados de realizar directamente su actualización de datos personales, a través del Sistema de Alta de Proveedores, de la Contaduría General de la UNAM, por lo cual no está dentro de nuestro ámbito de competencia.

VII. PERFILES DE USUARIO Y CONTRASEÑAS

El Sistema Institucional de Compras (SIC) está diseñado para que cada persona responsable tenga un usuario y contraseña para accesar a dicha aplicación, además que se tiene asignado roles por cada nivel de los usuarios que participan en el proceso, asimismo el SIC permite tener acceso remoto desde cualquier dispositivo, con el fin de facilitar la gestión de los trámites en todo momento y desde cualquier lugar.

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

Esta actividad es garantizada por la Dirección General de Proveeduría, quienes tienen el resguardo de los servidores y quienes proporcionan este sistema a todas las áreas de la UNAM.

IX. PLAN DE CONTINGENCIA

Esta actividad es garantizada por la Dirección General de Proveeduría, debido a que todos los usuarios podemos accesar desde cualquier dispositivo electrónico, por medio de internet.

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

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

Unidad Administrativa de la Secretaría de Desarrollo Institucional		
Identificador único	(SDI-UA-8)	
Nombre del sistema	**Sistema Institucional de Compras SIC**	
Recurso*	**Descripción***	**Control***
Asignación de roles y permisos para acceso al Sistema Institucional de Compras (SIC).	La seguridad se basa en roles que se asignan a una persona o grupos de manera general y local.	Asignación de roles.

7.2. Procedimiento para la revisión de las medidas de seguridad

Unidad Administrativa de la Secretaría de Desarrollo Institucional

Identificador único	(SDI-UA-8)	
Nombre del sistema	**Sistema Institucional de Compras SIC**	
Medida de seguridad*	**Procedimiento***	**Responsable***
Revisión en la actualización de roles y permisos	Con cada cambio de personal se eliminan los permisos que tenían asignados para ingresar a la aplicación.	Lic. Iván de Jesús Gutiérrez Rojas

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

Unidad Administrativa de la Secretaría de Desarrollo Institucional		
Identificador único	(SDI-UA-8)	
Nombre del sistema	**Sistema Institucional de Compras SIC**	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***
Principio del menor privilegio	Durante el análisis de riesgo del manejo del SIC, se determinó que todas las personas con acceso al sistema cuentan con los privilegios de acuerdo a su rol de participación.	Lic. Iván de Jesús Gutiérrez Rojas

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

Unidad Administrativa de la Secretaría de Desarrollo Institucional		
Identificador único	(SDI-UA-8)	
Nombre del sistema A1	**Sistema Institucional de Compras SIC**	
Medida de seguridad*	**Acciones***	**Responsable***
Una vez que el personal acreditado para ingresar a la aplicación causa baja de nuestra Dependencia Universitaria, se deben	Eliminar los privilegios del acceso al SIC.	Lic. Iván de Jesús Gutiérrez Rojas

quitar los privilegios de acceso al SIC.		

8. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

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

Unidad Administrativa de la Secretaría de Desarrollo Institucional			
Identificador único	(SDI-UA-8)		
Nombre del sistema	**Sistema Institucional de Compras SIC**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
La SDI solicitará a la Unidad de Transparencia de la UNAM programar un curso enfocado a la capacitación del personal involucrado en la captación, manejo, resguardo y seguridad de datos personales. De igual forma, se buscarán cursos relacionados que impartan otras instancias como el INAI.	Cursos relacionados con la protección y seguridad de datos personales	Capacitación por lo menos una vez al año.	Deberan asistir por lo menos dos personas de cada área que maneje datos personales en la SDI.

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

Unidad Administrativa de la Secretaría de Desarrollo Institucional			
Identificador único	(SDI-UA-8)		
Nombre del sistema	**Sistema Institucional de Compras SIC**		
Actividad*	**Descripción***	**Duración***	**Cobertura***

Difusión de protección de datos personales	El 25 de febrero de 2019, la UNAM difundió en la Gaceta UNAM los Lineamientos para la protección de datos personal en posesión de la UNAM	Permanente	Institucional

9. MEJORA CONTINUA

9.1. Actualización y mantenimiento de sistemas de información

Unidad Administrativa de la Secretaría de Desarrollo Institucional			
Identificador único*	(SDI-UA-8)		
Nombre del sistema	**Sistema Institucional de Compras SIC**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Esta actividad la realiza la Dirección General de Proveeduría.	N/A.	N/A	N/A

9.2. Actualización y mantenimiento de equipo de cómputo

Unidad Administrativa de la Secretaría de Desarrollo Institucional			
Identificador único	(SDI-UA-8)		
Nombre del sistema	**Sistema Institucional de Compras SIC**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Mantenimiento preventivo.	Realizar el mantenimiento preventivo del equipo de cómputo, tanto a nivel hardware, como software para mantenerlo funcional.	2 veces al año.	Equipos de la oficina de la Secretaría de Desarrollo Institucional.

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

Unidad Administrativa de la Secretaría de Desarrollo Institucional		
Identificador único	(SDI-UA-8)	
Nombre del sistema	**Sistema Institucional de Compras SIC**	
Proceso*	**Descripción***	**Responsable***
N/A	N/A	Esta actividad la realiza la Dirección General de Proveeduría.

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

Unidad Administrativa de la Secretaría de Desarrollo Institucional		
Identificador único	(SDI-UA-8)	
Nombre del sistema	**Sistema Institucional de Compras SIC**	
Proceso	**Descripción***	**Responsable***
Procesos de borrado seguro y disposición final de equipos y componentes informáticos.	Procesos de borrado seguro y disposición final de equipos y componentes informáticos.	Jefatura de Departamento de TIC de la SDI

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

El Sistema Institucional de Compras no tiene injerencia en la cancelación de tratamiento de datos personales, debido a que esta actividad depende de la Contaduría General de la UNAM.

UNIDAD ADMINISTRATIVA
DEPARTAMENTO DE BIENES Y SUMINISTROS Y SERVICIOS GENERALES
(9)

1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Unidad Administrativa de la Secretaría de Desarrollo Institucional	
Identificador único	(SDI-UA- 9)
Nombre del sistema	**Sistema de Videovigilancia**
Datos personales (sensibles o no) contenidos en el sistema*:	**1. Datos personales en general:** **a) Datos de identificación**: Imágenes del personal de la SDI y de la comunidad universitaria que nos visitan. **No se recaban datos personales sensibles**.
Responsable:	
Nombre*:	Mtra. Sara Angélica Hernández Bautista
Cargo*:	Jefa de Unidad Administrativa
Funciones*:	• Controlar el resguardo de imágenes de la Videograbadora a través de clave de acceso.
Obligaciones*:	• Conocer, proteger su integridad, resguardar y conservar la privacidad de los datos que se manejan y mantener la secrecía de la información. • Hacer uso de los datos únicamente en el ejercicio de sus funciones y para los fines para los que han sido recabados.
	Encargados:
Nombre del Encargado 1	L.C. César Munive Dorantes
Cargo:	Jefe del Departamento de Bienes y Suministros y Servicios Generales
Funciones:	• Apoyar a la Jefa de Unidad, en caso de alguna incidencia para accesar al sistema a través de su clave de acceso.
Obligaciones:	• Conocer, proteger su integridad, resguardar y conservar la privacidad de los datos que se manejan y mantener la secrecía de la información. • Hacer uso de los datos únicamente en el ejercicio de sus funciones y para los fines para los que han sido recabados.

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

Unidad Administrativa de la Secretaría de Desarrollo Institucional	
Identificador único	(SDI-UA-9)
Nombre del sistema	**Sistema de Videovigilancia**
Tipo de soporte:	Soporte electrónico.
Descripción:	Nube privada.

Características del lugar donde se resguardan los soportes:*	El Digital Video Recorder (DVR) se encuentra ubicado en la oficina de la Unidad Administrativa y los respaldos se hacen en un servidor dedicado.

3. ANÁLISIS DE RIESGOS

Eliminado: Dos renglones en los que se especifican los riesgos, seis con el impacto y diez con la mitigación, correspondientes al análisis de riesgos. Fundamento legal: artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública. En virtud de tratarse de información reservada.

Unidad Administrativa de la Secretaría de Desarrollo Institucional		
Identificador único*	(SDI-UA-9)	
Nombre del sistema	**Sistema de Videovigilancia**	
Riesgo*	**Impacto***	**Mitigación***
Comentario	Comentario	Comentario
Comentario	Comentario	Comentario

4. ANÁLISIS DE BRECHA

Eliminado: Cuatro renglones en los que se especifican las medias de seguridad actuales, siete con las medidas de seguridad necesarias y tres con las acciones para remediación, correspondientes al análisis de brecha. Fundamento legal: artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública. En virtud de tratarse de información reservada.

Unidad Administrativa de la Secretaría de Desarrollo Institucional		
Identificador único*	(SDI-UA-9)	
Nombre del sistema	**Sistema de Videovigilancia**	
Medida de seguridad actual*	**Medida de seguridad necesaria***	**Acciones para remediación***
Comentario	Comentario	Comentario

5. PLAN DE TRABAJO

Eliminado: Cuatro renglones en los que se especifican las actividades, trece con la descripción, trece con la duración y seis con la cobertura, correspondientes al plan de trabajo. Fundamento legal: artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública. En virtud de tratarse de información reservada.

Unidad Administrativa de la Secretaría de Desarrollo Institucional			
Identificador único*	(UA-SDI-9)		
Nombre del sistema	**Sistema Videovigilancia**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Comentario	Comentario	Comentario	Comentario

6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

I. TRANSFERENCIAS DE DATOS PERSONALES

Unidad Administrativa de la Secretaría de Desarrollo Institucional	
Identificador único	(SDI- UA-9)
Nombre del sistema	**Sistema de Videovigilancia**
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	NO APLICA
Transferencias mediante el traslado de soportes electrónicos:	NO APLICA
Transferencias mediante el traslado sobre redes electrónicas:	El dispositivo DVR graba la actividad en disco duro interno, en formato de compresión mp5, mismas que pueden ser revisadas a través de una red local.

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

NO APLICA

III. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

Para estar en la facultad de accesar al sistema para bajar alguna imagen especifica; se hace únicamente por solicitud de la Titular de la Oficina, a través de un correo electrónico.

IV. REGISTRO DE INCIDENTES:

No contamos con un procedimiento de atención de incidentes.

V. ACCESO A LAS INSTALACIONES

La Coordinación de las Comisiones Locales de Seguridad de la Torre de Rectoría son los encargados de la seguridad de las instalaciones de las diversas dependencias que convivimos en este edificio, por lo que la vigilancia y revisión de acceso y salida está a cargo de dicha coordinación.

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

El sistema de Videovigilancia de la SDI solo resguarda imágenes en video.

VII. PERFILES DE USUARIO Y CONTRASEÑAS

Las dos únicas personas facultadas para accesar al Sistema de Videovigilancia son:

La Jefa de la Unidad Administrativa y el Jefe del Departamento de Bienes y Suministros y Servicios Generales, los cuales cuentan con clave de acceso al Sistema.

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

La información únicamente se almacena por un periodo corto de tiempo en los discos internos.

IX. PLAN DE CONTINGENCIA

No se cuenta con un plan de Contingencia derivado que no se ha tenido ningún tipo de incidencia, desde que se instaló en 2015.

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

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

Unidad Administrativa de la Secretaría de Desarrollo Institucional		
Identificador único	(SDI-UA-9)	
Nombre del sistema	**Sistema de Videovigilancia**	
Recurso*	**Descripción***	**Control***
N/A	N/A	N/A

7.2 Procedimiento para la revisión de las medidas de seguridad

Unidad Administrativa de la Secretaría de Desarrollo Institucional		
Identificador único	(SDI-UA-9)	
Nombre del sistema	**Sistema de Videovigilancia**	
Medida de seguridad*	**Procedimiento***	**Responsable***
N/A	N/A	a) N/A

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

Unidad Administrativa de la Secretaría de Desarrollo Institucional

Identificador único	(SDI-UA-9)	
Nombre del sistema	**Sistema de Videovigilancia**	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***
N/A	N/A	N/A

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

Unidad Administrativa de la Secretaría de Desarrollo Institucional		
Identificador único	(SDI-UA-9)	
(Nombre del sistema A1)	**Sistema de Videovigilancia**	
Medida de seguridad*	**Acciones***	**Responsable***
N/A	N/A	2. N/A

8 PROGRAMA ESPECÍFICO DE CAPACITACIÓN

8.1 Programa de capacitación a los responsables de seguridad de datos personales

Unidad Administrativa de la Secretaría de Desarrollo Institucional			
Identificador único	(SDI-UA-9)		
Nombre del sistema	**Sistema de Videovigilancia**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
La SDI solicitará a la Unidad de Transparencia de la UNAM programar un curso enfocado a la capacitación del personal involucrado en la captación, manejo, resguardo y seguridad de datos	Cursos relacionados con la protección y seguridad de datos personales	Capacitación por lo menos una vez al año.	Deberan asistir por lo menos dos personas de cada área que maneje datos personales en la SDI.

personales. De igual forma, se buscarán cursos relacionados que impartan otras instancias como el INAI.			

8.2 Programa de difusión de la protección a los datos personales

Unidad Administrativa de la Secretaría de Desarrollo Institucional			
Identificador único	(SDI-UA-9)		
Nombre del sistema	**Sistema de Videovigilancia**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Difusión de protección de datos personales	El 25 de febrero de 2019, la UNAM difundió en la Gaceta UNAM los Lineamientos para la protección de datos personal en posesión de la UNAM	Permanente	Institucional

9 MEJORA CONTINUA

9.1 Actualización y mantenimiento de sistemas de información

Unidad Administrativa de la Secretaría de Desarrollo Institucional			
Identificador único*	(SDI-UA-9)		
Nombre del sistema	**Sistema de Videovigilancia**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Verificación del correcto funcionamiento del sistema	Entrar a la aplicación por lo menos una vez al mes, para verificar el correcto funcionamiento del	Permanente	Permanente, se procura que el sistemas funcione al 100% 24/7 por los 365 días del año.

	sistema y de las cámaras.		

9.2 Actualización y mantenimiento de equipo de cómputo

Unidad Administrativa de la Secretaría de Desarrollo Institucional			
Identificador único	(SDI-UA-9)		
Nombre del sistema	**Sistema de Videovigilancia**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
El departamento de TIC de la SDI, tiene como programa dar 2 mantenimientos al año a los equipos de cómputo para asegurar el correcto funcionamiento y en su caso la reparación de la misma.	Se calendariza los mantenimientos a través de oficio se notifica, para que el usuario este presente.	2 veces al año	Se busca mantener una buena calidad en los equipos de cómputo, de tal forma que no sean vulnerables de jackear información o de fácil acceso a los sistemas de videovigilancia en este caso.

9.3 Procesos para la conservación, preservación y respaldos de información

Unidad Administrativa de la Secretaría de Desarrollo Institucional		
Identificador único	(SDI-UA-9)	
Nombre del sistema	**Sistema de Videovigilancia**	
Proceso*	**Descripción***	**Responsable***
El propio sistema del equipo DVR, se encarga de respaldar la información durante un periodo de 11 días.	El dispositivo DVR graba la actividad en disco duro interno, en formato de compresión mp5, Las videograbaciones se resguardan por 11 días y al término del periodo, la imagen más reciente se reescribe sobre el video más antiguo.	Esta actividad está automatizada desde su instalación. Configurable por los usuarios con acceso al sistema.

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

Unidad Administrativa de la Secretaría de Desarrollo Institucional		
Identificador único	(SDI-UA-9)	
Nombre del sistema	**Sistema de Videovigilancia**	
Proceso	**Descripción***	**Responsable***
Procesos de borrado seguro y disposición final de equipos y componentes informáticos.	Procesos de borrado seguro y disposición final de equipos y componentes informáticos.	Esta actividad se realizará por el encargado del Departamento de TI interno.

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

El sistema de Videovigilancia no tiene facultades para recabar o cancelar ningún tipo de dato personal.

UNIDAD ADMINISTRATIVA
DEPARTAMENTO DE PERSONAL
(10)

1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Unidad Administrativa de la Secretaría de Desarrollo Institucional	
Identificador único*	(SDI-UA-10)
(Nombre del sistema A1) *	**Sistema Integral de Personal/FORMA UNICA ELECTRONICA (FUE)**
Datos personales (sensibles o no) contenidos en el sistema*:	**1. Datos personales en general:** **a) Datos de identificación**: Nombre, domicilio, teléfono particular, teléfono celular, correo electrónico, estado civil, firma, constancia de situación de fiscal, CURP, lugar de nacimiento, fecha de nacimiento, nacionalidad, edad, nombres de familiares, beneficiarios, fotografía, cuenta bancaria y banco, comprobante de último grado de estudios, **2. No recabamos datos sensibles.**
Responsable*:	
Nombre*:	**Mtra. Sara Angélica Hernández Bautista**
Cargo*:	Jefa de la Unidad Administrativa
Funciones*:	• Fiscalizar, conforme a la normatividad establecida por el Patronato Universitario, el uso de los recursos presupuestales y financieros asignados o generados por la dependencia.
Obligaciones*:	• Conocer, proteger su integridad, resguardar y conservar la privacidad de los datos que se manejan y mantener la secrecía de la información. • Hacer uso de los datos únicamente en el ejercicio de sus funciones y para los fines para los que han sido recabados.
	Encargados:
(Nombre del Encargado 1*)	**Nisa Cassandra Pérez Andrade**
Cargo*:	**Jefa del Departamento de Personal**
Funciones*:	• Gestionar ante la Dirección General de Personal los trámites administrativos que se deriven de la relación laboral tanto del personal de la Secretaría de Desarrollo Institucional como el de nuevo ingreso de las sub dependencias. • Dar seguimiento a los movimientos del personal de confianza, académico-administrativo y de base tramitados ante la Dirección General de Personal.

Obligaciones*:	• Conocer, proteger su integridad, resguardar y conservar la privacidad de los datos que se manejan y mantener la secrecía de la información. • Hacer uso de los datos únicamente en el ejercicio de sus funciones y para los fines para los que han sido recabados.
(Nombre del Encargado 2*)	**Noemi del Carmen Mauro Ibarra**
Cargo*:	**Asistente de Procesos**
Funciones*:	• Asistir en el proceso de la contratación del personal de base, funcionarios y confianza
Obligaciones*:	• Conocer, proteger su integridad, resguardar y conservar la privacidad de los datos que se manejan y mantener la secrecía de la información. • Hacer uso de los datos únicamente en el ejercicio de sus funciones y para los fines para los que han sido recabados.
(Nombre del Encargado 2*)	**Carlos Meza Luna**
Cargo*:	**Asistente Ejecutivo**
Funciones*:	• Asistir en el proceso de la contratación del personal de base, funcionarios y confianza
Obligaciones*:	• Conocer, proteger su integridad, resguardar y conservar la privacidad de los datos que se manejan y mantener la secrecía de la información. • Hacer uso de los datos únicamente en el ejercicio de sus funciones y para los fines para los que han sido recabados.
Nombre del Usuario 1	**Dra. Patricia Dolores Dávila Aranda**
Cargo:	**Secretaria de Desarrollo Institucional**
Funciones*:	• Autorizar y validar el proceso mediante firma electrónica.
Obligaciones*:	• Conocer, proteger su integridad, resguardar y conservar la privacidad de los datos que se manejan y mantener la secrecía de la información. • Hacer uso de los datos únicamente en el ejercicio de sus funciones y para los fines para los que han sido recabados.

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

Unidad Administrativa de la Secretaría de Desarrollo Institucional	
Identificador único¨*	(SDI-UA-10)
(Nombre del sistema A1*)	**Sistema Integral de Personal/FUE**
Tipo de soporte: *	Soporte físico: Expedientes de los interesados

Descripción: *	La documentación solicitada se almacena en el archivo en trámite de la SDI.
Características del lugar donde se resguardan los soportes: *	Se resguardan en el archivo de la Secretaría de Desarrollo Institucional

3. ANÁLISIS DE RIESGOS

Eliminado: Dos renglones en los que se especifican los riesgos, cinco con el impacto y doce con la mitigación, correspondientes al análisis de riesgos. Fundamento legal: artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública. En virtud de tratarse de información reservada.

Unidad Administrativa de la Secretaría de Desarrollo Institucional		
Identificador único*	(UA-SDI-10)	
Nombre del sistema	**Sistema Integral de Personal/FUE**	
Riesgo*	**Impacto***	**Mitigación***
Comentario	Comentario	Comentario
Comentario	Comentario	Comentario

4. ANÁLISIS DE BRECHA

Eliminado: Cuatro renglones en los que se especifican las medias de seguridad actuales, siete con las medidas de seguridad necesarias y tres con las acciones para remediación, correspondientes al análisis de brecha. Fundamento legal: artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública. En virtud de tratarse de información reservada.

Unidad Administrativa de la Secretaría de Desarrollo Institucional		
Identificador único*	(UA-SDI-10)	
Nombre del sistema	**Sistema Integral de Personal/FUE**	
Medida de seguridad actual*	**Medida de seguridad necesaria***	**Acciones para remediación***
Comentario	Comentario	Comentario

5. PLAN DE TRABAJO

Eliminado: Seis renglones en los que se especifican las actividades, treinta y cuatro con la descripción, seis con la duración y cinco con la cobertura, correspondientes al plan de trabajo. Fundamento legal: artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública. En virtud de tratarse de información reservada.

Unidad Administrativa de la Secretaría de Desarrollo Institucional			
Identificador único*	(UA-SDI-10)		
Nombre del sistema	**Sistema Integral de Personal/FUE**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Comentario	Comentario	Comentario	Comentario

Eliminado: Diez renglones en los que se especifica la descripción correspondiente al plan de trabajo. Fundamento legal: artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública. En virtud de tratarse de información reservada.

	Comentario [redacted]		

6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

I. TRANSFERENCIAS DE DATOS PERSONALES

Unidad Administrativa de la Secretaría de Desarrollo Institucional	
Identificador único	(UA-SDI-10)
Nombre del sistema	**Sistema Integral de Personal/FUE**
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	• El personal del Departamento de personal se encarga de llevar directamente los movimientos junto con los documentos para ingresarlos a la ventanilla de la DGPe.
Transferencias mediante el traslado de soportes electrónicos:	No se realiza traslado de soporte electrónico
Transferencias mediante el traslado sobre redes electrónicas:	• Carga de información de los interesados directamente en el SIP/FUE al cual se ingresa con un usuario y contraseña proporcionados por la Dirección General de Sistemas de Personal.

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

Se genera un expediente por cada interesado y es resguardado en el Archivo en trámite de la SDI

III. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

El Sistema Integral de Personal/FUE genera un seguimiento desde que se inicia el movimiento requerido hasta el final del mismo.

IV. REGISTRO DE INCIDENTES:

No contamos con un procedimiento de atención de incidentes

V. ACCESO A LAS INSTALACIONES:

La Coordinación de las Comisiones Locales de Seguridad de la Torre de Rectoría son los encargados de la seguridad de las instalaciones de las diversas dependencias que convivimos en este edificio, por lo que la vigilancia y revisión de acceso y salida está a cargo de dicha coordinación.

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

La jefa de personal se encarga de actualizar o modificar los datos que se requieran de los interesados.

VII. PERFILES DE USUARIO Y CONTRASEÑAS

El Sistema Integral de Personal está diseñado para que cada persona responsable tenga un usuario y contraseña para accesar a dicha aplicación y se puede trabajar en él únicamente con las IP autorizadas por la Dirección General de Sistemas de Personal de la DGPe.

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

Esta actividad es garantizada por la Dirección General de Personal.

IX. PLAN DE CONTINGENCIA

Esta actividad es garantizada por la Dirección General de Personal

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

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

Unidad Administrativa de la Secretaría de Desarrollo Institucional		
Identificador único	(UA-SDI-10)	
Nombre del sistema	**Sistema Integral de Personal/FUE**	
Recurso*	**Descripción***	**Control***
N/A	N/A	N/A

7.2. Procedimiento para la revisión de las medidas de seguridad

Unidad Administrativa de la Secretaría de Desarrollo Institucional		
Identificador único	(UA-SDI-10)	
Nombre del sistema	**Sistema Integral de Personal/FUE**	
Medida de seguridad*	**Procedimiento***	**Responsable***
N/A	N/A	b) N/A

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

Unidad Administrativa de la Secretaría de Desarrollo Institucional	
Identificador único	(UA-SDI-10)

Nombre del sistema	Sistema Integral de Personal/FUE	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***
N/A	N/A	N/A

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

Unidad Administrativa de la Secretaría de Desarrollo Institucional		
Identificador único	(UA-SDI-10)	
(Nombre del sistema A1)*	**Sistema Integral de Personal/FUE**	
Medida de seguridad*	**Acciones***	**Responsable***
N/A	N/A	3. N/A

8. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

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

Unidad Administrativa de la Secretaría de Desarrollo Institucional			
Identificador único	(UA-SDI-10)		
Nombre del sistema	**Sistema Integral de Personal/FUE**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
La SDI solicitará a la Unidad de Transparencia de la UNAM programar un curso enfocado a la capacitación del personal involucrado en la captación, manejo, resguardo y seguridad de datos personales.	Cursos relacionados con la protección y seguridad de datos personales	Capacitación por lo menos una vez al año.	Deberan asistir por lo menos dos personas de cada área que maneje datos personales en la SDI.

De igual forma, se buscarán cursos relacionados que impartan otras instancias como el INAI.			

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

Unidad Administrativa de la Secretaría de Desarrollo Institucional			
Identificador único	(UA-SDI-10)		
Nombre del sistema	**Sistema Integral de Personal/FUE**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Difusión de protección de datos personales	El 25 de febrero de 2019, la UNAM difundió en la Gaceta UNAM los Lineamientos para la protección de datos personal en posesión de la UNAM	Permanente	Institucional

9. MEJORA CONTINUA

9.1. Actualización y mantenimiento de sistemas de información

Unidad Administrativa de la Secretaría de Desarrollo Institucional			
Identificador único*	(UA-SDI-10)		
Nombre del sistema	**Sistema Integral de Personal/FUE**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Esta actividad la realiza la Dirección General de Personal	N/A	N/A	N/A

9.2. Actualización y mantenimiento de equipo de cómputo

Unidad Administrativa de la Secretaría de Desarrollo Institucional			
Identificador único	(UA-SDI-10)		
Nombre del sistema	**Sistema Integral de Personal/FUE**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Mantenimiento preventive	Realizar el mantenimiento preventive del equipo de cómputo tanto a nivel hardware como software para mantenerlo funcional	2 veces al año	Equipos de la oficina de la SDI

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

Unidad Administrativa de la Secretaría de Desarrollo Institucional		
Identificador único	(UA-SDI-10)	
Nombre del sistema	**Sistema Integral de Personal/FUE**	
Proceso*	**Descripción***	**Responsable***
N/a	N/A	Esta actividad la realiza la Dirección General de Personal

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

Unidad Administrativa de la Secretaría de Desarrollo Institucional		
Identificador único	(UA-SDI-10)	
Nombre del sistema	**Sistema Integral de Personal/FUE**	
Proceso	**Descripción***	**Responsable***

Procesos de borrado seguro y disposición final de equipos y componentes informáticos.	Procesos de borrado seguro y disposición final de equipos y componentes informáticos.	Jefatura de Departamento de TIC de la SDI

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

El Sistema Integral de Personal está a cargo de la Dirección General de Personal y de la Dirección General de Sistemas de la DGPe.

UNIDAD ADMINISTRATIVA
DEPARTAMENTO DE PERSONAL
(11)

1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Unidad Administrativa de la Secretaría de Desarrollo Institucional	
Identificador único*	(SDI-UA-11)
(Nombre del sistema A1) *	**Sistema Integral de Personal/Honorarios**
Datos personales (sensibles o no) contenidos en el sistema*:	**1. Datos personales en general:** **a) Datos de identificación:** Nombre, domicilio, teléfono particular, teléfono celular, correo electrónico, estado civil, firma, Constancia de situación de fiscal, CURP, lugar de nacimiento, fecha de nacimiento, nacionalidad, edad, nombres de familiares, beneficiarios, fotografía, cuenta bancaria y banco, comprobante de último grado de estudios, **2. No recabamos datos sensibles.**
Responsable*:	
Nombre*:	**Mtra. Sara Angélica Hernández Bautista**
Cargo*:	Jefa de la Unidad Administrativa
Funciones*:	• Fiscalizar, conforme a la normatividad establecida por el Patronato Universitario, el uso de los recursos presupuestales y financieros asignados o generados por la Dependencia.
Obligaciones*:	• Conocer, proteger su integridad, resguardar y conservar la privacidad de los datos que se manejan y mantener la secrecía de la información. • Hacer uso de los datos únicamente en el ejercicio de sus funciones y para los fines para los que han sido recabados.
	Encargados:
(Nombre del Encargado 1*)	**Nisa Cassandra Pérez Andrade**
Cargo*:	**Jefa del Departamento de Personal**
Funciones*:	• Efectuar el trámite ante la Dirección General de Personal y la Unidad de Proceso Administrativo correspondiente, para el pago de los honorarios por servicios profesionales.
Obligaciones*:	• Conocer, proteger su integridad, resguardar y conservar la privacidad de los datos que se manejan y mantener la secrecía de la información. • Hacer uso de los datos únicamente en el ejercicio de sus funciones y para los fines para los que han sido recabados.

(Nombre del Encargado 2*)	**Noemi del Carmen Mauro Ibarra**
Cargo*:	**Asistente de Procesos**
Funciones*:	• Asistir en el proceso de la contratación y pago de los prestadores de servicios profesionales
Obligaciones*:	• Conocer, proteger su integridad, resguardar y conservar la privacidad de los datos que se manejan y mantener la secrecía de la información. • Hacer uso de los datos únicamente en el ejercicio de sus funciones y para los fines para los que han sido recabados.
(Nombre del Encargado 2*)	**Carlos Meza Luna**
Cargo*:	**Asistente Ejecutivo**
Funciones*:	• Asistir en el proceso de la contratación y pago de los prestadores de servicios profesionales
Obligaciones*:	• Conocer, proteger su integridad, resguardar y conservar la privacidad de los datos que se manejan y mantener la secrecía de la información. • Hacer uso de los datos únicamente en el ejercicio de sus funciones y para los fines para los que han sido recabados.

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

Unidad Administrativa de la Secretaría de Desarrollo Institucional	
Identificador único¨*	(SDI-UA-11)
(Nombre del sistema A1*)	**Sistema Integral de Personal/Honorarios**
Tipo de soporte: *	Soporte físico: Expedientes de los interesados
Descripción: *	La documentación solicitada se almacena en el archivo en trámite de la SDI.
Características del lugar donde se resguardan los soportes: *	Se resguardan en el archivo de la Secretaría de Desarrollo Institucional

3. ANÁLISIS DE RIESGOS

Eliminado: Dos renglones en los que se especifican los riesgos, cinco con el impacto y doce con la mitigación, correspondientes al análisis de riesgos. Fundamento legal: artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública. En virtud de tratarse de información reservada.

Unidad Administrativa de la Secretaría de Desarrollo Institucional		
Identificador único*	(UA-SDI-11)	
Nombre del sistema	**Sistema Integral de Personal/Honorarios**	
Riesgo*	**Impacto***	**Mitigación***
Comentario	Comentario	Comentario
Comentario	Comentario	Comentario

Eliminado: Cuatro renglones en los que se especifican las medias de seguridad actuales, ocho con las medidas de seguridad necesarias y tres con las acciones para remediación, correspondientes al análisis de brecha. Fundamento legal: artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública. En virtud de tratarse de información reservada.

4. ANÁLISIS DE BRECHA

Unidad Administrativa de la Secretaría de Desarrollo Institucional		
Identificador único*	(UA-SDI-11)	
Nombre del sistema	**Sistema Integral de Personal/Honorarios**	
Medida de seguridad actual*	**Medida de seguridad necesaria***	**Acciones para remediación***
Comentario	Comentario	Comentario

5. PLAN DE TRABAJO

Eliminado: Seis renglones en los que se especifican las actividades, treinta y cuatro con la descripción, siete con la duración y cinco con la cobertura, correspondientes al plan de trabajo. Fundamento legal: artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública. En virtud de tratarse de información reservada.

Unidad Administrativa de la Secretaría de Desarrollo Institucional			
Identificador único*	(UA-SDI-11)		
Nombre del sistema	**Sistema Integral de Personal/Honorarios**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Comentario	Comentario	Comentario	Comentario

Eliminado: Diez renglones en los que se especifica la descripción correspondiente al plan de trabajo. Fundamento legal: artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública. En virtud de tratarse de información reservada.

	[redacted]		

6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

I. TRANSFERENCIAS DE DATOS PERSONALES

Unidad Administrativa de la Secretaría de Desarrollo Institucional	
Identificador único	(UA-SDI-11)
Nombre del sistema	**Sistema Integral de Personal/Honorarios**
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	No se realiza traslado de soporte físico
Transferencias mediante el traslado de soportes electrónicos:	No se realiza traslado de soporte electrónico
Transferencias mediante el traslado sobre redes electrónicas:	• Carga de información de los interesados directamente en el SIP/FUE al cual se ingresa con un usuario y contraseña proporcionados por la Dirección General de Sistemas de Personal de la DGPe. • La carga de documentos para el alta de cuentas bancarias se hace mediante la página https://portal.patronato.unam.mx/

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

Se genera un expediente por cada interesado y es resguardado en el Archivo en trámite de la SDI

III. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

El Sistema Integral de Personal/Honorarios genera un seguimiento desde que se inicia el proceso de contratación de los Prestadores de Servicios hasta la certificación del mismo

IV. REGISTRO DE INCIDENTES:

No contamos con un procedimiento de atención de incidentes

V. ACCESO A LAS INSTALACIONES

La Coordinación de las Comisiones Locales de Seguridad de la Torre de Rectoría son los encargados de la seguridad de las Instalaciones de las diversas Dependencias que convivimos en este Edificio, por lo que la vigilancia y revisión de acceso y salida está a cargo de dicha Coordinación.

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

Los encargados del sistema actualizan los datos que se requieran de los interesados.

VII. PERFILES DE USUARIO Y CONTRASEÑAS

El Sistema Integral de Personal está diseñado para que cada persona responsable tenga un usuario y contraseña para accesar a dicha aplicación y se puede trabajar en él únicamente con las IP autorizadas por la Dirección General de Sistemas de Personal.

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

Esta actividad es garantizada por la Dirección General de Personal.

IX. PLAN DE CONTINGENCIA

Esta actividad es garantizada por la Dirección General de Personal

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

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

Unidad Administrativa de la Secretaría de Desarrollo Institucional		
Identificador único	(UA-SDI-11)	
Nombre del sistema	**Sistema Integral de Personal/Honorarios**	
Recurso*	**Descripción***	**Control***
N/A	N/A	N/A

7.2 Procedimiento para la revisión de las medidas de seguridad

Unidad Administrativa de la Secretaría de Desarrollo Institucional		
Identificador único	(UA-SDI-11)	
Nombre del sistema	**Sistema Integral de Personal/Honorarios**	
Medida de seguridad*	**Procedimiento***	**Responsable***
N/A	N/A	c) N/A

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

Unidad Administrativa de la Secretaría de Desarrollo Institucional	
Identificador único	(UA-SDI-11)

Nombre del sistema	Sistema Integral de Personal/Honorarios	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***
N/A	N/A	N/A

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

Unidad Administrativa de la Secretaría de Desarrollo Institucional		
Identificador único	(UA-SDI-11)	
(Nombre del sistema A1)*	**Sistema Integral de Personal/Honorarios**	
Medida de seguridad*	**Acciones***	**Responsable***
N/A	N/A	4. N/A

8 PROGRAMA ESPECÍFICO DE CAPACITACIÓN

8.1 Programa de capacitación a los responsables de seguridad de datos personales

Unidad Administrativa de la Secretaría de Desarrollo Institucional			
Identificador único	(UA-SDI-11)		
Nombre del sistema	**Sistema Integral de Personal/Honorarios**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
La SDI solicitará a la Unidad de Transparencia de la UNAM programar un curso enfocado a la capacitación del personal involucrado en la captación, manejo, resguardo y seguridad de datos personales.	Cursos relacionados con la protección y seguridad de datos personales	Capacitación por lo menos una vez al año.	Deberan asistir por lo menos dos personas de cada área que maneje datos personales en la SDI.

De igual forma, se buscarán cursos relacionados que impartan otras instancias como el INAI.			

8.2 Programa de difusión de la protección a los datos personales

Unidad Administrativa de la Secretaría de Desarrollo Institucional			
Identificador único	(UA-SDI-11)		
Nombre del sistema	**Sistema Integral de Personal/Honorarios**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Difusión de protección de datos personales	El 25 de febrero de 2019, la UNAM difundió en la Gaceta UNAM los Lineamientos para la protección de datos personal en posesión de la UNAM	Permanente	Institucional

9 MEJORA CONTINUA

9.1 Actualización y mantenimiento de sistemas de información

Unidad Administrativa de la Secretaría de Desarrollo Institucional			
Identificador único*	(UA-SDI-11)		
Nombre del sistema	**Sistema Integral de Personal/Honorarios**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Registro y seguimiento de operaciones en el SIP/FUE.	Alimentar el sistema con los documentos e información solicitada dependiendo del movimiento	Permanente	Se trata de atender de manera oportuna las solicitudes del usuario.

9.2 Actualización y mantenimiento de equipo de cómputo

Unidad Administrativa de la Secretaría de Desarrollo Institucional			
Identificador único	(UA-SDI-11)		
Nombre del sistema	**Sistema Integral de Personal/Honorarios**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
N/A	N/A	N/A	Jefatura de Departamento de TIC de la SDI

9.3 Procesos para la conservación, preservación y respaldos de información

Unidad Administrativa de la Secretaría de Desarrollo Institucional		
Identificador único	(UA-SDI-11)	
Nombre del sistema	**Sistema Integral de Personal/Honorarios**	
Proceso*	**Descripción***	**Responsable***
N/a	N/A	Esta actividad la realiza la Dirección General de Personal

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

Unidad Administrativa de la Secretaría de Desarrollo Institucional		
Identificador único	(UA-SDI-11)	
Nombre del sistema	**Sistema Integral de Personal/Honorarios**	
Proceso	**Descripción***	**Responsable***
Procesos de borrado seguro y disposición final de equipos y componentes informáticos.	Procesos de borrado seguro y disposición final de equipos y componentes informáticos.	Jefatura de Departamento de TIC de la SDI

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

El Sistema Integral de Personal está a cargo de la Dirección General de Personal y de la Dirección General de Sistemas de la DGPe.

UNIDAD ADMINISTRATIVA
DEPARTAMENTO DE PRESUPUESTO
(12)

1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Unidad Administrativa de la Secretaría de Desarrollo Institucional	
Identificador único	(SDI-UA-12)
Nombre del sistema	**Sistema Integral de Administración Financiera (SIAF)**
Datos personales (sensibles o no) contenidos en el sistema*:	**1) Datos personales en general:** **Datos de identificación**: Nombre o razón social, domicilio fiscal, teléfono particular o celular, correo electrónico, RFC, Constancia de Situación Fiscal y datos bancarios. 2) **No se recaban datos personales sensibles**.
Responsable:	
Nombre*:	Mtra. Sara Angélica Hernández Bautista
Cargo*:	Jefa de Unidad Administrativa
Funciones*:	• Instrumentar mecanismos de coordinación y supervisión de los recursos presupuestales e ingresos extraordinarios asignados a la Secretaría de Desarrollo Institucional, a fin de tramitar los pagos de los prestadores de servicios que solicitan las áreas que la conforman para su buen funcionamiento • Establecer comunicación con las dependencias centralizadoras, para tratar los asuntos relacionados con la gestión administrativa, que realiza el departamento de Presupuesto. • Supervisar conforme a la normatividad institucional establecida por las dependencias de la UNAM, el uso adecuad de los recursos presupuestales y financieros asignados o generados por la Secretaría de Desarrollo Institucional.
Obligaciones*:	• Conocer, proteger su integridad, resguardar y conservar la privacidad de los datos que se manejan y mantener la secrecía de la información. • Hacer uso de los datos únicamente en el ejercicio de sus funciones y para los fines para los que han sido recabados.
	Encargados:
Nombre del Encargado 1	L.C. Isaac Pérez Hernández
Cargo:	Jefe del Departamento Presupuesto
Funciones:	• Supervisar el registro y control en el SIAF de las afectaciones que se realizan durante el ejercicio presupuestal, en estricta comunicación con los responsables de su ejercicio, a efecto de impedir sobregiros o cargos indebidos. • Registrar trámites de pagos a proveedores, viáticos, trabajos de campo, reembolsos, gastos de intercambio, becas, prestación de servicios y boletos de avión, con cargo al Presupuesto asignado y/o Ingresos Extraordinarios con que cuenta la Secretaría de Desarrollo Institucional.

Obligaciones:	• Conocer, proteger su integridad, resguardar y conservar la privacidad de los datos que se manejan y mantener la secrecía de la información. • Hacer uso de los datos únicamente en el ejercicio de sus funciones y para los fines para los que han sido recabados.
Nombre del Encargado 2	L. A. Iván Gutiérrez Rojas
Cargo:	Jefe de Área
Funciones:	• Registrar trámites de pagos a proveedores, viáticos, trabajos de campo, reembolsos, gastos de intercambio, becas, prestación de servicios y boletos de avión, con cargo al Presupuesto asignado y/o Ingresos Extraordinarios con que cuenta la Secretaría de Desarrollo Institucional.
Obligaciones:	• Conocer, proteger su integridad, resguardar y conservar la privacidad de los datos que se manejan y mantener la secrecía de la información. • Hacer uso de los datos únicamente en el ejercicio de sus funciones y para los fines para los que han sido recabados.
	Usuarios:
Nombre del Encargado 3	L.C. David Jiménez Figueroa
Cargo:	Asistente de Procesos
Funciones*:	• Registrar trámites de pagos a proveedores, viáticos, trabajos de campo, reembolsos, gastos de intercambio, becas, prestación de servicios y boletos de avión, con cargo al Presupuesto asignado y/o Ingresos Extraordinarios con que cuenta la Secretaría de Desarrollo Institucional.
Obligaciones*:	• Conocer, proteger su integridad, resguardar y conservar la privacidad de los datos que se manejan y mantener la secrecía de la información. • Hacer uso de los datos únicamente en el ejercicio de sus funciones y para los fines para los que han sido recabados.

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

Unidad Administrativa de la Secretaría de Desarrollo Institucional	
Identificador único	(SDI-UA-12)
Nombre del sistema	**Sistema Integral de Administración Financiera (SIAF)**
Tipo de soporte:	Sistema electrónico.
Descripción:	Servidor de la SDI Página Web.
Características del lugar donde se resguardan los soportes:*	Equipos de cómputo que tienen instalado el Sistema SIAF. Área de servidores bajo el resguardo de la Jefa del Departamento de TIC´s. Página web: https://directoriodeproveedores.patronato.unam.mx, que corresponde al "Padrón de Proveedores y Contratistas" de la UNAM.

SIN TEXTO

3. ANÁLISIS DE RIESGOS

Eliminado: Cinco renglones en los que se especifican los riesgos, diez con el impacto y dieciséis con la mitigación, correspondientes al análisis de riesgos. Fundamento legal: artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública. En virtud de tratarse de información reservada.

Unidad Administrativa de la Secretaría de Desarrollo Institucional		
Identificador único*	(SDI-UA-12)	
Nombre del sistema	**Sistema Integral de Administración Financiera (SIAF)**	
Riesgo*	**Impacto***	**Mitigación***
Comentario	Comentario	Comentario
Comentario	Comentario	Comentario

4. ANÁLISIS DE BRECHA

Eliminado: Cuatro renglones en los que se especifican las medias de seguridad actuales, cuatro con las medidas de seguridad necesarias y tres con las acciones para remediación, correspondientes al análisis de brecha. Fundamento legal: artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública. En virtud de tratarse de información reservada.

Unidad Administrativa de la Secretaría de Desarrollo Institucional		
Identificador único*	(SDI-UA-12)	
Nombre del sistema	**Sistema Integral de Administración Financiera (SIAF)**	
Medida de seguridad actual*	**Medida de seguridad necesaria***	**Acciones para remediación***
Comentario	Comentario	Comentario

5. PLAN DE TRABAJO

Eliminado: Dos renglones en los que se especifican las actividades, dieciséis con la descripción, tres con la duración y cinco con la cobertura, correspondientes al plan de trabajo. Fundamento legal: artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública. En virtud de tratarse de información reservada.

Unidad Administrativa de la Secretaría de Desarrollo Institucional			
Identificador único*	(SDI-UA-12)		
Nombre del sistema	**Sistema Integral de Administración Financiera (SIAF)**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Comentario	Comentario	Comentario	Comentario

6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

I. TRANSFERENCIAS DE DATOS PERSONALES

Unidad Administrativa de la Secretaría de Desarrollo Institucional	
Identificador único	(SDI-UA-12)
Nombre del sistema	**Sistema Integral de Administración Financiera (SIAF)**
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	No se realiza traslado de soporte físico
Transferencias mediante el traslado de soportes electrónicos:	No se realiza traslado de soporte electrónico
Transferencias mediante el traslado sobre redes electrónicas:	• Carga de información de proveedores en la página web: https://directoriodeproveedores.patronato.unam.mx, que corresponde al "Padrón de Proveedores y Contratistas" de la UNAM. • En el Padrón de Proveedores y Contratistas de la UNAM, a través de dirección electrónica, se registra los datos personales de las personas y/o empresas que desean formar parte de los proveedores que prestan sus servicios a las Dependencias y Entidades Académicas de la UNAM. • Para el acceso a la página electrónica, es necesario contar con un usuario y contraseña. • El Patronato de la Universidad Nacional Autónoma de México (UNAM) protegerá y tratará los datos personales que se recaben en este sitio web, bajo responsabilidad de la Contaduría General. • El Patronato utilizará los datos solicitados para brindar el servicio de pago por transferencias bancarias, actualizar el "Padrón de Proveedores y Contratistas", así como para dar cumplimiento a obligaciones tributarias de la UNAM.

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

El "Padrón de Proveedores y Contratistas" de la UNAM no realiza tratamiento de datos personales con soportes físicos, ya que se encuentra a través de soporte electrónico a través de internet.

III. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

El "Padrón de Proveedores y Contratistas" genera un número de proveedor por cada registro que se realiza, tanto para personas físicas, como para personas morales.

Con el número de proveedor que le fue asignado y su RFC, en el SIAF permite identificar las operaciones y compromisos que contrae con la UNAM con el proveedor.

IV. REGISTRO DE INCIDENTES

Para el SIAF, en caso de presentar algún incidente, emite mensajes de alerta a través de la pantalla del equipo de cómputo donde se encuentre cargado el sistema, dejando registro en el servidor que aloja la información que se registra por cada operación.

Para "Padrón de Proveedores y Contratistas" de la UNAM, no contamos con una bitácora de incidentes, debido a que la administración del sitio web, se encuentra Centralizada.

V. ACCESO A LAS INSTALACIONES

La Coordinación de las Comisiones Locales de Seguridad de la Torre de Rectoría son los encargados de la seguridad de las Instalaciones de las diversas dependencias que convivimos en este edificio, por lo que la vigilancia y revisión de acceso y salida está a cargo de dicha coordinación.

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

Los proveedores son los encargados de realizar la notificación en caso de alguna actualización de datos personales, misma que es transferida a través de la página web: https://directoriodeproveedores.patronato.unam.mx, que corresponde al "Padrón de Proveedores y Contratistas" de la UNAM.

VII. PERFILES DE USUARIO Y CONTRASEÑAS

El SIAF está diseñado para que cada persona responsable tenga un usuario y contraseña para acceso al Sistema, a través del equipo de cómputo en donde se encuentre cargado, además que se tiene asignado roles por cada nivel de los usuarios que participan en el proceso de registro de trámites de pagos a proveedores, viáticos, trabajos de campo, reembolsos, gastos de intercambio, becas, prestación de servicios y boletos de avión, con cargo al Presupuesto asignado y/o Ingresos Extraordinarios con que cuenta la Secretaría de Desarrollo Institucional.

El "Padrón de Proveedores y Contratistas" está diseñado para que cada persona responsable tenga un usuario y contraseña, pueda tener acceso al sitio web, únicamente para realizar el registro de alta de un nuevo proveedor, o bien realizar alguna actualización de datos personales.

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

En el caso del SIAF esta actividad es garantizada por la Jefa de Departamento de TIC´s de la SDI.

En el caso del "Padrón de Proveedores y Contratistas", esta actividad es garantizada por el Patronato Universitario a través de la Contaduría General.

IX. PLAN DE CONTINGENCIA

En el caso del SIAF esta actividad es garantizada por la Jefa de Departamento de TIC´s de la SDI.

En el caso del “Padrón de Proveedores y Contratistas”, esta actividad es garantizada por el Patronato Universitario a través de la Contaduría General.

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

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

Unidad Administrativa de la Secretaría de Desarrollo Institucional		
Identificador único	(SDI-UA-12)	
Nombre del sistema	**Sistema Integral de Administración Financiera (SIAF)**	
Recurso*	**Descripción***	**Control***
N/A	N/A	N/A

7.2 Procedimiento para la revisión de las medidas de seguridad

Unidad Administrativa de la Secretaría de Desarrollo Institucional		
Identificador único	(SDI-UA-12)	
Nombre del sistema	**Sistema Integral de Administración Financiera (SIAF)**	
Medida de seguridad*	**Procedimiento***	**Responsable***
N/A	N/A	d) N/A

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

Unidad Administrativa de la Secretaría de Desarrollo Institucional		
Identificador único	(SDI-UA-12)	
Nombre del sistema	**Sistema Integral de Administración Financiera (SIAF)**	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***
N/A	N/A	N/A

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

Unidad Administrativa de la Secretaría de Desarrollo Institucional		
Identificador único	(SDI-UA-12)	
(Nombre del sistema A1)*	**Sistema Integral de Administración Financiera (SIAF)**	
Medida de seguridad*	**Acciones***	**Responsable***
N/A	N/A	5. N/A

8 PROGRAMA ESPECÍFICO DE CAPACITACIÓN

8.1 Programa de capacitación a los responsables de seguridad de datos personales

Unidad Administrativa de la Secretaría de Desarrollo Institucional			
Identificador único	(SDI-UA-12)		
Nombre del sistema	**Sistema Integral de Administración Financiera (SIAF)**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
La SDI solicitará a la Unidad de Transparencia de la UNAM programar un curso enfocado a la capacitación del personal involucrado en la captación, manejo, resguardo y seguridad de datos personales. De igual forma, se buscarán cursos relacionados que impartan otras instancias como el INAI.	Cursos relacionados con la protección y seguridad de datos personales	Capacitación por lo menos una vez al año.	Deberan asistir por lo menos dos personas de cada área que maneje datos personales en la SDI.

8.2 Programa de difusión de la protección a los datos personales

Unidad Administrativa de la Secretaría de Desarrollo Institucional			
Identificador único	(SDI-UA-12)		
Nombre del sistema	**Sistema Integral de Administración Financiera (SIAF)**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Difusión de protección de datos personales	El 25 de febrero de 2019, la UNAM difundió en la Gaceta UNAM los Lineamientos para la protección de datos personal en posesión de la UNAM	Permanente	Institucional

9 MEJORA CONTINUA

9.1 Actualización y mantenimiento de sistemas de información

Unidad Administrativa de la Secretaría de Desarrollo Institucional			
Identificador único*	(SDI-UA-12)		
Nombre del sistema	**Sistema Integral de Administración Financiera (SIAF)**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Esta actividad la realiza el Instituto de Ingeniería.	N/A	N/A	N/A

9.2 Actualización y mantenimiento de equipo de cómputo

Unidad Administrativa de la Secretaría de Desarrollo Institucional	
Identificador único	(SDI-UA-12)

Nombre del sistema	**Sistema Integral de Administración Financiera (SIAF)**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Mantenimiento preventivo	Realizar el mantenimiento preventivo del equipo de trabajo tanto a nivel hardware como software para mantenerlo funcional.	2 veces al año	Equipos de la oficina de la Secretaria de Desarrollo Institucional.

9.3 Procesos para la conservación, preservación y respaldos de información

Unidad Administrativa de la Secretaría de Desarrollo Institucional		
Identificador único	(SDI-UA-12)	
Nombre del sistema	**Sistema Integral de Administración Financiera (SIAF)**	
Proceso*	**Descripción***	**Responsable***
Contar con un servidor con acceso restringido en donde se almacena la información de datos personales que se capturan para atender los trámites de las distintas áreas que integran la Secretaría de Desarrollo Institucional.	Área soporte encargada de ejecutar acciones para garantizar la seguridad de la información, minimizando alguna fuga de información.	Jefa de Departamento de TIC´s.

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

Unidad Administrativa de la Secretaría de Desarrollo Institucional	
Identificador único	(SDI-UA-12)
Nombre del sistema	**Sistema Integral de Administración Financiera (SIAF)**

Proceso	Descripción*	Responsable*
Procesos de borrado seguro y disposición final de equipos y componentes informáticos.	Procesos de borrado seguro y disposición final de equipos y componentes informáticos.	Jefa de Departamento de TIC.

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

El SIAF está diseñado para que cada persona responsable tenga un usuario y contraseña para acceso al Sistema, a través del equipo de cómputo en donde se encuentre cargado, además que se tiene asignado roles por cada nivel de los usuarios que participan en el proceso de registro o eliminación de datos personales.

Las personas que cuenten con usuario y contraseña al "Padrón de Proveedores y Contratistas", no tiene injerencia en la cancelación de tratamiento de datos personales, debido a que esta actividad depende del Patronato Universitario a través de la Contaduría General de la UNAM.

UNIDAD ADMINISTRATIVA
DEPARTAMENTO DE PRESUPUESTO
(13)

1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Unidad Administrativa de la Secretaría de Desarrollo Institucional	
Identificador único	(SDI-UA-13)
Nombre del sistema	**Sistema Factura Digital UNAM**
Datos personales (sensibles o no) contenidos en el sistema*:	**1. Datos personales en general:** **a) Datos de identificación**: Nombre o razón social, domicilio fiscal, teléfono particular o celular, correo electrónico, RFC, Constancia de Situación Fiscal y datos bancarios. **2. No se recaban datos personales sensibles**
Responsable:	
Nombre*:	Mtra. Sara Angélica Hernández Bautista
Cargo*:	Jefa de Unidad Administrativa
Funciones*:	• Supervisar conforme a la normatividad institucional establecida por las dependencias de la UNAM, el uso adecuad de los ingresos extraordinarios generados por la SDI.
Obligaciones*:	• Conocer, proteger su integridad, resguardar y conservar la privacidad de los datos que se manejan y mantener la secrecía de la información. • Hacer uso de los datos únicamente en el ejercicio de sus funciones y para los fines para los que han sido recabados.
	Encargados:
Nombre del Encargado 1	L.C. Isaac Pérez Hernández
Cargo:	Jefe del Departamento Presupuesto
Funciones:	• Emisión de CFDI´s como mecanismo de comprobación fiscal, para la generación, procesamiento, transmisión y resguardo de los documentos fiscales de manera digital.
Obligaciones:	• Conocer, proteger su integridad, resguardar y conservar la privacidad de los datos que se manejan y mantener la secrecía de la información. • Hacer uso de los datos únicamente en el ejercicio de sus funciones y para los fines para los que han sido recabados.

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

Unidad Administrativa de la Secretaría de Desarrollo Institucional	
Identificador único	(SDI-UA-13)
Nombre del sistema	**Sistema Factura Digital UNAM**

Tipo de soporte:	Sistema electrónico.
Descripción:	Nube privada.
Características del lugar donde se resguardan los soportes:*	Servidores del Patronato Universitario.

3. ANÁLISIS DE RIESGOS

Eliminado: Cuatro renglones en los que se especifican los riesgos, nueve con el impacto y catorce con la mitigación, correspondientes al análisis de riesgos. Fundamento legal: artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública. En virtud de tratarse de información reservada.

Unidad Administrativa de la Secretaría de Desarrollo Institucional		
Identificador único*	(SDI-UA-13)	
Nombre del sistema	**Sistema Factura Digital UNAM**	
Riesgo*	**Impacto***	**Mitigación***
Comentario	Comentario	Comentario
Comentario	Comentario	Comentario

4. ANÁLISIS DE BRECHA

Eliminado: Siete renglones en los que se especifican las medias de seguridad actuales, once con las medidas de seguridad necesarias y tres con las acciones para remediación, correspondientes al análisis de brecha.
Fundamento legal: artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública. En virtud de tratarse de información reservada.

Unidad Administrativa de la Secretaría de Desarrollo Institucional		
Identificador único*	(SDI-UA-13)	
Nombre del sistema	**Sistema Factura Digital UNAM**	
Medida de seguridad actual*	**Medida de seguridad necesaria***	**Acciones para remediación***
Comentario	Comentario	Comentario

5. PLAN DE TRABAJO

Eliminado: Cuatro renglones en los que se especifican las actividades, diez con la descripción, tres con la duración y cinco con la cobertura, correspondientes al plan de trabajo. Fundamento legal: artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública. En virtud de tratarse de información reservada.

Unidad Administrativa de la Secretaría de Desarrollo Institucional			
Identificador único*	(SDI-UA-13)		
Nombre del sistema	**Sistema Factura Digital UNAM**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Comentario	Comentario	Comentario	Comentario

6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

I. TRANSFERENCIAS DE DATOS PERSONALES

Unidad Administrativa de la Secretaría de Desarrollo Institucional	
Identificador único	(SDI-UA-13)
Nombre del sistema	**Sistema Factura Digital UNAM**
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	No se realiza traslado de soporte físico
Transferencias mediante el traslado de soportes electrónicos:	No se realiza traslado de soporte electrónico
Transferencias mediante el traslado sobre redes electrónicas:	• Carga de información de proveedores y solicitantes de un CFDI´s en el Sistema de Factura Digital, administrado por el Patronato Universitario. • Para el acceso al sistema, es necesario contar con un usuario y contraseña. • El Patronato de la Universidad Nacional Autónoma de México (UNAM) protegerá y tratará los datos personales que se recaben en el sistema, bajo responsabilidad de la Contaduría General.

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

El Sistema de Factura Digital no realiza tratamiento de datos personales con soportes físicos, ya que se encuentra a través de soporte electrónico a través del mismo sistema.

III. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

El Sistema de Factura Digital cuenta con una opción de Consulta, la cual permite visualizar los usuarios que ingresaron al sistema, la fecha y hora en que se emitió un CFDI.

IV. REGISTRO DE INCIDENTES:

No contamos con un procedimiento de atención de incidentes.

V. ACCESO A LAS INSTALACIONES

La Coordinación de las Comisiones Locales de Seguridad de la Torre de Rectoría son los encargados de la seguridad de las instalaciones de las diversas dependencias que convivimos en este edificio, por lo que la vigilancia y revisión de acceso y salida está a cargo de dicha Coordinación.

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

La Contaduría General, es la encargada realizar las actualizaciones y/o notificaciones de los posibles cambios realizados al sistema.

VII. PERFILES DE USUARIO Y CONTRASEÑAS

El Sistema de Factura Digital está diseñado para que cada persona responsable tenga un usuario y contraseña y pueda tener acceso al sistema para la emisión de un nuevo CFDI. Los usuarios y contraseñas son autorizados por el Patronato Universitario a través de la Contaduría General.

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

Esta actividad es garantizada por el Patronato Universitario a través de la Contaduría General.

IX. PLAN DE CONTINGENCIA

Esta actividad es garantizada por el Patronato Universitario a través de la Contaduría General.

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

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

Unidad Administrativa de la Secretaría de Desarrollo Institucional		
Identificador único	(SDI-UA-13)	
Nombre del sistema	**Sistema Factura Digital UNAM**	
Recurso*	**Descripción***	**Control***
N/A	N/A	N/A

7.2 Procedimiento para la revisión de las medidas de seguridad

Unidad Administrativa de la Secretaría de Desarrollo Institucional		
Identificador único	(SDI-UA-13)	
Nombre del sistema	**Sistema Factura Digital UNAM**	
Medida de seguridad*	**Procedimiento***	**Responsable***
N/A	N/A	e) N/A

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

Unidad Administrativa de la Secretaría de Desarrollo Institucional		
Identificador único	(SDI-UA-13)	
Nombre del sistema	**Sistema Factura Digital UNAM**	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***
N/A	N/A	N/A

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

Unidad Administrativa de la Secretaría de Desarrollo Institucional		
Identificador único	(SDI-UA-13)	
(Nombre del sistema A1)*	**Sistema Factura Digital UNAM**	
Medida de seguridad*	**Acciones***	**Responsable***
N/A	N/A	6. N/A

8 PROGRAMA ESPECÍFICO DE CAPACITACIÓN

8.1 Programa de capacitación a los responsables de seguridad de datos personales

Unidad Administrativa de la Secretaría de Desarrollo Institucional			
Identificador único	(SDI-UA-13)		
Nombre del sistema	**Sistema Factura Digital UNAM**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
La SDI solicitará a la Unidad de Transparencia de la UNAM programar un curso enfocado a la capacitación del	Cursos relacionados con la protección y seguridad de datos personales	Capacitación por lo menos una vez al año.	Deberan asistir por lo menos dos personas de cada área que maneje datos personales en la SDI.

personal involucrado en la captación, manejo, resguardo y seguridad de datos personales. De igual forma, se buscarán cursos relacionados que impartan otras instancias como el INAI.			

8.2 Programa de difusión de la protección a los datos personales

Unidad Administrativa de la Secretaría de Desarrollo Institucional			
Identificador único	(SDI-UA-13)		
Nombre del sistema	**Sistema Factura Digital UNAM**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Difusión de protección de datos personales	El 25 de febrero de 2019, la UNAM difundió en la Gaceta UNAM los Lineamientos para la protección de datos personal en posesión de la UNAM	Permanente	Institucional

9 MEJORA CONTINUA

9.1 Actualización y mantenimiento de sistemas de información

Unidad Administrativa de la Secretaría de Desarrollo Institucional			
Identificador único*	(SDI-UA-13)		
Nombre del sistema	**Sistema Factura Digital UNAM**		
Actividad*	**Descripción***	**Duración***	**Cobertura***

Esta actividad la realiza el Patronato Universitario a través de la Contaduría General.	N/A	N/A	N/A

9.2 Actualización y mantenimiento de equipo de cómputo

Unidad Administrativa de la Secretaría de Desarrollo Institucional			
Identificador único	(SDI-UA-13)		
Nombre del sistema	**Sistema Factura Digital UNAM**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Mantenimiento preventivo	Realizar el mantenimiento preventivo del equipo de trabajo tanto a nivel hardware como software para mantenerlo funcional.	2 veces al año	Equipos de la oficina de la Secretaria de Desarrollo Institucional.

9.3 Procesos para la conservación, preservación y respaldos de información

Unidad Administrativa de la Secretaría de Desarrollo Institucional		
Identificador único	(SDI-UA-13)	
Nombre del sistema	**Sistema Factura Digital UNAM**	
Proceso*	**Descripción***	**Responsable***
N/A	N/A	Esta actividad la realiza la Contaduría General.

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

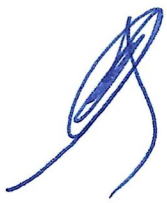
Unidad Administrativa de la Secretaría de Desarrollo Institucional		
Identificador único	(SDI-UA-13)	
Nombre del sistema	**Sistema Factura Digital UNAM**	
Proceso	**Descripción***	**Responsable***
Procesos de borrado seguro y disposición final de equipos y componentes informáticos.	Procesos de borrado seguro y disposición final de equipos y componentes informáticos.	Jefa de Departamento de TIC´s.

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

Las personas que cuenten con usuario y contraseña al Sistema de Factura Digital, no tienen injerencia en la cancelación de tratamiento de datos personales, debido a que esta actividad depende del Patronato Universitario a través de la Contaduría General de la UNAM.

Secretaría de Desarrollo Institucional
Documento de Seguridad
Partes clasificadas: Análisis de riesgos (riesgo, impacto y mitigación), páginas 10, 22, 23, 34, 35, 47, 58, 59, 69, 70, 71, 85, 98, 109, 121, 133, 146 y 158; Análisis de brecha (medida de seguridad actual, medida de seguridad necesaria y acciones para remediación), páginas 11, 24, 36, 48, 60, 72, 87, 99, 110, 122, 134, 147 y 159, y Plan de trabajo (actividad, descripción duración y cobertura), páginas 12, 25, 37, 49, 61, 73, 74, 88, 100, 111, 123, 124, 135, 136, 148 y 160.
Periodo de reserva: Por un periodo de cinco años, que se computarán a partir de la fecha de la resolución.
Fundamento: Artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP) y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública (LFTAIP).
En virtud de tratarse de información reservada que obstruya la prevención o persecución de los delitos.
Fecha y número de acta de la sesión: 19/08/2022 y acta CTUNAM/525/2022

11. APROBACIÓN DEL DOCUMENTO DE SEGURIDAD

		Nombre y firma de quienes revisaron el presente documento:
Responsable del desarrollo:	Ing. Linda Ma. del C. Rey Hernández Jefa del Departamento de TIC linda.rey@unam.mx	
Revisó:	Lic. Edgar Mauricio Reyes Tableros Coordinador de Análisis y Gestión Jurídica emrt@unam.mx	
Autorizó:	Dra. Patricia Dolores Dávila Aranda Secretaria de Desarrollo Institucional sdi@unam.mx	
Fecha de aprobación:	16 de agosto de 2022	
Fecha de actualización:	16 de agosto de 2022	

COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

RESOLUCIÓN: CTUNAM/525/2022

Visto el expediente relativo a la clasificación de reserva total de una parte de la información, para la elaboración de la versión pública , que someten el **Instituto de Matemáticas,** el **Instituto de Fisiología Celular,** la **Dirección General de la Escuela Nacional Colegio de Ciencias** y **Humanidades,** la **Escuela Nacional Colegio de Ciencias y Humanidades Planteles Azcapotzalco, Vallejo, Naucalpan, Oriente y Sur**, la **Facultad de Filosofía y Letras,** la **Coordinación de Difusión Cultural**, la **Dirección General de Estudios de Legislación Universitaria,** el **Centro Universitario de Teatro,** la **Dirección General de Radio UNAM,** la **Secretaría de Desarrollo Institucional,** el **Instituto de Física**, el **Consejo Académico del Área de las Ciencias Biológicas, Químicas y de la Salud,** el **Comité de Análisis para las Intervenciones Urbanas, Arquitectónicas y de las Ingenierías,** el **Museo Universitario del Chopo,** la **Dirección General de Música,** la **Dirección de Danza,** el **Centro de Investigaciones en Geografía Ambiental, Campus Morelia,** el **Museo Universitario de Arte Contemporáneo,** la **Defensoría de los Derechos Universitarios, Igualdad y Atención de la Violencia de Género,** el **Instituto de Química,** la **Dirección de Literatura y Fomento a la Lectura,** la **Dirección General de Servicios Administrativos,** la **Dirección de Teatro UNAM,** el **Centro de Ciencias Genómicas,** la **Facultad de Artes y Diseño,** la **Dirección General de Televisión Universitaria,** el **Centro Cultural Universitario Tlatelolco,** la **Dirección General de Orientación y Atención Educativa,** el **Consejo Académico del Área de las Ciencias Sociales,** la **Escuela Nacional de Estudios Superiores, Unidad Mérida,** el **Instituto de Ecología,** la **Dirección General de Cooperación e Internacionalización,** el **Instituto de Investigaciones Biomédicas,** la **Casa del Lago "Mtro. Juan José Arreola",** la **Coordinación para la Igualdad de Género,** la **Dirección General de la Escuela Nacional Preparatoria** y la **Escuela Nacional Preparatoria, Planteles 3 "Justo Sierra"** y **4 "Vidal Castañeda y Nájera"** y la **Dirección General del Deporte Universitario,** en relación con sus respectivos **Documentos de Seguridad**, se procede a dictar la presente resolución con base en los siguientes:

A N T E C E D E N T E S

I. Con fecha 26 de enero de 2017 se publicó en el Diario Oficial de la Federación el Decreto por el que se expide la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, reglamentaria de los artículos 6o., Base A y 16, segundo párrafo, de la Constitución Política de los Estados Unidos Mexicanos, en materia de protección de datos personales en posesión de sujetos obligados.

II. Mediante Acuerdo **ACT-PUB/19/12/2017.10**, de fecha 19 de diciembre de 2017, publicado en el Diario Oficial de la Federación con fecha 26 de enero de 2018, el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales aprobó los Lineamientos Generales de Protección de Datos Personales para el Sector Público.

III. A través del Acuerdo **ACT-PUB/11/11/2020.05**, de fecha 11 de noviembre de 2020, publicado en el Diario Oficial de la Federación con fecha 25 de noviembre de 2020, dicho Órgano Garante aprobó la adición de un Título Décimo a los Lineamientos Generales de Protección de Datos Personales para el Sector Público, a fin de establecer las disposiciones generales que permitirán desarrollar el procedimiento de diseño y aplicación del sistema y procedimiento para llevar a cabo la evaluación sobre el desempeño de los responsables

respecto al cumplimiento de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y demás disposiciones que resulten aplicables en la materia.

IV. Por Acuerdo **ACT-PUB/17/11/2021.05**, de fecha 17 de noviembre de 2021, publicado en el Diario Oficial de la Federación con fecha 26 de noviembre de 2021, el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales aprobó los "Instrumentos Técnicos que refiere el Título Décimo de los Lineamientos Generales de Protección de Datos Personales para el Sector Público, en materia de evaluación del desempeño de los sujetos obligados del sector público federal en el cumplimiento a la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados".

V. Los artículos 247 y 248 de Lineamientos Generales de Protección de Datos Personales para el Sector Público, así como las reglas Décima Tercera y Décima Cuarta del apartado "V. Reglas de Generales de Evaluación" del Documento Técnico de Evaluación y sus anexos de los Instrumentos Técnicos que refiere el Título Décimo de los Lineamientos Generales de Protección de Datos Personales para el Sector Público, en materia de Evaluación del Desempeño de los Sujetos Obligados del Sector Público Federal en el Cumplimiento a la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, establecen que la información y documentos que se pongan a disposición de los titulares de datos personales y del Instituto, deberán ser revisados por el responsable a fin de verificar que no contengan información confidencial o reservada y, de ser el caso, deberá publicarse la versión pública de dicha documentación.

Por otra parte, en el apartado "VI. Metodología, criterios, formatos e indicadores en materia de evaluación del desempeño de los responsables respecto al cumplimiento de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y demás disposiciones que resulten aplicables en la materia", Capítulo II. Criterios y formatos, **Vertiente 2**: Deberes, **Variable 2.1** Deber de seguridad, se establece que el responsable, por ningún motivo, debe publicar el documento de seguridad de manera íntegra, por lo que deberá poner a disposición la versión pública del mismo, en la cual se deberá proteger la información relativa al plan de trabajo, el análisis de riesgo y el análisis de brecha.

VI. En términos de los artículos 106, fracción II, de la Ley General de Transparencia y Acceso a la Información Pública; 98 fracción II de la Ley Federal de Transparencia y Acceso a la Información Pública, así como 34, fracción II del Reglamento de Transparencia y Acceso a la Información Púbica de la Universidad Nacional Autónoma de México, la clasificación de la información será procedente cuando, entre otros supuestos, se determiné mediante una resolución de autoridad competente.

VII. La Presidencia del Comité de Transparencia recibió diversos oficios, mediante los cuales las Áreas Universitarias sometieron a consideración de este Cuerpo Colegiado, la clasificación parcial de información reservada de sus Documentos de Seguridad, mismos que se enlistan a continuación:

COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

RESOLUCIÓN: CTUNAM/525/2022

Oficio	Área Universitaria	Fecha de presentación
IMAT/D048/2022	Instituto de Matemáticas	15/08/2022
IFCE/DIR/184/2022	Instituto de Fisiología Celular	
CCHDG/DIR/145/08/2022	Dirección General de la Escuela Nacional Colegio de Ciencias y Humanidades	
CCHA/DIR/415/VIII/2022	Plantel Azcapotzalco de la Escuela Nacional Colegio de Ciencias y Humanidades	
CCHN.91.20/580/2022	Plantel Naucalpan de la Escuela Nacional Colegio de Ciencias y Humanidades	
CCHO/DIR/445/2022	Plantel Oriente de la Escuela Nacional Colegio de Ciencias y Humanidades	
OF/CCHS/DIR/160/2022	Plantel Sur de la Escuela Nacional Colegio de Ciencias y Humanidades	
CCHV/OJ/135/2022	Plantel Vallejo de la Escuela Nacional Colegio de Ciencias y Humanidades	
FFLE/CP/034/2022	Facultad de Filosofía y Letras	
CODC/182/2022	Coordinación de Difusión Cultural	
DGEL/JT/3454/2022	Dirección General de Estudios de Legislación Universitaria	16/08/2022
CUTE/DIR/66/2022	Centro Universitario de Teatro	
DGRU/115/2022	Dirección General de Radio UNAM	
SDI/116/2022	Secretaría de Desarrollo Institucional	17/08/2022
IFIS/D/221/2022 IFIS/D/223/2022	Instituto de Física	
CJBS/112/22	Consejo Académico del Área de las Ciencias Biológicas, Químicas y de la Salud	
CAI/063/2022	Comité de Análisis para las Intervenciones Urbanas, Arquitectónicas y de las Ingenierías	
DIR/MUCH/0160/2022	Museo Universitario del Chopo	
DGMU/114/08/2022	Dirección General de Música	
DDAN/0356/2022	Dirección de Danza	
CIGA/D/133/2022	Centro de Investigaciones en Geografía Ambiental, Campus Morelia	
DiGAV/D/2315/2022	Museo Universitario de Arte Contemporáneo	
DDUIAVG/T/2427/2022	Defensoría de los Derechos Universitarios, Igualdad y Atención de la Violencia de Género	
IQUI 427/2022	Instituto de Química	
DLFL/208/2022	Dirección de Literatura y Fomento a la	

	Lectura	
DGSA/0381/2022	Dirección General de Servicios Administrativos	
DTEA/107/2022	Dirección de Teatro UNAM	
ENP3/DIRE/239/2022	Escuela Nacional Preparatoria, Plantel 3	
CCG/DIR/293/2022	Centro de Ciencias Genómicas	
FAD/DIR/445/2022	Facultad de Artes y Diseño	
DGTV/DG/197/2022	Dirección General de Televisión Universitaria	
CCUT/139/2022	Centro Cultural Universitario Tlatelolco	
ENPDG/314/2022	Dirección General de la Escuela Nacional Preparatoria	
DGOAE/416/2022	Dirección General de Orientación y Atención Educativa	
CJCS/124/2022	Consejo Académico del Área de las Ciencias Sociales	
ENES/MID/OFJ/199/2022	Escuela Nacional de Estudios Superiores, Unidad Mérida	
IECO/DIR/327/2022	Instituto de Ecología	
DGECI/DG/0869/2022	Dirección General de Cooperación e Internacionalización	
IIB/DIR/309/2022	Instituto de Investigaciones Biomédicas	
DCLA/Of.096/2022	Casa del Lago "Mtro Juan José Arreola"	
ENP4/DIR/108/2022	Escuela Nacional Preparatoria, Plantel 4	
CIG/C/320/2022	Coordinación para la Igualdad de Género	
DGDU/CJ/930/2022	Dirección General del Deporte Universitario	

En dichos oficios, las Áreas Universitarias informaron lo siguiente:

> *"Los Instrumentos Técnicos a los que se refiere el Título Décimo de los Lineamientos Generales de Protección de Datos Personales para el Sector Público en materia de evaluación del desempeño de los sujetos obligados del sector público federal en el cumplimiento a la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados[1]; exige elaborar versión pública del documento de seguridad de esta área universitaria.*
>
> *Una vez analizada la información que se solicitó en el primer punto del 'Documento de seguridad', se observó que la misma se ajusta al supuesto de reserva contemplado en los artículos 113, fracción VII de la Ley General de Transparencia y*

[1] *DOF: 26 de noviembre de 2021*

Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública, ya que su divulgación obstruiría el deber de esta Universidad de establecer y mantener las medidas de seguridad técnica, administrativa y física de los datos personales que los titulares confían a esta institución.

En este contexto, la información puede ser clasificada como reservada en términos de los artículos 106, fracción II, de la Ley General de Transparencia y Acceso a la Información Pública (Ley General) y 98 fracción II de la Ley Federal de Transparencia y Acceso a la Información Pública (Ley Federal), en relación con los artículos 247 y 248 de Lineamientos Generales de Protección de Datos Personales para el Sector Público y las reglas generales de evaluación Décima Tercera y Décima Cuarta del apartado V. Reglas de Generales de Evaluación, del Documento Técnico de Evaluación y sus anexos de los Instrumentos Técnicos que refiere el Título Décimo de los Lineamientos Generales de Protección de Datos Personales para el Sector Público, en materia de Evaluación del Desempeño de los Sujetos Obligados del Sector Público Federal en el Cumplimiento a la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

A efecto de cumplir con lo señalado, se realiza la siguiente prueba de daño relativa al documento de seguridad de datos personales que obran en el Sistema de Gestión de Seguridad de Datos Personales … El documento de seguridad contiene los siguientes apartados cuya autorización de reserva total se solicita a ese Comité:

Anexos o Políticas	***Contenido y su afectación***	***Páginas***
a) Análisis de riesgos	*El análisis de riesgos contiene información sobre las vulnerabilidades de la infraestructura tecnológica … y otorga herramientas a las personas para implementar un ataque informático a los activos críticos y no críticos.*	…
b) Análisis de brecha	*El análisis de brecha integra información relativa a la seguridad de la infraestructura tecnológica; enlistan los controles de seguridad con los que cuenta esta área; y menciona las herramientas que se deben adquirir para garantizar un nivel más alto de seguridad de los sistemas de información.*	…
c) Plan de Trabajo	*El plan de trabajo define los controles de seguridad a implementar de acuerdo con el resultado del análisis de riesgos y del análisis de brecha, priorizando las medidas de seguridad más relevantes con base en el riesgo real detectado. El uso de esta información permite inferir nuestros riesgos, por cuánto tiempo seguirán así hasta el momento que se implementen nuevos controles.*	…

Los fundamentos y motivos se exponen a continuación:

- *Existe un riesgo real, demostrable e identificable en perjuicio del nexo causal que prevé la hipótesis de reserva ahora analizada contemplada en los artículos 113, fracción VII, y 110, fracción VII, de las Leyes General y Federal de Transparencia y Acceso a la Información Pública, respectivamente, pues los documentos consistentes en análisis de riesgo, el análisis de brecha, las políticas de respaldo y el plan de trabajo de esta dependencia contienen información de cómo se protegen los datos personales de los titulares que nos confiaron su información personal y que es nuestra responsabilidad garantizar. Es un riesgo real el hecho de que toda persona que quiera ocasionar la pérdida, destrucción, robo, copia, uso, acceso o tratamiento no autorizado, daño, alteración o modificación no autorizada de datos personales, puede hacerlo si cuenta con la información exacta de las vulnerabilidades de un área universitaria, lo que esta serie de documentos les otorga directamente si se difundiera la información.*

- *Divulgar el análisis de riesgo, el análisis de brecha … y el plan de trabajo … evidencian los nuevos controles que estamos pendientes de implementar, describen la forma en cómo almacenamos técnicamente los datos personales, cómo protegemos los sistemas automatizados de información, qué medidas de seguridad administrativas, físicas y técnicas planemos establecer de manera gradual y de conformidad con las prioridades y presupuestos otorgado.*

- *En este sentido la revelación de la información que obra el análisis de riesgo, el análisis de brecha, las políticas de respaldo y el plan de trabajo de esta área revela y hace identificable las formas en que es posible atacar o vulnerar nuestros sistemas de información que resguardan datos personales que obran en nuestros archivos y dejaría imposibilitada a esta área para reaccionar ante posibles amenazas.*

La prueba de daño precitada, además de colmar los extremos establecidos en los numerales 97 y 111 de la Ley Federal de Transparencia y Acceso a la Información Pública, en relación con el 104 de la Ley General de Transparencia y Acceso a la Información Pública; también se realiza de conformidad con el Vigésimo Sexto de los Lineamientos Generales en materia de Clasificación y Desclasificación de la Información así como para la elaboración de versiones públicas, donde se prevé que podrá considerarse como información reservada, aquélla que obstruya la prevención de delitos al obstaculizar las acciones implementadas por las autoridades para evitar su comisión, o menoscabar o limitar la capacidad de las autoridades para evitar la comisión de delitos.

En esa inteligencia, el dar a conocer el análisis de riesgo, el análisis de brecha y el plan de trabajo de esta área universitaria, no podrían prevenirse actos ilícitos que pudieran realizarse en contra de los sistemas de información y tratamiento de datos personales, así como en contra de los activos e infraestructura crítica de esta

dependencia; por lo que es posible advertir que algunas de las posibles consecuencias de divulgar dicha información podrían derivar en la comisión de diversos delitos tipificados en el Código Penal Federal, como accesos no autorizados a los sistemas, robos de información, suplantación de identidades, entre otros. Es decir, se advierte que la negativa de acceso a la información se motiva en evitar o prevenir la comisión del delito al vulnerar las medidas de seguridad establecidas por esta Área Universitaria, con relación al cumplimiento de los principios de protección de datos personales previsto en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

En tal sentido, proteger la información de los documentos relativos al análisis de riesgo, al análisis de brecha y al plan de trabajo de esta área se adecua al principio de proporcionalidad porque se justifica negar su divulgación, toda vez que la pretensión de fondo que persigue la reserva de la información consiste en prevenir las conductas antijurídicas tipificadas, aunado a que la restricción es temporal, hasta en tanto las medidas tomadas caduquen; de igual manera, con la no divulgación de la información se contribuye a garantizar la protección de los datos personales de no solo la comunidad universitaria sino de cualquiera que ponga la confianza en esta Universidad para resguardar sus datos personales.

Por tales motivos, respetuosamente, se propone la reserva total de cada uno de esos documentos, que obran como anexos y políticas del documento de seguridad de esta área universitaria, por un periodo de 5 años, de conformidad con los artículos 32 y 36 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

En virtud de lo anterior, le solicito de la manera más atenta que ese Cuerpo Colegiado tenga a bien emitir la resolución que en derecho corresponda …" (sic).

Establecidos los antecedentes del presente asunto, este Comité procede al análisis de los argumentos referidos con antelación, al tenor de las siguientes:

C O N S I D E R A C I O N E S

PRIMERA. Con fundamento en lo dispuesto por los artículos 10 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México, así como 8, fracción VI del Reglamento de Responsabilidades Administrativas de las y los Funcionarios y Empleados de la Universidad Nacional Autónoma de México, este Órgano Colegiado rige su funcionamiento, entre otros, bajo los principios de imparcialidad, certeza, legalidad, objetividad y profesionalismo. Por ello, al ser un asunto propuesto, entre otras Áreas Universitarias, por la **Defensoría de los Derechos Universitarios, Igualdad y Atención de la Violencia de Género**, así como por la **Dirección General de Estudios de Legislación Universitaria**, dependiente de la Oficina de la Abogacía General, en este acto, la Titular de la Defensoría de los Derechos Universitarios, Igualdad y Atención de la Violencia de Género e integrante de este Cuerpo Colegiado, Guadalupe Barrena Nájera, el Abogado General y Presidente del Comité de Transparencia, Alfredo Sánchez Castañeda, así como el Director General de Asuntos Jurídicos y

Secretario Técnico de este Comité, Lic. Jorge Barrera Gutiérrez, formalmente se excusan de conocer del caso, para no afectar la imparcialidad del mismo.

SEGUNDA. De conformidad con lo dispuesto en los artículos 1, 10 y 15, fracción X del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México, el Comité de Transparencia de la Universidad Nacional Autónoma de México es competente para analizar la clasificación de reserva total de una parte de la información, para la elaboración de la versión pública de los Documentos de Seguridad, propuesta por el **Instituto de Matemáticas,** el **Instituto de Fisiología Celular,** la **Dirección General de la Escuela Nacional Colegio de Ciencias** y **Humanidades,** la **Escuela Nacional Colegio de Ciencias y Humanidades Planteles Azcapotzalco, Vallejo, Naucalpan, Oriente y Sur**, la **Facultad de Filosofía y Letras,** la **Coordinación de Difusión Cultural**, la **Dirección General de Estudios de Legislación Universitaria,** el **Centro Universitario de Teatro,** la **Dirección General de Radio UNAM,** la **Secretaría de Desarrollo Institucional,** el **Instituto de Física**, el **Consejo Académico del Área de las Ciencias Biológicas, Químicas y de la Salud,** el **Comité de Análisis para las Intervenciones Urbanas, Arquitectónicas y de las Ingenierías,** el **Museo Universitario del Chopo,** la **Dirección General de Música,** la **Dirección de Danza,** el **Centro de Investigaciones en Geografía Ambiental, Campus Morelia,** el **Museo Universitario de Arte Contemporáneo,** la **Defensoría de los Derechos Universitarios, Igualdad y Atención de la Violencia de Género,** el **Instituto de Química,** la **Dirección de Literatura y Fomento a la Lectura,** la **Dirección General de Servicios Administrativos,** la **Dirección de Teatro UNAM,** el **Centro de Ciencias Genómicas,** la **Facultad de Artes y Diseño,** la **Dirección General de Televisión Universitaria,** el **Centro Cultural Universitario Tlatelolco,** la **Dirección General de Orientación y Atención Educativa,** el **Consejo Académico del Área de las Ciencias Sociales,** la **Escuela Nacional de Estudios Superiores, Unidad Mérida,** el **Instituto de Ecología,** la **Dirección General de Cooperación e Internacionalización,** el **Instituto de Investigaciones Biomédicas,** la **Casa del Lago "Mtro. Juan José Arreola",** la **Coordinación para la Igualdad de Género,** la **Dirección General de la Escuela Nacional Preparatoria** y la **Escuela Nacional Preparatoria, Planteles 3 "Justo Sierra"** y **4 "Vidal Castañeda y Nájera"** y la **Dirección General del Deporte Universitario,** y determinar, en consecuencia, si la confirma, modifica o revoca.

TERCERA. De conformidad con lo dispuesto en los artículos 97 de la Ley Federal de Transparencia y Acceso a la Información Pública, así como 33 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México, **los titulares de las Áreas Universitarias son responsables de clasificar la información que obre en sus archivos**, debiendo comunicar al Comité mediante oficio, de forma fundada y motivada, esa clasificación.

En tal virtud, el **Instituto de Matemáticas,** el **Instituto de Fisiología Celular,** la **Dirección General de la Escuela Nacional Colegio de Ciencias** y **Humanidades,** la **Escuela Nacional Colegio de Ciencias y Humanidades Planteles Azcapotzalco, Vallejo, Naucalpan, Oriente y Sur**, la **Facultad de Filosofía y Letras,** la **Coordinación de Difusión Cultural**, la **Dirección General de Estudios de Legislación Universitaria,** el **Centro Universitario de Teatro,** la **Dirección General de Radio UNAM,** la **Secretaría de Desarrollo Institucional,** el **Instituto de**

Física, el **Consejo Académico del Área de las Ciencias Biológicas, Químicas y de la Salud,** el **Comité de Análisis para las Intervenciones Urbanas, Arquitectónicas y de las Ingenierías,** el **Museo Universitario del Chopo,** la **Dirección General de Música,** la **Dirección de Danza,** el **Centro de Investigaciones en Geografía Ambiental, Campus Morelia,** el **Museo Universitario de Arte Contemporáneo,** la **Defensoría de los Derechos Universitarios, Igualdad y Atención de la Violencia de Género,** el **Instituto de Química,** la **Dirección de Literatura y Fomento a la Lectura,** la **Dirección General de Servicios Administrativos,** la **Dirección de Teatro UNAM,** el **Centro de Ciencias Genómicas,** la **Facultad de Artes y Diseño,** la **Dirección General de Televisión Universitaria,** el **Centro Cultural Universitario Tlatelolco,** la **Dirección General de Orientación y Atención Educativa,** el **Consejo Académico del Área de las Ciencias Sociales,** la **Escuela Nacional de Estudios Superiores, Unidad Mérida,** el **Instituto de Ecología,** la **Dirección General de Cooperación e Internacionalización,** el **Instituto de Investigaciones Biomédicas,** la **Casa del Lago "Mtro. Juan José Arreola",** la **Coordinación para la Igualdad de Género,** la **Dirección General de la Escuela Nacional Preparatoria** y la **Escuela Nacional Preparatoria, Planteles 3 "Justo Sierra"** y **4 "Vidal Castañeda y Nájera"** y la **Dirección General del Deporte Universitario,** clasificaron como información reservada, por un periodo de **cinco años**, la relativa al **Análisis de Riesgo**, al **Análisis de Brecha** y al **Plan de Trabajo**, conforme a lo expuesto en el antecedente VII de la presente resolución, por actualizarse el supuesto establecido en los artículos 113, fracción VII y 110, fracción VII de las Leyes General y Federal de Transparencia y Acceso a la Información Pública, respectivamente.

Ahora bien, los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública, establecen lo siguiente:

> *"… Como información reservada podrá clasificarse aquella cuya publicación:*
>
> *[…]*
>
> ***VII.** Obstruya la prevención o persecución de los delitos;*
>
> *[…]".*

En correlación con los artículos antes mencionados, el numeral Vigésimo Sexto de los Lineamientos Generales en Materia de Clasificación y Desclasificación de la Información, así como para la Elaboración de Versiones Públicas, establece los parámetros para la procedencia de la causal de reserva prevista en el artículo 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública:

> *"**Vigésimo sexto**. De conformidad con el artículo 113, fracción VII de la Ley General, podrá considerarse como información reservada, **aquella que obstruya la prevención de delitos al obstaculizar las acciones implementadas por las autoridades para evitar su comisión, o menoscabar o limitar la capacidad de las autoridades para evitar la comisión de delitos.***

…”.

Énfasis añadido.

De lo anterior se desprende, entre otras cuestiones, que podrá clasificarse como reservada aquella información que obstruya la prevención de delitos, ya sea por obstaculizar las acciones implementadas para evitar la comisión de los mismos, o bien, por menoscabar o limitar la capacidad para evitarlos.

Al respecto, cabe tener en consideración lo establecido en el documento de trabajo del 12º Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal de la Organización de las Naciones Unidas, en el cual se define la prevención del delito de la siguiente manera: “*La prevención del delito engloba toda la labor realizada para reducir el riesgo de que se cometan delitos y sus efectos perjudiciales en las personas y la sociedad…*”.

Por otro lado, las Directrices para la prevención del delito de la Organización de las Naciones Unidas enumeran tres enfoques, a saber, la prevención social, la prevención basada en la comunidad y la prevención de situaciones propicias al delito; este último tiene por objeto reducir las oportunidades y los incentivos para delinquir, maximizar el riesgo de ser aprehendido y reducir al mínimo los beneficios del delito. En este sentido, el enfoque de prevención de situaciones está orientada en formas específicas de delincuencia.

Desde el punto de vista criminológico, prevenir es conocer con anticipación la probabilidad de una conducta criminal disponiendo de los medios necesarios para evitarla. Es decir, no permitir que alguna situación llegue a darse cuando ésta se estima inconveniente.

Ahora bien, cabe destacar que conforme a las Directrices de la Organización para la Cooperación y el Desarrollo Económico, sobre protección de la privacidad y flujos transfronterizos de datos personales, los sectores público y privado, como principio básico, deben emplear salvaguardas razonables de seguridad para proteger los datos personales contra riesgos, tales como pérdida, acceso no autorizado, destrucción, uso, modificación o divulgación de los mismos; asimismo, se establece el principio de responsabilidad que recae sobre todo controlador de datos y su deber en el cumplimiento de las medidas que hagan efectivos los principios señalados anteriormente.

Asimismo, el artículo 7 del Convenio para la Protección de las Personas con Respecto al Tratamiento Automatizado de Datos de Carácter Personal, adoptado en Estrasburgo, Francia, el 28 de enero de 1981**,** publicado mediante Decreto de fecha 28 de septiembre de 2018 en el Diario Oficial de la Federación, establece que los Estados miembros deberán tomar medidas de seguridad apropiadas para la protección de datos de carácter personal registrados en ficheros automatizados contra la destrucción accidental o no autorizada, o la pérdida accidental, así como contra el acceso, la modificación o la difusión no autorizados.

Por su parte, el artículo 30, fracción V de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, dispone como uno de los mecanismos que deberá adoptar el responsable para cumplir con el principio de responsabilidad establecido en dicha Ley General,

contar con un sistema de supervisión y vigilancia, interna y/o externa, incluidas auditorías, para comprobar el cumplimiento de las políticas de protección de datos personales.

De igual forma, de conformidad con el artículo 33, fracción VII de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, para establecer y mantener las medidas de seguridad para la protección de los datos personales, el Sujeto Obligado deberá monitorear y revisar de manera periódica las medidas de seguridad implementadas, así como las amenazas y vulneraciones a las que están sujetos los datos personales, para lo cual en términos del numeral 63 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público, el responsable deberá monitorear, entre otras cuestiones, lo siguiente:

- Las nuevas amenazas que podrían estar activas dentro y fuera de su organización y que no han sido valoradas;
- La posibilidad de que vulnerabilidades nuevas o incrementadas sean explotadas por las amenazas correspondientes;
- Las vulnerabilidades identificadas para determinar aquéllas expuestas a amenazas nuevas o pasadas que vuelvan a surgir;
- El cambio en el impacto o consecuencias de amenazas valoradas, vulnerabilidades y riesgos en conjunto, que resulten en un nivel inaceptable de riesgo, y
- Los incidentes y vulneraciones de seguridad ocurridas.

De conformidad con lo anterior, con independencia del tipo de sistema en el que se encuentren los datos personales o el tipo de tratamiento que se efectúe, para establecer y mantener las medidas de seguridad de carácter administrativo, físico y técnico para la protección de los datos personales, que permitan protegerlos contra daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado, así como garantizar su confidencialidad, integridad y disponibilidad, el responsable deberá monitorear y revisar de manera periódica dichas medidas, donde no podrá pasar inadvertidas las nuevas amenazas, las posibles vulnerabilidades, los riesgos en conjunto, los incidentes y las vulneraciones de seguridad ocurridas, entre otras.

En ese sentido, el artículo 35 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, establece que los sujetos obligados deben elaborar un documento de seguridad, entendiéndose como tal, el instrumento que describe y da cuenta de manera general sobre las medidas de seguridad técnicas, físicas y administrativas adoptadas por el responsable para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que posee.

Ahora bien, de conformidad con los artículos 33 y 35 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, en relación con los numerales 55 al 64 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público, el documento de seguridad deberá contener, cuando menos, el inventario de datos personales y de los sistemas de tratamiento; las funciones y obligaciones de las personas que traten datos personales; **el análisis de riesgos, de brecha, el plan de trabajo**, los mecanismos de monitoreo y revisión de las medidas de seguridad y el programa general de capacitación. Dicho documento deberá actualizarse cuando se produzcan modificaciones sustanciales al tratamiento de datos personales que deriven en un cambio de nivel de riesgo; como resultado de un proceso de mejora

continua, derivado del monitoreo y revisión del sistema de gestión; como resultado de un proceso de mejora para mitigar el impacto de una vulneración a la seguridad ocurrida; así como con la implementación de acciones correctivas y preventivas ante una vulneración de seguridad.

En ese sentido, el segundo párrafo del artículo 5 de las Normas Complementarias sobre Medidas de Seguridad Técnicas, Administrativas y Físicas para la Protección de Datos Personales en Posesión de la Universidad, dispone que el documento de seguridad, deberá contener las medidas de seguridad administrativa, física y técnica aplicables a los sistemas de tratamiento de datos personales del Área Universitaria, con el fin de asegurar la integridad, confidencialidad y disponibilidad de la información personal que éstos contienen.

Además de lo anterior, de conformidad con el artículo 19, fracción I, incisos b) y c) de las Normas Complementarias sobre Medidas de Seguridad Técnicas, Administrativas y Físicas para la Protección de Datos Personales en Posesión de la Universidad, durante el tratamiento automatizado de los datos personales, los sistemas de información deberán establecer las medidas de seguridad en los periodos de inactividad o mantenimiento, así como generar respaldos y aplicar los mecanismos de control y protección para su resguardo.

En este sentido, de difundirse la información contenida en los apartados relativos al **Análisis de Riesgos, al Análisis de Brecha**, al **Plan de Trabajo**, así como a **toda aquella información que se encuentre directamente relacionada con alguno de dichos apartados** o que **revele vulnerabilidades en la protección de los datos personales en poder de las Áreas Universitarias,** se haría del conocimiento público la falta o debilidad de seguridad en un activo o grupo de activos, físicos o electrónicos, que puede ser explotada por una o más amenazas, lo que conllevaría a la materialización de las mismas y ocasionar la pérdida, destrucción no autorizada o incluso la sustracción de los datos personales en posesión de la Universidad, así como el robo, extravío o copia no autorizada de los mismos, su uso, acceso o tratamiento no autorizado, además del daño, alteración o modificación no autorizada, incluso impidiendo su recuperación, vulnerando así la seguridad de los datos personales.

Bajo estos argumentos se advierte que la clasificación de la información contenida en el **Análisis de Riesgos,** en el **Análisis de Brecha**, en **Plan de Trabajo**, así como **toda aquella información que se encuentre directamente relacionada con alguno de dichos apartados** o que **revele vulnerabilidades en la protección de los datos personales en poder de las Áreas Universitarias**, tiene como propósito evitar o prevenir la comisión de conductas ilícitas, tales como el acceso ilícito a equipos y sistema de informática, la cual se encuentra prevista en el Título Noveno, Revelación de Secretos y Acceso Ilícito a sistemas y equipos de informática, Capítulo II, Acceso Ilícito a sistemas y equipos de informática, del Código Penal Federal en el cual se dispone lo siguiente:

> *"Artículo 211 bis 1.- Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.*

> *Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a un año de prisión y de cincuenta a ciento cincuenta días multa".*
>
> *"Artículo 211 bis 2.- Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de uno a cuatro años de prisión y de doscientos a seiscientos días multa.*
>
> *Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.*
>
> *…".*

De la normativa señalada se advierte que comete el **delito de acceso ilícito a sistemas y equipos de informática** todo aquel que **sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad**, **sean o no propiedad del Estado**, o bien, conozca o copie dicha información; conductas que de igual manera se pueden materializar en los archivos físicos, ya que es factible **sustraer, ocultar, alterar, mutilar, destruir o inutilizar, total o parcialmente, los datos personales contenidos en los documentos bajo custodia de las Áreas Universitarias**, por lo que la misma protección deberá otorgarse a los sistemas electrónicos, así como a los archivos físicos con los que se cuenta.

Por lo que de darse a conocer la información relativa al **Análisis de Riesgos,** al **Análisis de Brecha**, al **Plan de Trabajo**¸ así como a **toda aquella información que se encuentre directamente relacionada con alguno de dichos apartados** o **revele vulnerabilidades en la protección de los datos personales en poder de las Áreas Universitarias,** la cual se encuentra contenida en los documentos de seguridad remitidos por las Áreas Universitarias, se darían a conocer las acciones implementadas o por implementar, de acuerdo con el análisis de riesgos y de brecha, priorizando las medidas de seguridad más relevantes e inmediatas a establecer, así como las amenazas y vulnerabilidades existentes para los datos personales y los recursos involucrados en su tratamiento, como pueden ser: hardware, software, personal del responsable, manejo de documentos físicos y/o electrónicos, entre otros, lo que representa para las Áreas Universitarias un riesgo evidente para la estabilidad de la ejecución de las medidas de seguridad adoptadas para resguardar los datos en su poder, en tanto la publicación de esa información revelaría elementos que de manera concatenada con otra información que pudiera generarse o que se haya generado, evidenciaría vulnerabilidades que pudieran ser aprovechadas por personas dedicadas a la comisión de conductas ilícitas y con ello poner en riesgo la seguridad de los datos personales tratados en el desempeño y/o ejercicio de sus competencias, facultades y/o funciones.

De esta forma, se colige que con la publicidad de la información referida, se generaría un riesgo potencial tanto para la documentación física como para la infraestructura tecnológica de las Áreas Universitarias, ya que la información relativa a las medidas físicas, administrativas y técnicas puede ser utilizada para propiciar, entre otros, actos vandálicos, o bien, ataques informáticos de diversa índole, al hacerse identificables las vulnerabilidades que pueden ser explotadas y causar un daño a los documentos físicos y/o electrónicos que obran en los archivos, así como a la infraestructura informática, programas y desarrollos tecnológicos de las Áreas Universitarias, lo que limitaría severamente su capacidad para prevenir conductas ilícitas, tales como las relacionadas en párrafos anteriores.

Por lo anterior, se concluye que la información solicitada actualiza la causal de reserva prevista en los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública, así como en el numeral Vigésimo Sexto de los Lineamientos Generales en Materia de Clasificación y Desclasificación de la Información, así como para la Elaboración de Versiones Públicas.

Así, en términos del artículo 104 de la Ley General de Transparencia y Acceso a la Información Pública, se analiza la siguiente prueba de daño:

> *"Artículo 104. En la aplicación de la prueba de daño, el sujeto obligado deberá justificar que:*
>
> *I. La divulgación de la información representa un riesgo real, demostrable e identificable de perjuicio significativo al interés público o a la seguridad nacional;*
> *II. El riesgo de perjuicio que supondría la divulgación supera el interés público general de que se difunda, y*
> *III. La limitación se adecua al principio de proporcionalidad y representa el medio menos restrictivo disponible para evitar el perjuicio".*

I. La divulgación de la información representa un riesgo real, demostrable e identificable de perjuicio significativo al interés público.

De difundirse el plan de trabajo, el análisis de riesgos y el análisis de brecha del documento de seguridad, se afectarían las medidas y acciones implementadas por las Áreas Universitarias para reducir el riesgo de que se cometa una conducta o un comportamiento que pueda dañar o convertir a esta Universidad y su comunidad en sujetos o víctimas de conductas ilícitas.

Lo anterior, toda vez que la publicidad de la información contenida en el **análisis de riesgos, de brecha** y el **plan de trabajo,** así como **toda aquella información que se encuentre directamente relacionada con alguno de dichos apartados** o **revele vulnerabilidades en la protección de los datos personales en poder de las Áreas Universitarias**, representa un riesgo potencial para las Áreas Universitarias, pues a través

de dicha información se podrían identificar vulnerabilidades que pueden ser aprovechadas para realizar conductas contrarias a derecho, tales como actos vandálicos, o bien, ataques informáticos de diversa índole, disminuyendo la capacidad de las Áreas Universitarias para responder ante posibles amenazas.

En ese sentido la divulgación de la información representa un riesgo real, demostrable e identificable de perjuicio significativo al interés público.

II. El riesgo de perjuicio que supondría la divulgación supera el interés público general de que se difunda.

El perjuicio que en su caso ocasionaría al interés público la divulgación de la información en cuestión, supera al perjuicio que se ocasionaría al no publicarla, pues con la difusión de la información contenida en el **análisis de riesgos, de brecha y el plan de trabajo,** así como **toda aquella información que se encuentre directamente relacionada con alguno de dichos apartados** o **revele vulnerabilidades en la protección de los datos personales en poder de las Áreas Universitarias**, se limitaría la capacidad de las Áreas Universitarias para prevenir la comisión de conductas ilícitas.

De ahí resulta evidente que el riesgo de perjuicio que supondría la divulgación de la información solicitada, supera el interés público general de que se difunda.

III. La limitación se adecua al principio de proporcionalidad y representa el medio menos restrictivo disponible para evitar el perjuicio.

Se considera que la limitación de acceso a la información solicitada se ajusta al principio de proporcionalidad, toda vez que se justifica negar su acceso, a cambio de garantizar la capacidad de las Áreas Universitarias para implementar todas aquellas medidas y acciones tendientes a reducir el riesgo de que se cometa una conducta ilícita que pudiera vulnerar los datos personales cuyo tratamiento realizan las Áreas Universitarias, en el desempeño y/o ejercicio de sus competencias, facultades o funciones.

En ese sentido, se considera que la limitación representa el medio menos restrictivo disponible para evitar el perjuicio ya que únicamente se restringirá el acceso a la información por un periodo de **cinco años**, el cual se computará a partir de la fecha en que se emite la presente resolución y hasta la fecha de término del periodo, o bien, se interrumpirá antes si desaparecen las causas que originaron la reserva de la información, lo que suceda primero. De tal forma que no se afecte la capacidad de este sujeto obligado para prevenir la comisión de conductas ilícitas, pero tampoco se prive de manera trascendente el acceso a la información, en su momento, ya que éste no se verá restringido por un periodo mayor al previsto por la norma.

Por lo antes mencionado, se colman las hipótesis de las fracciones I, II y III, dispuestas en el artículo 104 de la Ley General de Transparencia y Acceso a la Información Pública, por lo que es procedente **CONFIRMAR** la reserva total de una parte de la información para la elaboración de la

versión pública propuesta por el **Instituto de Matemáticas,** el **Instituto de Fisiología Celular,** la **Dirección General de la Escuela Nacional Colegio de Ciencias** y **Humanidades,** la **Escuela Nacional Colegio de Ciencias y Humanidades Planteles Azcapotzalco, Vallejo, Naucalpan, Oriente y Sur**, la **Facultad de Filosofía y Letras,** la **Coordinación de Difusión Cultural**, la **Dirección General de Estudios de Legislación Universitaria,** el **Centro Universitario de Teatro,** la **Dirección General de Radio UNAM,** la **Secretaría de Desarrollo Institucional,** el **Instituto de Física**, el **Consejo Académico del Área de las Ciencias Biológicas, Químicas y de la Salud,** el **Comité de Análisis para las Intervenciones Urbanas, Arquitectónicas y de las Ingenierías,** el **Museo Universitario del Chopo,** la **Dirección General de Música,** la **Dirección de Danza,** el **Centro de Investigaciones en Geografía Ambiental, Campus Morelia,** el **Museo Universitario de Arte Contemporáneo,** la **Defensoría de los Derechos Universitarios, Igualdad y Atención de la Violencia de Género,** el **Instituto de Química,** la **Dirección de Literatura y Fomento a la Lectura,** la **Dirección General de Servicios Administrativos,** la **Dirección de Teatro UNAM,** el **Centro de Ciencias Genómicas,** la **Facultad de Artes y Diseño,** la **Dirección General de Televisión Universitaria,** el **Centro Cultural Universitario Tlatelolco,** la **Dirección General de Orientación y Atención Educativa,** el **Consejo Académico del Área de las Ciencias Sociales,** la **Escuela Nacional de Estudios Superiores, Unidad Mérida,** el **Instituto de Ecología,** la **Dirección General de Cooperación e Internacionalización,** el **Instituto de Investigaciones Biomédicas,** la **Casa del Lago "Mtro. Juan José Arreola",** la **Coordinación para la Igualdad de Género,** la **Dirección General de la Escuela Nacional Preparatoria** y la **Escuela Nacional Preparatoria, Planteles 3 "Justo Sierra"** y **4 "Vidal Castañeda y Nájera"** y la **Dirección General del Deporte Universitario,** por un periodo de **cinco años**, que se computarán a partir de la fecha de la presente resolución, de conformidad con lo establecido en los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.

CUARTA. Este Comité considera pertinente orientar a las Áreas Universitarias, a efecto de que en la elaboración de la versión pública de sus respectivos documentos de seguridad, tengan en cuenta lo siguiente:

- Deberán testar las secciones o información correspondientes al "Análisis de Riesgo", al "Análisis de Brecha", al "Plan de Trabajo", así como toda aquella información que se encuentre directamente relacionada con alguno de dichos apartados o revele vulnerabilidades en la protección de los datos personales en su poder; para lo cual deberán emplear un medio que no permita la visualización de la misma y que no impida la lectura de aquella información que no es considerada como reservada. Al respecto, es importante precisar que **no deberán suprimirse las secciones** donde se contenga la información objeto de reserva.

- Deberán insertar un cuadro de texto en el cual se indiquen:

  - Las partes o secciones reservadas.

- El fundamento legal que sustenta la reserva, así como el plazo de ésta, mismos que se encuentran indicados en el último párrafo de la consideración **TERCERA** de la presente resolución.

Lo anterior, de conformidad con lo dispuesto en los numerales Quincuagésimo Noveno, Sexagésimo y Sexagésimo Primero de los Lineamientos Generales en Materia de Clasificación y Desclasificación de la Información, así como para la Elaboración de Versiones Públicas.

Por lo expuesto, y con fundamento en lo dispuesto por los artículos 6, apartado A de la Constitución Política de los Estados Unidos Mexicanos; 1, 6, 7, 8, 23, 44, fracción II, 113, fracción VII, 137 inciso a) de la Ley General de Transparencia y Acceso a la Información Pública; 65, fracción II, 110, fracción VII, y 140, fracción I de la Ley Federal de Transparencia y Acceso a la Información Pública; 1, 15, fracción X, 38, último párrafo del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México, este Comité de Transparencia:

R E S U E L V E

PRIMERO. Con fundamento en lo dispuesto en los artículos 1, 10, 11, 15 fracción X y 31, fracción I del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México, 137, inciso a) de la Ley General de Transparencia y Acceso a la Información Pública y 140, fracción I de la Ley Federal de Transparencia y Acceso a la Información Pública, este Comité de Transparencia **CONFIRMA** la **CLASIFICACIÓN** de **RESERVA** total de una parte la información para la elaboración de la versión pública de los Documentos de Seguridad, propuesta por el **Instituto de Matemáticas,** el **Instituto de Fisiología Celular,** la **Dirección General de la Escuela Nacional Colegio de Ciencias** y **Humanidades,** la **Escuela Nacional Colegio de Ciencias y Humanidades Planteles Azcapotzalco, Vallejo, Naucalpan, Oriente y Sur**, la **Facultad de Filosofía y Letras,** la **Coordinación de Difusión Cultural**, la **Dirección General de Estudios de Legislación Universitaria,** el **Centro Universitario de Teatro,** la **Dirección General de Radio UNAM,** la **Secretaría de Desarrollo Institucional,** el **Instituto de Física**, el **Consejo Académico del Área de las Ciencias Biológicas, Químicas y de la Salud,** el **Comité de Análisis para las Intervenciones Urbanas, Arquitectónicas y de las Ingenierías,** el **Museo Universitario del Chopo,** la **Dirección General de Música,** la **Dirección de Danza,** el **Centro de Investigaciones en Geografía Ambiental, Campus Morelia,** el **Museo Universitario de Arte Contemporáneo,** la **Defensoría de los Derechos Universitarios, Igualdad y Atención de la Violencia de Género,** el **Instituto de Química,** la **Dirección de Literatura y Fomento a la Lectura,** la **Dirección General de Servicios Administrativos,** la **Dirección de Teatro UNAM,** el **Centro de Ciencias Genómicas,** la **Facultad de Artes y Diseño,** la **Dirección General de Televisión Universitaria,** el **Centro Cultural Universitario Tlatelolco,** la **Dirección General de Orientación y Atención Educativa,** el **Consejo Académico del Área de las Ciencias Sociales,** la **Escuela Nacional de Estudios Superiores, Unidad Mérida,** el **Instituto de Ecología,** la **Dirección General de Cooperación e Internacionalización,** el **Instituto de Investigaciones Biomédicas,** la **Casa del Lago "Mtro. Juan José Arreola",** la **Coordinación para la Igualdad de Género,** la **Dirección General de la**

Escuela Nacional Preparatoria y la **Escuela Nacional Preparatoria, Planteles 3 "Justo Sierra"** y **4 "Vidal Castañeda y Nájera"** y la **Dirección General del Deporte Universitario,** en relación con el **Análisis de Riesgos**, el **Análisis de Brecha** y el **Plan de Trabajo**, así como **toda aquella información que se encuentre directamente relacionada con alguno de dichos apartados** o **revele vulnerabilidades en la protección de los datos personales en poder de las Áreas Universitarias**, por un periodo de **cinco años**, contados a partir de la fecha de la presente resolución, o bien, hasta en tanto se extingan las causas que dieron origen a la reserva de la información.

Lo anterior, en términos de la consideración **TERCERA** de la presente resolución.

SEGUNDO. Se instruye a las Áreas Universitarias a efecto de que elaboren la versión pública en términos de lo dispuesto en la consideración **CUARTA.**

TERCERO. Con fundamento en los artículos 45, fracción V y 137, último párrafo de la Ley General de Transparencia y Acceso a la Información Pública: así como 53, fracción VI, inciso c) del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México, notifíquese la presente resolución por correo institucional al **Instituto de Matemáticas,** al **Instituto de Fisiología Celular,** a la **Dirección General de la Escuela Nacional Colegio de Ciencias** y **Humanidades,** a la **Escuela Nacional Colegio de Ciencias y Humanidades Planteles Azcapotzalco, Vallejo, Naucalpan, Oriente y Sur**, a la **Facultad de Filosofía y Letras,** a la **Coordinación de Difusión Cultural**, a la **Dirección General de Estudios de Legislación Universitaria,** al **Centro Universitario de Teatro,** a la **Dirección General de Radio UNAM**, a la **Secretaría de Desarrollo Institucional,** al **Instituto de Física**, al **Consejo Académico del Área de las Ciencias Biológicas, Químicas y de la Salud,** al **Comité de Análisis para las Intervenciones Urbanas, Arquitectónicas y de las Ingenierías,** al **Museo Universitario del Chopo,** a la **Dirección General de Música,** a la **Dirección de Danza,** al **Centro de Investigaciones en Geografía Ambiental, Campus Morelia,** al **Museo Universitario de Arte Contemporáneo,** a la **Defensoría de los Derechos Universitarios, Igualdad y Atención de la Violencia de Género,** al **Instituto de Química,** a la **Dirección de Literatura y Fomento a la Lectura,** a la **Dirección General de Servicios Administrativos,** a la **Dirección de Teatro UNAM,** al **Centro de Ciencias Genómicas,** a la **Facultad de Artes y Diseño,** a la **Dirección General de Televisión Universitaria,** al **Centro Cultural Universitario Tlatelolco,** a la **Dirección General de Orientación y Atención Educativa,** al **Consejo Académico del Área de las Ciencias Sociales,** la **Escuela Nacional de Estudios Superiores, Unidad Mérida,** al **Instituto de Ecología,** a la **Dirección General de Cooperación e Internacionalización,** al **Instituto de Investigaciones Biomédicas,** a la **Casa del Lago "Mtro. Juan José Arreola",** a la **Coordinación para la Igualdad de Género,** a la **Dirección General de la Escuela Nacional Preparatoria** y a la **Escuela Nacional Preparatoria, Planteles 3 "Justo Sierra"** y **4 "Vidal Castañeda y Nájera",** a la **Dirección General del Deporte Universitario,** así como a la Unidad de Transparencia de esta Universidad, para los efectos procedentes.

Así lo resolvió por unanimidad de votos de sus integrantes, el Comité de Transparencia de la Universidad Nacional Autónoma de México, en términos de los artículos 1, 11, 15, 20 y 53,

fracción VI del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

POR MI RAZA HABLARÁ EL ESPÍRITU"
Ciudad Universitaria, Cd. Mx., 19 de agosto de 2022

Archivo	08-ctunam-525-2022-docto-seg-1.pdf		
Identificador único (hash)	5c7a552404c38ce4b052cc8e212d4579a13448672db8ce248b096c2e568ad6cf		
Fecha y hora de cierre	19/08/2022 16:28:33	**Fecha y hora de emisión**	19/08/2022 16:30:53
Número de páginas	19	**Firmantes**	4

Firmantes

Nombre	Lic. MARIA ELENA GARCIA MELENDEZ	**Fecha y hora de firma**	19/08/2022 15:18:41
Directora General para la Prevención y Mejora de la Gestión Institucional y Suplente del Contralor			
Hash Firma	cbaca6eb689a47d8770065a6f6ff297b80269e390ef3f832d480a433bf1abbfbf4ed2ced4f3f344361b247c806f9e1e2		

Nombre	Ing. Ricardo Ramírez Ortiz	**Fecha y hora de firma**	19/08/2022 15:41:03
Director General de Servicios Generales y Movilidad			
Hash Firma	1ad0c05aa515c5cfb0a9def95dd4b62ff2c74d8447fbdc4130479cece21b04b4035d4865b90866689b75f86c70c2ce60		

Nombre	JOSE MELJEM MOCTEZUMA	**Fecha y hora de firma**	19/08/2022 16:28:33
Titular de la Unidad de Transparencia			
Hash Firma	8d01b7ff1fe5c4c30fcea6d96019f992ef58adde4f23ce469572c785c60d3e1d5d9bbef4bfee618dddfc45f27edac3db		

Nombre	Dra. Jacqueline Peschard Mariscal	**Fecha y hora de firma**	19/08/2022 16:19:26
Especialista			
Hash Firma	460b366695dd8e79de4878edcf8017579ce607f70964c5cabc1bcba1cdfd08f60261a88559c3ef1d8ea03ae660538626		

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	