Universidad Nacional Autónoma de México

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

ÍNDICE DE ANEXOS

Anexo I: Documento de Seguridad de Datos Personales:

Anexo II: Formato universitario de *"Solicitud de ejercicio de Derechos ARCO"*

Anexo III: Carta de confidencialidad

Anexo IV: Ruta crítica para el cumplimiento de las Medidas de Seguridad Técnicas (MST)

Anexo V: Formatos para el cumplimiento de las Medidas de Seguridad Técnicas (MST)

ANEXO I: DOCUMENTO DE SEGURIDAD DE DATOS PERSONALES

ÍNDICE

Introducción

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

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

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

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

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

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

1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

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

(Denominación del área específica del Área Universitaria A)	
Identificador único*	DGPU01 (Dirección General del Patrimonio Universitario)
(Nombre del sistema A1) *	**Sistema de Control de Gestión**
Datos personales (sensibles o no) contenidos en el sistema*:	1. Datos personales en general: Nombre Completo Domicilio 2. Datos personales sensibles: NO
Responsable*:	
Nombre*:	**Mtra. Adriana Zamora Mariaca**
Cargo*:	**Coordinadora de Gestión**
Funciones*:	Estar a cargo del tratamiento automatizado de los datos personales, así como su destino y resguardo al interior de la DGPU.
Obligaciones*:	Supervisar el envío de la información a las diferentes áreas de la DGPU. Supervisar la incorporación de nuevas funcionalidades en el Sistema.
	Encargados[1]:
(Nombre del Encargado 1*)	**Oscar Blanco Badillo**
Cargo*:	**Jefe del Departamento de Sistemas de la DGPU**
Funciones*:	Administrador del Sistema de Control de Gestión
Obligaciones*:	Respaldo de información Propuesta de incorporación de nuevas funcionalidades Vigilar que el sistema cumpla con las medidas de seguridad técnica Capacitación técnica a los usuarios
(Nombre del Encargado 2*)	
Cargo*:	
Funciones*:	
Obligaciones*:	
	Usuarios:
(Nombre del Usuario 1*)	Yanet Mendoza Hernández
Cargo*:	Coordinadora
Funciones*:	Operar el control de gestión Recepción de documentación Registro de información Turno de documentación mediante el control de gestión
Obligaciones*:	Cumplir con la obligación legal de resguardo de datos

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

	personales Administrar la información contenida en el sistema Resguardar la confidencialidad de los datos personales Prever el posible acceso no autorizado al sistema y al archivo físico
(Nombre del Usuario 2*)	Armando Haro Estrop
Cargo*:	Director de Área
Funciones*:	Operar el control de gestión Recepción de documentación Registro de información Turno de documentación mediante el control de gestión
Obligaciones*:	Cumplir con la obligación legal de resguardo de datos personales Administrar la información contenida en el sistema Resguardar la confidencialidad de los datos personales Prever el posible acceso no autorizado al sistema y al archivo físico
(Nombre del Usuario 3*)	Alejandro Fargas Campos
Cargo*:	Director de Área
Funciones*:	Operar el control de gestión Recepción de documentación Registro de información Turno de documentación mediante el control de gestión
Obligaciones*:	Cumplir con la obligación legal de resguardo de datos personales Administrar la información contenida en el sistema Resguardar la confidencialidad de los datos personales Prever el posible acceso no autorizado al sistema y al archivo físico
(Nombre del Usuario 4*)	Enrique Donnadieu Farrett
Cargo*:	Director de Área
Funciones*:	Operar el control de gestión Recepción de documentación Registro de información Turno de documentación mediante el control de gestión
Obligaciones*:	Cumplir con la obligación legal de resguardo de datos personales Administrar la información contenida en el sistema Resguardar la confidencialidad de los datos personales Prever el posible acceso no autorizado al sistema y al archivo físico
(Nombre del Usuario 5*)	Olivia Sánchez Valencia
Cargo*:	Jefe de Departamento
Funciones*:	Operar el control de gestión Recepción de documentación Registro de información Turno de documentación mediante el control de gestión
Obligaciones*:	Cumplir con la obligación legal de resguardo de datos personales Administrar la información contenida en el sistema Resguardar la confidencialidad de los datos personales Prever el posible acceso no autorizado al sistema y al

	archivo físico
(Nombre del Usuario 6*)	Sonia Hernández Ramírez
Cargo*:	Jefe de Departamento
Funciones*:	Operar el control de gestión Recepción de documentación Registro de información Turno de documentación mediante el control de gestión
Obligaciones*:	Cumplir con la obligación legal de resguardo de datos personales Administrar la información contenida en el sistema Resguardar la confidencialidad de los datos personales Prever el posible acceso no autorizado al sistema y al archivo físico
(Nombre del Usuario 7*)	Victoria Martínez Gutierrez
Cargo*:	Jefe de Departamento
Funciones*:	Operar el control de gestión Recepción de documentación Registro de información Turno de documentación mediante el control de gestión
Obligaciones*:	Cumplir con la obligación legal de resguardo de datos personales Administrar la información contenida en el sistema Resguardar la confidencialidad de los datos personales Prever el posible acceso no autorizado al sistema y al archivo físico
(Nombre del Usuario 8*)	María Inés González González
Cargo*:	Jefe de Departamento
Funciones*:	Operar el control de gestión Recepción de documentación Registro de información Turno de documentación mediante el control de gestión
Obligaciones*:	Cumplir con la obligación legal de resguardo de datos personales Administrar la información contenida en el sistema Resguardar la confidencialidad de los datos personales Prever el posible acceso no autorizado al sistema y al archivo físico
(Nombre del Usuario 9*)	Edgar Cruz García
Cargo*:	Jefe de Departamento
Funciones*:	Operar el control de gestión Recepción de documentación Registro de información Turno de documentación mediante el control de gestión
Obligaciones*:	Cumplir con la obligación legal de resguardo de datos personales Administrar la información contenida en el sistema Resguardar la confidencialidad de los datos personales Prever el posible acceso no autorizado al sistema y al archivo físico
(Nombre del Usuario 10*)	Javier Moreno Zurita

Cargo*:	Jefe de Departamento
Funciones*:	Operar el control de gestión Recepción de documentación Registro de información Turno de documentación mediante el control de gestión
Obligaciones*:	Cumplir con la obligación legal de resguardo de datos personales Administrar la información contenida en el sistema Resguardar la confidencialidad de los datos personales Prever el posible acceso no autorizado al sistema y al archivo físico
(Nombre del Usuario 11*)	Carlos Castro Rosendi
Cargo*:	Jefe de Departamento
Funciones*:	Operar el control de gestión Recepción de documentación Registro de información Turno de documentación mediante el control de gestión
Obligaciones*:	Cumplir con la obligación legal de resguardo de datos personales Administrar la información contenida en el sistema Resguardar la confidencialidad de los datos personales Prever el posible acceso no autorizado al sistema y al archivo físico

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

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

(Denominación del área específica del Área Universitaria A)*	
Identificador único¨*	DGPU01 (Dirección General del Patrimonio Universitario)
(Nombre del sistema A1*)	Sistema de Control de Gestión
Tipo de soporte[2]:*	Electrónico y físico
Descripción[3]:*	Se almacena como archivo pdf en el sistema
Características del lugar donde se resguardan los soportes[4]:*	Alojamiento en un servidor de la DGPU, y lo físico en el archivo de la oficina de la Dirección General.
Descripción*:	Expedientes

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

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

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

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

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

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

3. ANÁLISIS DE RIESGOS

De conformidad a los numerales Quincuagésimo Primero, Quincuagésimo Segundo, Quincuagésimo Sexto, Quincuagésimo Octavo y Sexagésimo de los Lineamientos Generales en Materia de Clasificación y Desclasificación de la Información, así como para la Elaboración de Versiones Públicas	Fecha de clasificación:	En Sesión Ordinaria del 19 de agosto de 2022, el Comité de Transparencia de la UNAM confirmó la reserva parcial de la información mediante resolución CTUNAM/____/2022
	Área:	Dirección General para la Prevención y Mejora de la Gestión Institucional.
	Información reservada:	En su totalidad, el apartado identificado como "*5. PLAN DE TRABAJO.*", contenido en las páginas 18 a 20.
	Periodo de reserva:	5 años.
	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 relación con 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.

(Denominación del área específica del Área Universitaria A)*		
Identificador único*	DGPU01 (Dirección General del Patrimonio Universitario)	
(Nombre del sistema A1) *	*Sistema de Control de Gestión*	
Riesgo*	**Impacto***	**Mitigación***
[redacted]	[redacted]	[redacted]

4. ANÁLISIS DE BRECHA

De conformidad a los numerales Quincuagésimo Primero, Quincuagésimo Segundo, Quincuagésimo Sexto, Quincuagésimo Octavo y Sexagésimo de los Lineamientos Generales en Materia de Clasificación y Desclasificación de la Información, así como para la Elaboración de Versiones Públicas	Fecha de clasificación:	En Sesión Ordinaria del 19 de agosto de 2022, el Comité de Transparencia de la UNAM confirmó la reserva parcial de la información mediante resolución CTUNAM/____/2022
	Área:	Dirección General para la Prevención y Mejora de la Gestión Institucional.
	Información reservada:	En su totalidad, el apartado identificado como "*5. PLAN DE TRABAJO.*", contenido en las páginas 18 a 20.
	Periodo de reserva:	5 años.
	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 relación con 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.

(Denominación del área específica del Área Universitaria A)*		
Identificador único*	DGPU01 (Dirección General del Patrimonio Universitario)	
(Nombre del sistema A1) *	*Sistema de Control de Gestión*	
Medida de seguridad actual*	**Medida de seguridad necesaria***	**Acciones para remediación***
[redacted]	[redacted]	[redacted]

5. PLAN DE TRABAJO

De conformidad a los numerales Quincuagésimo Primero, Quincuagésimo Segundo, Quincuagésimo Sexto, Quincuagésimo Octavo y Sexagésimo de los Lineamientos Generales en Materia de Clasificación y Desclasificación de la Información, así como para la Elaboración de Versiones Públicas	Fecha de clasificación:	En Sesión Ordinaria del 19 de agosto de 2022, el Comité de Transparencia de la UNAM confirmó la reserva parcial de la información mediante resolución CTUNAM/_____/2022
	Área:	Dirección General para la Prevención y Mejora de la Gestión Institucional.
	Información reservada:	En su totalidad, el apartado identificado como "*5. PLAN DE TRABAJO.*", contenido en las páginas 18 a 20.
	Periodo de reserva:	5 años.
	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 relación con 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.

(Denominación del área específica del Área Universitaria A)*			
Identificador único*	DGPU01 (Dirección General del Patrimonio Universitario)		
(Nombre del sistema A1) *	*Sistema de Control de Gestión*		
Actividad*	**Descripción***	**Duración***	**Cobertura***
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]

6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

I. TRANSFERENCIAS DE DATOS PERSONALES

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

(Denominación del área específica del Área Universitaria A)*	
Identificador único*	DGPU01 (Dirección General del Patrimonio Universitario)
(Nombre del sistema A1)*	*Sistema de Control de Gestión*
TRANSFERENCIAS DE DATOS PERSONALES	

Transferencias mediante el traslado de soportes físicos:[5]	No se realizan transferencia de datos personales mediante el traslado de soportes físicos.
Transferencias mediante el traslado de soportes electrónicos:	No se realizan transferencia de datos personales mediante el traslado de soportes electrónicos.
Transferencias mediante el traslado sobre redes electrónicas:	No se realizan transferencia de datos personales mediante el traslado sobre redes electrónicas.

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

1. Señalar las medidas de seguridad que ha implementado el área universitaria para el resguardo de los soportes físicos del sistema de manera que evite la alteración, pérdida o acceso no autorizado a los mismos.[6]
Bajo llave con acceso restringido.
2. Señalar en un listado las personas (nombre, cargo, funciones y obligaciones) que tienen acceso a los soportes físicos del sistema.[7]
Yanet Mendoza Hernández
Adriana Zamora Mariaca
Cynthia Abigail Beristain Contreras
Marcela Coria Céspedes

II. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

1. Los datos que se registran en las bitácoras:[8]

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

[6] Por ejemplo, se espera que precise si los formatos impresos, documentos, listados o expedientes están foliados, cosidos o engargolados, si los muebles o la estantería donde residen cuentan con cerradura, si existen mecanismos para regular la temperatura y la humedad, si existen sistemas de tratamiento de datos personales de detección y/o supresión de incendios, si cuenta con mecanismos para regular y mantener el suministro continuo de energía eléctrica, entre otras posibles medidas.

[7] En caso de ser muchas personas, se sugiere agregar el listado como Anexo al Documento de seguridad.

[8] Las áreas de informática y seguridad de la información han designado una persona que se encarga de realizar un análisis de las bitácoras generadas. Las siguientes características aplican al caso:

No se llevan a cabo bitácoras

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

2. Si las bitácoras están en soporte físico o en soporte electrónico;[9]
3. Lugar dónde almacena las bitácoras y por cuánto tiempo;
4. La manera en que asegura la integridad de las bitácoras, y

---

a) Se cuenta con la ayuda de una herramienta informática adquirida para tal propósito.
b) Cada semana se llevan a cabo análisis de bitácoras, pero no de todas ellas. Depende de la bitácora y de las amenazas detectadas en el entorno.

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

a) Las autorizaciones emitidas para facultar el acceso a un funcionario universitario a fin de que éste, en el ejercicio de sus funciones, pueda interactuar con uno o más de los sistemas de tratamiento de datos personales a su cargo.
b) La asignación, actualización y reemplazo de las llaves que entrega a los autorizados para que éstos puedan abrir el mecanismo de apertura de la puerta en la zona de acceso restringido. Las acciones que los autorizados llevan a cabo en el área de resguardo. Para ello, designa a un Encargado quien anota lo siguiente: Quién solicita el acceso, cuándo se lleva a cabo (fecha y hora de entrada y salida), la razón que lo motiva y número del expediente utilizado.
c) El préstamo de expedientes es asistido por un sistema de tratamiento de datos personales de cómputo que utiliza códigos de barras en los gafetes del personal autorizado y en los expedientes.
d) El sistema de tratamiento de datos personales de préstamo de expedientes genera una bitácora electrónica que se respalda diariamente en un servidor dentro del centro de cómputo que administra el área de informática. Su integridad se garantiza copiando dicha bitácora en un CD-R diariamente.
e) El Encargado del sistema de tratamiento de datos personales es la persona designada para analizar la bitácora cada mes mediante una herramienta adquirida para tal fin.

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

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

a) Las bitácoras de eventos ocurridos a nivel *sistema de tratamiento de datos personales operativo* en los equipos (servidores, cortafuegos, almacenamiento masivo) que habilitan la operación del sistema de tratamiento de datos personales. Entre otras, se generan bitácoras para desempeño del servidor: intentos de acceso (exitosos y fallidos); accesos denegados a usuarios y terminales; uso de herramientas para administración del servidor, y fecha y hora de los eventos anteriores.
b) Las bitácoras de eventos generados a nivel *software aplicativo* del sistema de tratamiento de datos personales. Entre otras, se generan bitácoras para mensajes de error; apertura, modificación y cierre de archivos; violaciones de seguridad detectadas por el software aplicativo, y fecha y hora de estos eventos.
c) Las bitácoras de eventos relativos a las actividades de usuarios (capturistas, Encargados, el propio responsable y el administrador del servidor) en su interacción con el sistema de tratamiento de datos personales. Entre otras, se generan bitácoras para: archivos servicios y recursos utilizados; intentos de acceso (exitosos y fallidos); comandos y operaciones iniciadas, y fecha y hora de dichos eventos.
d) El conjunto de bitácoras permite registrar, entre otros, los siguientes datos: Quién accede a los datos personales, desde dónde y con qué; accesos (intentos exitosos y fallidos) y salidas; propósito del acceso (sólo para modificaciones en el software aplicativo); operaciones llevadas a cabo; datos personales (registros y campos) utilizados de la base de datos, y fecha y hora de estos eventos.
e) Las bitácoras arriba mencionadas están todas en soportes electrónicos y se almacenan al menos por dos años en CD-R. Se tiene una copia en el centro de datos y otra se lleva a una bóveda bancaria subcontratada también para los respaldos.

II. La integridad de las bitácoras se garantiza copiándolas en un servidor del centro de datos el cual las graba en CD-R. Algunas se copian cada hora, otras a diario. La integridad de las copias se garantiza además con "resúmenes" creados por un algoritmo "digestor". Se cuenta con una herramienta de software que automatiza estas operaciones.
III. Se pueden realizar análisis focalizados a mayor profundidad en caso de presentarse un incidente que así lo requiera.

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

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

III. REGISTRO DE INCIDENTES:

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

No se ha presentado ningún incidente

1. Los datos que registra:
   a) La persona que resolvió el incidente;
   b) La metodología aplicada;[10]
   c) Para soportes físicos: Los oficios, documentos, expedientes, estantes o archiveros, tanto los dañados como los recuperados, y
   d) Para soportes electrónicos: Los campos, registros, tablas, bases de datos o archivos electrónicos, tanto dañados como recuperados, el nombre de los sistemas y la infraestructura afectada, indicar si el incidente afectó el servidor principal y los servidores de respaldo, etc.
2. Si el registro está en soporte físico o en soporte electrónico;
3. Cómo asegura la integridad de dicho registro, y
4. Para el caso de soportes electrónicos, quién autoriza la recuperación de datos.

V. ACCESO A LAS INSTALACIONES

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

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

Para las personas que acceden a sus instalaciones:

[10] **Ejemplo de procedimiento en caso de presentarse un incidente:**
- **a)** El Encargado elabora y entrega un informe al responsable a más tardar al día siguiente de haber ocurrido el incidente. Dicho informe precisa los soportes físicos o electrónicos afectados y, en su caso, los recuperados.
- **b)** El incidente se registra en una hoja de cálculo anotando quién resolvió el incidente y los soportes dañados y recuperados. Dicha hoja está protegida con una contraseña de acceso. Su integridad se garantiza generando y almacenando un resumen creado por un algoritmo digestor en un servidor del centro de datos y respaldándola en un CD-R después de registrar un incidente.
- **c)** En caso de robo o extravío de datos personales, el responsable del sistema de tratamiento de datos personales, al tener conocimiento del incidente, da vista al titular de la dependencia o entidad para su conocimiento y al titular del área jurídica o aquél que tenga facultades para presentar denuncias o querellas ante el Ministerio Público para que, en el ámbito de sus atribuciones, determine lo conducente.
- **d)** A no más de 3 días naturales de haber ocurrido el incidente, el responsable del sistema de tratamiento de datos personales da aviso al público mediante un desplegado de prensa que difunde el hecho por diversos medios, según la gravedad del caso, a escala local, regional o nacional.
- **e)** En caso de robo o extravío de datos personales, se alerta a los titulares de los datos afectados para que tomen sus precauciones ante el posible uso ilegal de su información. Para tal efecto, el responsable del sistema de tratamiento de datos personales da aviso por escrito a dichos titulares, a más tardar cinco días naturales de haber ocurrido el incidente, recabando el acuse de recibo de esta notificación. Adicionalmente, se da aviso por correo electrónico o por teléfono.

No hay acceso de personas a las instalaciones donde se manejan el Sistema de Control de Gestión, así como no hay acceso de personas a las instalaciones donde se resguardan los archivos físicos de documentación.

a) ¿Cómo las identifica?
b) ¿Cómo las autentifica?
c) ¿Cómo les autoriza el acceso?

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

No hay acceso de personas a las instalaciones donde se manejan el Sistema de Control de Gestión, así como no hay acceso de personas a las instalaciones donde se resguardan los archivos físicos de documentación.

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

Para las personas que acceden a dichos espacios interiores:

1. ¿Cómo las identifica?
2. ¿Cómo las autentifica?
3. ¿Cómo les autoriza el acceso?

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

Por la naturaleza de la información consignada en el Sistema de Control de Gestión, no existe la necesidad de llevar a cabo la actualización de la misma, en virtud de que trata de trámites únicos cuya vigencia tiene fin.

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

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

VII. PERFILES DE USUARIO Y CONTRASEÑAS

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

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

El Sistema de Control de Gestión está basado en usuarios y roles.

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

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

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

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

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

4. Administración de perfiles de usuario y contraseñas:

a) ¿Quién da de alta nuevos perfiles?
El administrador del sistema
b) ¿Quién autoriza la creación de nuevos perfiles?
La Coordinadora de Gestión
c) ¿Se lleva registro de la creación de nuevos perfiles?
si

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

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

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

1. Señalar si realiza respaldos
   a) Completos_X, diferenciales ___ o incrementales___;
   b) De forma automática ____ o Manual ___X__,
   c) Periodicidad con que los realiza: Diario de Base de Datos y semanal de archivos almacenados.
2. El tipo de medios (por ejemplo: cintas magnéticas, discos duros, CD-ROM, entre otros) que utiliza para almacenar las copias de seguridad;[11]
   Disco Duro
3. Cómo y dónde archiva esos medios, y

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

En el área de sistemas

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

El Jefe de Departamento de Sistemas

IX. PLAN DE CONTINGENCIA

1. Presentar el plan de contingencia con el cual garantiza la continuidad de la operación del sistema o informar si no lo tiene, pero se encuentra desarrollándolo.
   En caso de contingencia como lo fue la Pandemia por el virus Covid-19, y a efecto de continuar dando el servicio bajo medidas de seguridad de datos personales, se implementaron con los responsables del manejo del Sistema de Control de Gestión, se habilitó por usuario el acceso remoto.
2. Si cuenta con plan de contingencia y lo ha implementado, deberá indicar si realiza pruebas de eficiencia de este.
   Cuando se ha requerido utilizar el plan de contingencia, las pruebas de eficiencia son realizadas diariamente por el Jefe del Departamento de Sistemas
3. Informar si cuenta con un sitio redundante (alterno) y señalar lo siguiente:
   no
   a) El tipo de sitio (caliente, tibio o frío);[12]
   b) Si el sitio es propio o subcontratado con un tercero;
   c) Los procedimientos, el equipo y el personal que designa para poner en marcha tal sitio y
   d) Tiempo que le lleva poner en marcha el sitio, según las pruebas de eficiencia.

Continuar los mismos pasos con el siguiente SISTEMA A2. (Nombre del sistema A2)[13], B1. (Nombre del sistema B1), etc.

I. Transferencias de datos personales
II. Resguardo de sistemas de tratamiento de datos personales con soportes físicos
III. Bitácoras para accesos y operación cotidiana
IV. Registro de incidentes
V. Acceso a las instalaciones
VI. Actualización del sistema de tratamiento de datos personales
VII. Perfiles de usuario y contraseñas
VIII. Procedimientos de respaldo y recuperación de datos
IX. Plan de contingencia

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

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

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

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

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

(Denominación del área específica del Área Universitaria A)*		
Identificador único*	DGPU01 (Dirección General del Patrimonio Universitario)	
(Nombre del sistema A1)*	*Sistema de Control de Gestión*	
Recurso*	**Descripción***	**Control***
El Sistema de Control de Gestión se encuentra detrás de un Firewall, por lo que sólo se tiene acceso desde el interior de la DGPU	*El administrador de la red del Patronato Universitario, en caso de haber algún intento o mensaje de alerta lo notifica al Jefe de Departamento de Sistemas de la DGPU*	*No aplica*

7.2. Procedimiento para la revisión de las medidas de seguridad

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

(Denominación del área específica del Área Universitaria A)*		
Identificador único*	DGPU01 (Dirección General del Patrimonio Universitario)	
(Nombre del sistema A1)*	*Sistema de Control de Gestión*	
Medida de seguridad*	**Procedimiento***	**Responsable***
Instalar las actualizaciones de seguridad más recientes	*Revisión y actualización del sistema operativo*	*El Jefe del Departamento del Sistemas de la DGPU*

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

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

(Denominación del área específica del Área Universitaria A)*		
Identificador único*	DGPU01 (Dirección General del Patrimonio Universitario)	
(Nombre del sistema A1)*	*Sistema de Control de Gestión*	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***
Revisión de los usuarios del Sistema de Control de Gestión	*Garantizar que los usuarios operarios están activos en la DPGU.*	*El Jefe del Departamento del Sistemas de la DGPU*

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

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

(Denominación del área específica del Área Universitaria A)*		
Identificador único*	DGPU01 (Dirección General del Patrimonio Universitario)	
(Nombre del sistema A1)*	*Sistema de Control de Gestión*	
Medida de seguridad*	**Acciones***	**Responsable***
Se corrobora con el Jefe de Departamento inmediato la permanencia del usuario.	*Actualización del estatus y la platilla de usuarios para el acceso al Sistema de Control de Gestión*	*El Jefe del Departamento del Sistemas de la DGPU*

8. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

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

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

(Denominación del área específica del Área Universitaria A)*	
Identificador único*	DGPU01 (Dirección General del Patrimonio Universitario)
(Nombre del sistema A1)*	*Sistema de Control de Gestión*

Actividad*	Descripción*	Duración*	Cobertura*
Capacitación sobre el manejo del Sistema de Control de Gestión al contar con personal de nuevo ingreso.	*La Capacitación se realiza junto con el Usuario toda vez que el sistema es de fácil manejo.*	*1 hora*	*Personal de la DGPU*
Notificación mediante el sistema con guías de las nuevas funcionalidades implementadas	*La Capacitación se realiza publicando la guía en el sistema, en la pantalla de inicio*	*1 hora*	*Personal de la DGPU*

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

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

(Denominación del área específica del Área Universitaria A)*			
Identificador único*	DGPU01 (Dirección General del Patrimonio Universitario)		
(Nombre del sistema A1)*	*Sistema de Control de Gestión*		
Actividad*	**Descripción***	**Duración***	**Cobertura***
No se cuenta con un programa de difusión de la protección de datos personales.			

9. MEJORA CONTINUA

9.1. Actualización y mantenimiento de sistemas de información

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

(Denominación del área específica del Área Universitaria A)*	
Identificador único*	DGPU01 (Dirección General del Patrimonio Universitario)
(Nombre del sistema A1)*	*Sistema de Control de Gestión*

Actividad*	Descripción*	Duración*	Cobertura*
El Sistema de Control de Gestión fue Desarrollado por el Jefe de Departamento de Sistemas de la DGPU	*Se trata de un sistema, estructurado para cubrir las necesidades de registro, resguardo, respaldo, asignación y verificación de las solicitudes que ingresan a la DGPU*	*En promedio se realiza una actualización de funcionalidad al año*	*La Dirección General del Patrimonio Universitario*

9.2. Actualización y mantenimiento de equipo de cómputo

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

(Denominación del área específica del Área Universitaria A)*			
Identificador único*	DGPU01 (Dirección General del Patrimonio Universitario)		
(Nombre del sistema A1)*	*Sistema de Control de Gestión*		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Diagnóstico de los equipos de cómputo utilizado para el funcionamiento del Sistema de Control de Gestión	*Revisión de los equipos, evaluación de obsolescencia y en su caso cambio de equipo.*	*Cada 3 años o cuando se requiere.*	*Capacidad y velocidad para procesar datos.*

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

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

(Denominación del área específica del Área Universitaria A)*		
Identificador único*	DGPU01 (Dirección General del Patrimonio Universitario)	
(Nombre del sistema A1)*	*Sistema de Control de Gestión*	
Proceso*	**Descripción***	**Responsable***
Verificación periódica de	*Se sube una base de datos de*	*Jefe del Departamento de*

los respaldos del Sistema de Control de Gestión	*prueba con la información respaldada para garantizar su integridad*	*Sistemas de la DGPU*

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

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

(Denominación del área específica del Área Universitaria A)*		
Identificador único*	DGPU01 (Dirección General del Patrimonio Universitario)	
(Nombre del sistema A1)*	*Sistema de Control de Gestión*	
Proceso*	**Descripción***	**Responsable***
Al dar de baja el equipo asignados a los usuarios por obsolescencia o falla, se lleva a cabo de acuerdo a la normatividad en la materia, el borrado de información	*Se corre el comando en Windows para tal efecto.*	*Jefe del Departamento de Sistemas de la DGPU*

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

No se ha presentado el caso

(Informar y describir el procedimiento para la cancelación de un sistema de tratamiento de datos personales.)[14]

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

a) Denominación

[14] La cancelación da lugar al bloqueo de los datos, esto es, el periodo en el que la autoridad conservará los datos para efectos de responsabilidades, el cual será equivalente al plazo de prescripción de las acciones derivadas de la relación jurídica que funda el tratamiento en términos de la normatividad de aplicable y, cumplido este plazo, deberá procederse a la supresión del dato que implica el borrado físico del mismo.
Bajo este contexto, la cancelación no supone automáticamente la supresión o borrado físico de los datos, sino que se debe determinar un período o fase previa de bloqueo de los datos, en el cual no se podrá disponer de tales datos en la misma medida en que la podría hacerse por el área universitaria de estar en operación el Sistema de tratamiento de datos personales.
La cancelación de sistema de tratamiento de datos personales debe considerar lo establecido en los Lineamientos Generales para la Organización, Administración y Conservación de los Archivos de la Universidad Nacional Autónoma de México, así como el Catálogo de disposición documental de la Universidad del año respectivo, a fin de atender al valor documental de la información contenida en el mismo.

b) Motivo de la cancelación

B) PLAZOS Y CONDICIONES PARA EL BLOQUEO DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES:[15]

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

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

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

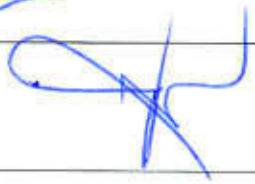
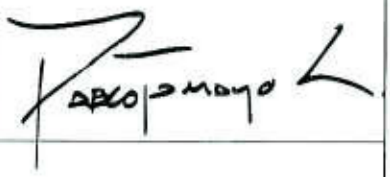
(Describir el procedimiento para suprimir el sistema, una vez cumplido el plazo de bloqueo)

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

(Describir las técnicas para la eliminación física del sistema)

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

11. APROBACIÓN DEL DOCUMENTO DE SEGURIDAD

		Nombre y firma de quienes revisaron el presente documento:
Responsable del desarrollo:	T.I. Oscar Blanco Badillo Jefe del Departamento de Sistemas 555622-6357 oscar.blanco@patronato.unam.mx	
Revisó:	Mtra. Adriana Zamora Mariaca Coordinadora de Gestión 55562263561 adriana.zamora@patronato.unam.mx	
Autorizó:	Mtro. Pablo Tamayo Castroparedes Director General del Patrimonio Universitario 55562263561 pablo.tamayo@unam.mx	
Fecha de aprobación:	(Incluir la fecha de liberación del documento)	
Fecha de actualización:	(Incluir la primer versión e ir agregando las subsiguientes del documento)	