ESCUELA NACIONAL DE ESTUDIOS SUPERIORES UNIDAD MORELIA

DOCUMENTO DE SEGURIDAD

Morelia, Michoacán 16 agosto de 2022.

Índice.

Presentación.

Desde su creación en el año 2012, la Escuela Nacional de Estudios Superiores Unidad Morelia busca mantener en sus programas educativos un enfoque multidisciplinario con un modelo educativo innovador, flexible y con nuevas licenciaturas en todos los campos del conocimiento. En particular, la ENES Unidad Morelia, ofrece a sus alumnos una fuerte vinculación con la investigación dada la cercanía y participación de académicos de los centros de investigación que forman parte del campus. La mayoría de las licenciaturas de la ENES son carreras vinculadas con la investigación, pues sus programas conjuntan dos o más disciplinas y fueron creadas con el sustento de varias entidades académicas.

Este documento tiene el objetivo de documentar las actividades realizadas para integrar nuestro Sistema de Gestión de la Seguridad de Datos Personales en la ENES Morelia. Se trata de la primera versión del documento, el cual se enriquecerá conforme se vayan cumpliendo las tareas trazadas en el mismo, se hagan verificaciones de medidas implantadas o se cree o modifique sustancialmente algún sistema de tratamiento de datos personales.
El alcance de este sistema se centra en proteger “Todos los datos personales y datos personales sensibles que recabe y trate la ENES Morelia” de accesos no autorizados o de tratamientos distintos a los fines para los que fueron recabados.

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 dependencia 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 dependencia 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 describen 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”.*

Sistemas de Tratamiento de Datos Personales.

La ENES Morelia cuenta con diferentes Sistemas y Aplicaciones que facilitan la ejecución de los procesos de las diferentes áreas académico-administrativas, algunos de los cuales hacen tratamiento de datos personales de alumnos, profesores y trabajadores.

A continuación se enlistan los sistemas que hacen tratamiento de datos personales en la ENES Morelia:

- FOCO
- PRESTAD
- INGRESSIO
- CRONOS
- ESCOLARES
- CODR
- SISTEMA DE INFORMES ANUALES PARA PROFESORES
- SISTEMA PARA CONTRATACIÓN DE PROFESORES
- SISTEMA PARA REGISTRO DE PRÁCTICAS Y TRABAJOS DE CAMPO
- SISTEMA PARA LA EVALUACIÓN DOCENTE
- COMISIÓN DE RECURSOS
- PLATAFORMA DE ENCUESTAS
- MOODLE

Sistema de Formación Complementaria e Ingresos Extraordinarios (FOCO)

Automatiza los procesos de registro a eventos (académicos o culturales) de formación complementaria de diferentes áreas de la ENES Morelia como: Centro de Idiomas (CIEM), Coordinación de Humanidades y Artes, Departamento de Educación Continua, Centro de Autoacceso Mediateca, Centro Cultural, Área de prevención y apoyo a la Salud, Coordinación de Atención y Servicios a la Comunidad. Gestiona diferentes tipos de eventos como: cursos, talleres, auto accesos, diplomados, exámenes, congresos, etc. Permite el registro de personas locales, nacionales y extranjeras. Los usuarios registrados en eventos pueden realizar sus pagos mediante fichas de depósito bancarias emitidas desde el sistema mediante su integración con Patronato Universitario. El sistema permite la consulta de movimientos bancarios por referencia, de manera que si una ficha es pagada, se podrá visualizar como tal 72 horas después. Los administradores del sistema pueden gestionar descuentos y recargos sobre sus eventos mediante la autorización manual o automática. Asimismo, es posible gestionar convocatorias con periodos específicos de registro que son puestas en marcha de manera automática en las fechas establecidas en las mismas. El sistema también apoya labores administrativas mediante la generación de reportes como: descarga de pagos por conciliar, descarga de registros por convocatoria, visualización de ingresos por convocatoria, agrupación de registros para la emisión de una ficha de depósito única, descarga de registros por oficina virtual, numeralia sobre los estados de origen de usuarios por evento. Es posible realizar la solicitud de facturas de registros pagados.

ANEXO I: Documento de Seguridad de datos personales

ÍNDICE

INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Secretaría Técnica	
Identificador único*	EM015
Nombre del sistema*	Sistema de Formación Complementaria e Ingresos Extraordinarios (FOCO)
Datos personales (sensibles o no) contenidos en el sistema*:	Nombre, domicilio particular (calle, colonia, delegación o municipio, estado, código postal), teléfono (particular, celular y/o institucional), correo electrónico (personal o institucional), RFC, CURP, estado de origen, institución de procedencia, fecha de nacimiento, edad, contacto de emergencia (nombre, parentesco y teléfono), tipo de sangre, alergias, escolaridad máxima, sexo, tipo de usuario (externo, egresado o comunidad UNAM), programa académico (alumnos y exalumnos UNAM), número de trabajador (UNAM) o número de cuenta (alumnos y exalumnos UNAM). Datos de facturación: Nombre o razón social y RFC.
Responsable*:	Escuela Nacional de Estudios Superiores Unidad Morelia
Nombre*:	Dr. Santiago Cortés Hernández
Cargo*:	Secretario Técnico
Funciones*:	Decidir sobre el tratamiento automatizado de los datos personales, así como el contenido, finalidad y uso del sistema.
Obligaciones*:	- Decidir a qué usuarios se les da acceso al sistema con privilegios administrativos. - Decidir sobre la incorporación de nuevas funcionalidades en el sistema. - Vigilar que el sistema cumpla con todas las medidas de seguridad técnicas, físicas y administrativas.
	Encargados[1]:
(Nombre del Encargado 1*)	Mtro. José Alfredo Noriega Carmona
Cargo*:	Técnico Académico en Desarrollo de Software

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

Funciones*:	Realizar el proceso de software con la finalidad de atender las necesidades administrativas de la ENES Morelia, dicha actividad involucra la captación de datos personales de usuarios con la finalidad de brindar apoyo técnico y administrativo a los responsables de procesos de registro a eventos académicos, deportivos y culturales de diferentes áreas de la institución.
Obligaciones*:	Procurar la protección de los datos personales contenidos en el sistema mediante la implementación de estrategias y mecanismos de seguridad en su desarrollo y mantenimiento.
	Usuarios:
(Nombre del Usuario 1*)	Gabriela Juárez Pérez
Cargo*:	Coordinadora del Centro de Idiomas
Funciones*:	Brindar seguimiento a los procesos de registro de usuarios.
Obligaciones*:	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 desempeña en la Universidad mediante el uso del sistema.
(Nombre del Usuario 2*)	Bertha Karina Godina Sepúlveda
Cargo*:	Coordinadora del Centro de Auto Acceso y Mediateca
Funciones*:	Brindar seguimiento a los procesos de registro de usuarios.
Obligaciones*:	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 desempeña en la Universidad mediante el uso del sistema.
(Nombre del Usuario 3*)	Claudia Orozco Hernández
Cargo*:	Jefe de Departamento de Educación Continua
Funciones*:	Brindar seguimiento a los procesos de registro de usuarios.
Obligaciones*:	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 desempeña en la Universidad mediante el uso del sistema.

(Nombre del Usuario 4*)	María Dolores Rodríguez Guzmán
Cargo*:	Coordinadora de Atención y Servicios a la Comunidad
Funciones*:	Brindar seguimiento a los procesos de registro de usuarios pertenecientes a la comunidad UNAM.
Obligaciones*:	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 desempeña en la Universidad mediante el uso del sistema.
(Nombre del Usuario 5*)	María García Guzmán
Cargo*:	Delegada Administrativa del Centro Cultural
Funciones*:	Brindar seguimiento a los procesos de registro de usuarios.
Obligaciones*:	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 desempeña en la Universidad mediante el uso del sistema.
(Nombre del Usuario 6*)	Luis Francisco Ambriz Vázquez
Cargo*:	Área de prevención y apoyo a la salud
Funciones*:	Brindar seguimiento a los procesos de registro de usuarios pertenecientes a la comunidad UNAM.
Obligaciones*:	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 desempeña en la Universidad mediante el uso del sistema.

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

Secretaría Técnica	
Identificador único*	EM015

Nombre del sistema*	Sistema de Formación Complementaria e Ingresos Extraordinarios (FOCO)
Tipo de soporte[2]:*	Electrónico
Descripción[3]:*	Base de datos
Características del lugar donde se resguardan los soportes[4]:*	[redacted]

Eliminado: Información específica sobre el lugar donde se resguardan los soportes de la información.

Fundamentación: De conformidad con 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 los artículos 32 y 36 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

Motivación: En virtud de que estos datos hace identificable las formas en que es posible atacar o vulnerar nuestros sistemas de información que resguardan datos personales y 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.

[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.

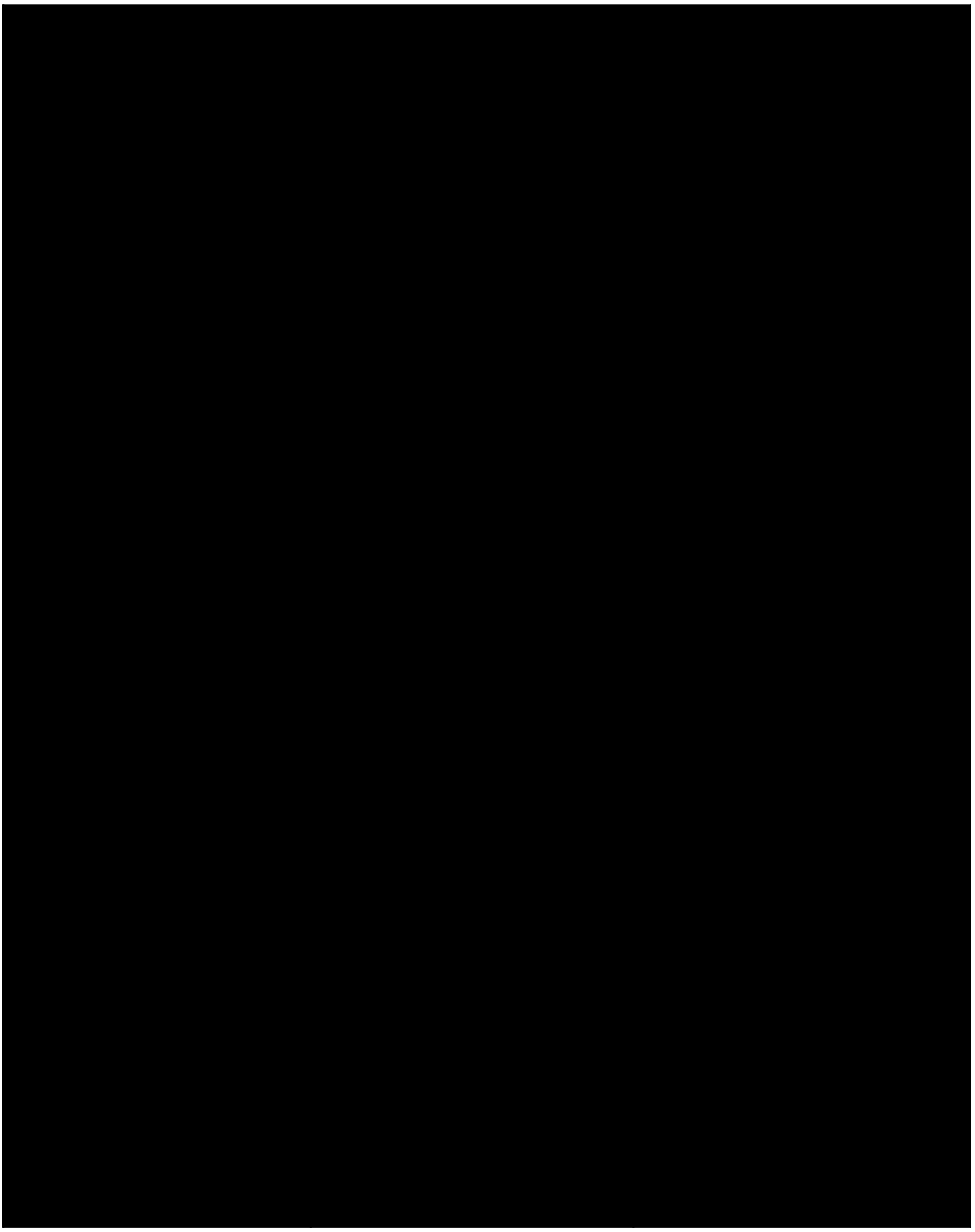
[4] Para describir las características del lugar donde se resguardan los soportes, se deberá considerar lo siguiente:

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



[redacted]

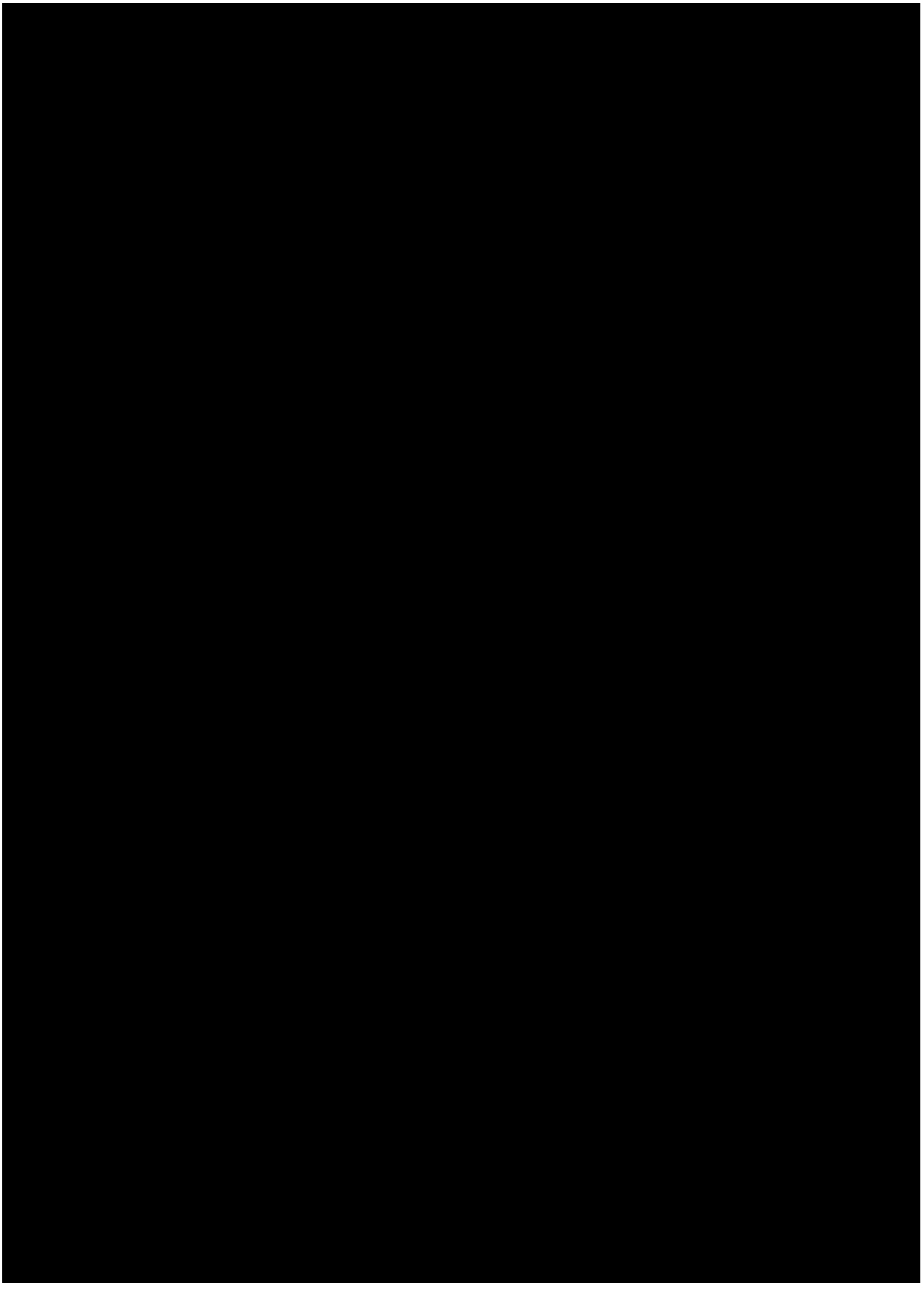
Eliminado: Análisis de riesgos.

Fundamentación: De conformidad con 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 los artículos 32 y 36 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

Motivación: En virtud de que estos datos hace identificable las formas en que es posible atacar o vulnerar nuestros sistemas de información que resguardan datos personales y 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.

4. ANÁLISIS DE BRECHA

[redacted]



[redacted]

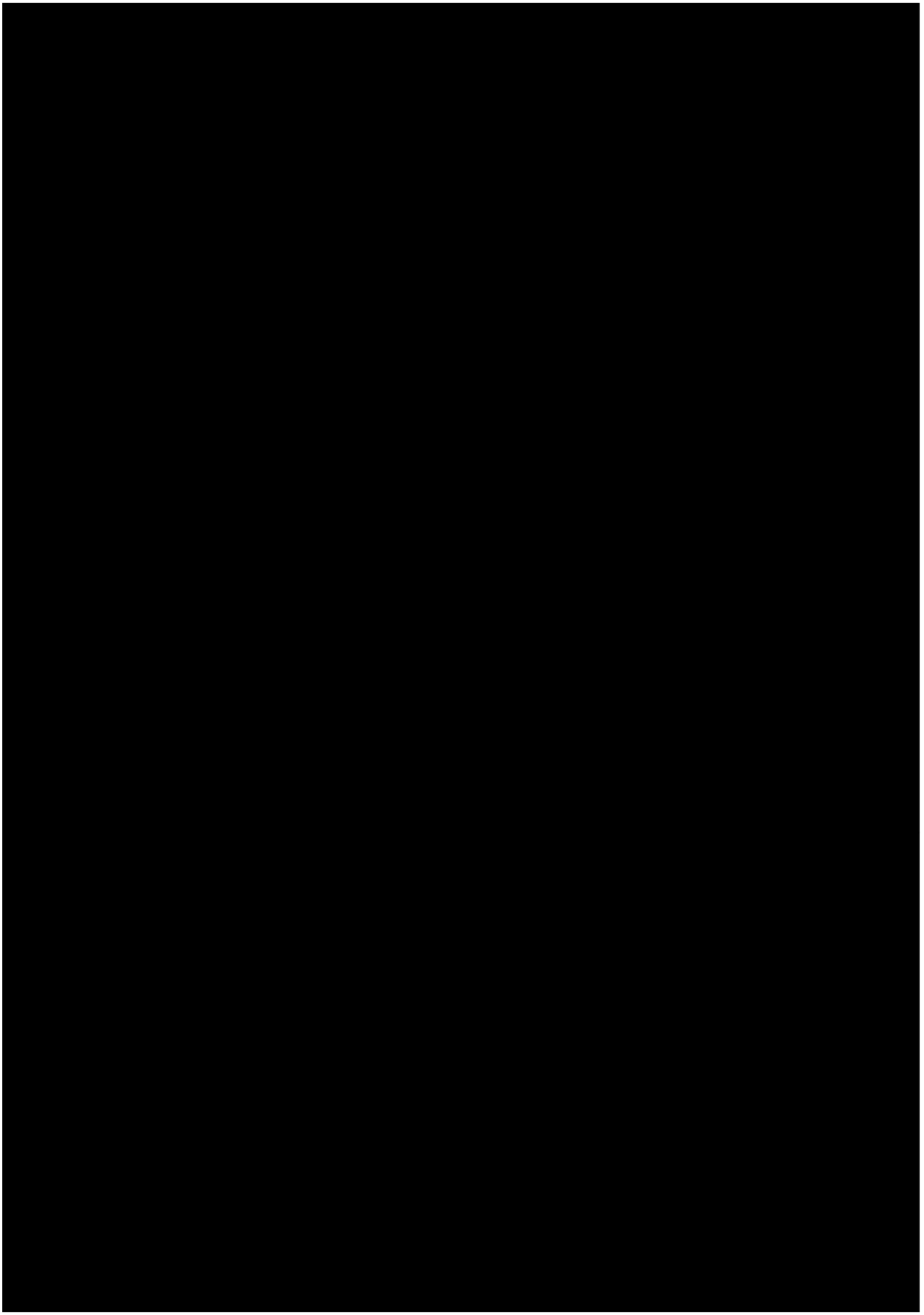
Eliminado: Análisis de brecha.

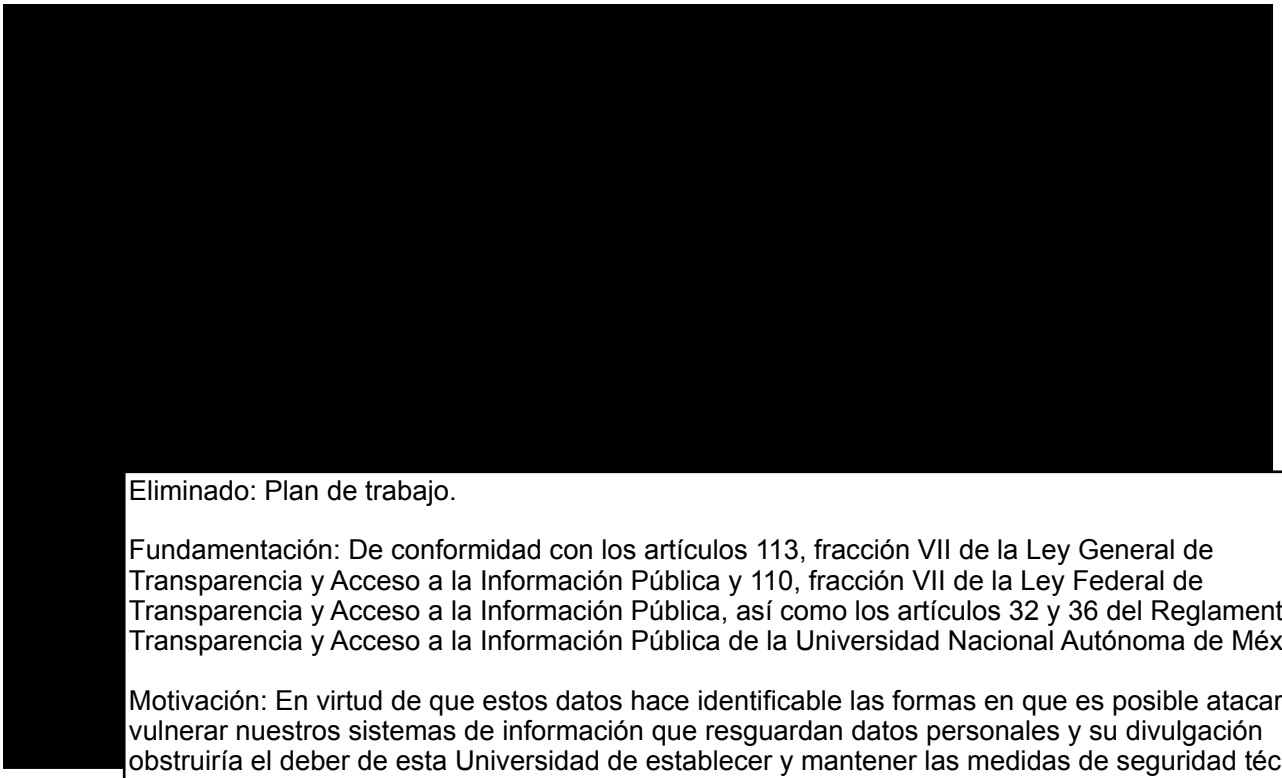
Fundamentación: De conformidad con los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública, así como los artículos 32 y 36 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

Motivación: En virtud de que estos datos hace identificable las formas en que es posible atacar o vulnerar nuestros sistemas de información que resguardan datos personales y 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.

5. PLAN DE TRABAJO

[redacted]





Eliminado: Plan de trabajo.

Fundamentación: De conformidad con 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 los artículos 32 y 36 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

Motivación: En virtud de que estos datos hace identificable las formas en que es posible atacar o vulnerar nuestros sistemas de información que resguardan datos personales y 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.

6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

I. TRANSFERENCIAS DE DATOS PERSONALES

Secretaría Técnica*	
Identificador único*	EM015
(Nombre del sistema A1)*	Sistema de Formación Complementaria e Ingresos Extraordinarios (FOCO)
TRANSFERENCIAS DE DATOS PERSONALES	

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

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

El Sistema de Formación Complementaria e Ingresos Extraordinarios (FOCO) no realiza tratamiento de datos personales con soportes físicos, ya que se encuentra en soporte electrónico mediante el uso de una base de datos.

1. Señalar las medidas de seguridad que ha implementado el área universitaria para el resguardo de los soportes físicos del sistema de manera que evite la alteración, pérdida o acceso no autorizado a los mismos.[6]
2. Señalar en un listado las personas (nombre, cargo, funciones y obligaciones) que tienen acceso a los soportes físicos del sistema.[7]

II. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

La información correspondiente al presente apartado es registrada de manera automática por el sistema, y se encuentra almacenada en el servidor.

---

[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.

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

   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]

---

[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:

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.

3. Lugar dónde almacena las bitácoras y por cuánto tiempo;
4. La manera en que asegura la integridad de las bitácoras, y
5. Respecto del análisis de las bitácoras:
   a) Quién es el responsable de analizarlas (si es el área universitaria o si es un tercero) y cada cuándo las analiza, y
   b) Para el caso de que las bitácoras estén en soporte electrónico: las herramientas de análisis utilizadas.

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 cuenta con un procedimiento de atención de incidentes.

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 electrónicos7: 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):

[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.

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

Para las personas que acceden a sus instalaciones:

a) ¿Cómo las identifica?
No se cuenta con mecanismos de identificación.

b) ¿Cómo las autentifica?
No se cuenta con mecanismos de autenticación.

c) ¿Cómo les autoriza el acceso?
No se cuenta con mecanismos de control de acceso.

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

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

Para las personas que acceden a dichos espacios interiores:

1. ¿Cómo las identifica?
Se tiene definida una lista de acceso para el personal autorizado.
2. ¿Cómo las autentifica?
Mediante credencial y número de trabajador.
3. ¿Cómo les autoriza el acceso?
Si se encuentran en la lista de acceso autorizada, o si son proveedores acompañados por un empleado autorizado. Se les solicita se registren en la bitácora correspondiente.

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

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

Los usuarios pueden realizar la actualización de sus datos personales una vez que han ingresado al sistema mediante su credencial de acceso, en el apartado “Actualizar mis datos”. Los menores de edad son registrados en el sistema por parte de sus padres o tutor.

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

VII. PERFILES DE USUARIO Y CONTRASEÑAS

1. Modelo de control de acceso:
Está basado en roles.

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

a) ¿Cuenta con un sistema operativo de red instalado en sus equipos?
Si

b) ¿Proporciona dicho sistema operativo un manejo riguroso de perfiles de usuario y contraseñas?
Si

c) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?
Si

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

a) ¿Ofrece dicho software un manejo riguroso de perfiles de usuario y contraseñas?
Si

b) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?
Solo las contraseñas.

4. Administración de perfiles de usuario y contraseñas:

a) ¿Quién da de alta nuevos perfiles?
Los usuarios sin privilegios administrativos pueden darse de alta en el sistema por sí mismos, con el fin de registrarse a eventos académicos o culturales.

b) ¿Quién autoriza la creación de nuevos perfiles?
El Secretario Técnico autoriza la creación de nuevos perfiles con privilegios administrativos.

c) ¿Se lleva registro de la creación de nuevos perfiles?
Desde el sistema es posible visualizar la creación de perfiles.

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

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

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

c) ¿Cómo se evita el acceso remoto no autorizado?
- Se cuenta con controles de acceso basados en roles y privilegios.
- El acceso remoto a los servidores se realiza mediante conexiones VPN habilitadas únicamente a los responsables de los sistemas.
- Implementación de captcha en el inicio de sesión del sistema.

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: _Semanal_

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 y de estado sólido
3. Cómo y dónde archiva esos medios, y Consultar los documentos: “Plan de respaldos ENES Morelia” y “Bitácora de control de los respaldos”.
4. Quién es el responsable de realizar estas operaciones (el área universitaria o un tercero). El área universitaria.

IX. PLAN DE CONTINGENCIA

1. Presentar el plan de contingencia con el cual garantiza la continuidad de la operación del sistema o informar si no lo tiene, pero se encuentra desarrollándolo.
   Se cuenta con algunas medidas como las especificadas en el documento: Medidas de seguridad en los periodos de inactividad o mantenimiento, pero no se tiene desarrollado el plan de contingencia.
2. Si cuenta con plan de contingencia y lo ha implementado, deberá indicar si realiza pruebas de eficiencia de este.
   No se cuenta con plan de contingencia.
3. Informar si cuenta con un sitio redundante (alterno) y señalar lo siguiente:
   a) El tipo de sitio (caliente, tibio o frío);[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.

No se cuenta con un sitio redundante.

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

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

[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.

[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.

Secretaría Técnica*		
Identificador único*	EM015	
Nombre del sistema*	Sistema de Formación Complementaria e Ingresos Extraordinarios (FOCO)	
Recurso*	**Descripción***	**Control***
Herramientas automatizadas	Se utilizan diversas herramientas para realizar pruebas de penetración y escaneo de puertos abiertos.	Las herramientas utilizadas están bajo el control y operación de personal de UNAM CERT. Responsables: Personal de la Coordinación de Seguridad de la Información - UNAM CERT.
Bitácora del sistema	Revisión aleatoria	Revisar de manera regular la bitácora con el fin de indagar si hubiera algún uso o comportamiento inusual en la aplicación mediante el análisis de excepciones. Responsable: Mtro. José Alfredo Noriega Carmona
Correo electrónico	Envío de reportes mediante correos electrónicos autenticados.	Los reportes en formato XLSX que contienen datos personales son enviados directamente al buzón de correo electrónico del usuario con privilegios administrativos. Responsable de la implementación: Mtro. José Alfredo Noriega Carmona

7.2. Procedimiento para la revisión de las medidas de seguridad

Secretaría Técnica*		
Identificador único*	EM015	
Nombre del sistema*	Sistema de Formación Complementaria e Ingresos Extraordinarios (FOCO)	
Medida de seguridad*	**Procedimiento***	**Responsable***
Principio del menor privilegio	Revisiones periódicas de las cuentas de los usuarios del sistema.	El responsable de realizar la revisión es el Mtro. José Alfredo Noriega Carmona La duración de la revisión es un día hábil.
Plan de respaldos de información	Revisión y validación del historial de respaldos del sistema.	El responsable de realizar la revisión es el Mtro. José Alfredo Noriega Carmona La duración de la revisión es un día hábil.
Sincronizar la fecha y hora con el servidor NTP (Network Time Protocol) oficial de la UNAM	Revisiones periódicas de la hora y fecha del sistema.	El responsable de realizar la revisión es el Mtro. Froylan Hernández Rendón La duración de la revisión es un día hábil.
Instalar y mantener actualizado el software antimalware.	Revisión y actualización de la versión del software antivirus y de la base de datos.	El responsable de realizar la revisión es el Mtro. Froylan Hernández Rendón La duración de la revisión es un día hábil.
Instalar las actualizaciones de seguridad más recientes disponibles.	Revisión y actualizaciones del sistema operativo.	El responsable de realizar la revisión es el Mtro. Froylan Hernández Rendón

		La duración de la revisión es un día hábil.

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

Secretaría Técnica*		
Identificador único*	EM015	
Nombre del sistema*	Sistema de Formación Complementaria e Ingresos Extraordinarios (FOCO)	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***
Principio del menor privilegio	Se encontró que todas las cuentas de usuarios del sistema cuentan con los privilegios correspondientes.	El responsable de realizar la revisión es el Mtro. José Alfredo Noriega Carmona
Plan de respaldos de información	Se cuenta con respaldos actualizados de la información del sistema.	El responsable de realizar la revisión es el Mtro. José Alfredo Noriega Carmona
Sincronizar la fecha y hora con el servidor NTP (Network Time Protocol) oficial de la UNAM	La fecha y hora están sincronizadas con el servidor NTP de la UNAM.	El responsable de realizar la revisión es el Mtro. Froylan Hernández Rendón
Instalar y mantener actualizado el software antimalware.	El Software antivirus está actualizado.	El responsable de realizar la revisión es el Mtro. Froylan Hernández Rendón
Instalar las actualizaciones de seguridad más recientes disponibles.	El sistema operativo cuenta con las actualizaciones correspondientes.	El responsable de realizar la revisión es el Mtro. Froylan Hernández Rendón

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

Secretaría Técnica*		
Identificador único*	EM015	
Nombre del sistema*	Sistema de Formación Complementaria e Ingresos Extraordinarios (FOCO)	
Medida de seguridad*	**Acciones***	**Responsable***
Uso de certificados SSL	Realizar la renovación anual del certificado SSL para el subdominio donde se encuentra el sistema.	El responsable de las acciones es el Mtro. Froylan Hernández Rendón.
Actualización del lenguaje de programación	Actualizar el lenguaje de programación a la última versión estable disponible a petición del responsable del sistema.	El responsable de las acciones es el Mtro. Froylan Hernández Rendón.

8. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

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

Secretaría Técnica*			
Identificador único*	EM015		
Nombre del sistema*	Sistema de Formación Complementaria e Ingresos Extraordinarios (FOCO)		
Actividad*	**Descripción***	**Duración***	**Cobertura***

Capacitación para la Protección de Datos Personales	Curso en línea	25 horas. Fecha de inicio: 20 de noviembre de 2020. Fecha de término: 17 de enero de 2021	Público objetivo: Enlaces de Transparencia, Responsables de Seguridad de Datos Personales, Responsables de Tecnologías de la Información, así como funcionarios y empleados universitarios. Sin vigencia. Sin frecuencia de actualización.
Medidas de Seguridad Técnicas para la Protección de Datos Personales	Curso en línea	25 horas. Fecha de inicio: 8 de febrero de 2021. Fecha de término: 14 de marzo de 2021.	Público objetivo: Enlaces de Transparencia, Responsables de Seguridad de Datos Personales, Responsables de Tecnologías de la Información, así como funcionarios y empleados universitarios. Sin vigencia. Sin frecuencia de actualización.
Elaboración de Documento de Seguridad y Sistema de Gestión de Seguridad de Datos Personales de las áreas universitarias	Curso en línea	25 horas. Fecha de inicio: 25 de marzo de 2022 Fecha de término: 25 de marzo de 2022.	Público objetivo: Enlaces de Transparencia, Responsables de Seguridad de Datos Personales, Responsables de Tecnologías de la Información, así como funcionarios y empleados universitarios. Sin vigencia. Sin frecuencia de actualización.
La importancia de la protección de datos personales	Seminario en línea	1 hora.	Público en general.

		Fecha: 16 de junio de 2022.	Sin vigencia. Sin frecuencia de actualización.

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

Secretaría Técnica*			
Identificador único*	EM015		
Nombre del sistema*	Sistema de Formación Complementaria e Ingresos Extraordinarios (FOCO)		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Indique actividad, tema, recursos para la difusión. Agregar un renglón por cada elemento	*Describa el tipo de elemento, sus objetivos y forma de impartición, publicación o distribución*	*Indique duración del elemento en horas, días, meses, su fecha de inicio y de término*	*Mencione público objetivo, vigencia del elemento y frecuencia de actualización*

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

9. MEJORA CONTINUA

9.1. Actualización y mantenimiento de sistemas de información

Secretaría Técnica*	
Identificador único*	EM015

Nombre del sistema*	Sistema de Formación Complementaria e Ingresos Extraordinarios (FOCO)		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Actualización de tecnologías de desarrollo	1.Solicitar la actualización del lenguaje de programación en el servidor de pruebas. 3. Actualizar el framework de desarrollo de la aplicación y sus dependencias. 2. Realizar exhaustivas pruebas de funcionalidad en busca de errores, bugs o problemas de compatibilidad como consecuencia de las actualizaciones anteriores. 3. Corregir y/o refactorizar características del sistema. 4. Aplicar modificaciones realizadas en el servidor de pruebas y verificar el correcto funcionamiento. 5. Llevar a cabo todas las actualizaciones anteriores en el servidor de producción.	12 meses	BackEnd de la aplicación: tecnologías de desarrollo.

9.2. Actualización y mantenimiento de equipo de cómputo

Secretaría Técnica*			
Identificador único*	EM015		
Nombre del sistema*	Sistema de Formación Complementaria e Ingresos Extraordinarios (FOCO)		
Actividad*	**Descripción***	**Duración***	**Cobertura***

Indique actividad. Agregar un renglón por cada elemento	*Describa el tipo de actividad, sus objetivos e impacto la actualización o mantenimiento del equipo de cómputo*	*Indique duración en la ejecución de la actividad en horas, días, meses, su fecha de inicio y de término*	*Mencione los aspectos de equipo de cómputo que son resueltos, total o parcialmente, por la actividad.*

No se han asignado recursos para la actualización del equipo de cómputo.

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

Secretaría Técnica*		
Identificador único*	EM015	
Nombre del sistema*	Sistema de Formación Complementaria e Ingresos Extraordinarios (FOCO)	
Proceso*	**Descripción***	**Responsable***
El formato de los archivos de respaldo de información corresponde a información en texto plano.	Se realiza una verificación regular de que el contenido de los respaldos de información es accesible y funcional.	Responsable del proceso: Mtro. José Alfredo Noriega Carmona Tiempo máximo de ejecución en días: 1
El proceso de respaldo de información se encuentra contenido en el documento Plan de respaldos ENES Morelia	El proceso se describe en el documento Plan de respaldos ENES Morelia	Responsable del proceso: Mtro. José Alfredo Noriega Carmona Tiempo máximo de ejecución en días: 1

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

Secretaría Técnica*		
Identificador único*	EM015	
(Nombre del sistema A1)*	Sistema de Formación Complementaria e Ingresos Extraordinarios (FOCO)	
Proceso*	**Descripción***	**Responsable***
El proceso se encuentra contenido en el documento Borrado Seguro ENES Morelia	El proceso se describe en el documento Borrado Seguro ENES Morelia	Responsable del proceso de borrado seguro: Mtro. José Alfredo Noriega Carmona Responsable de la disposición final de equipos o componentes de cómputo: Mtro. Froylán Hernández Rendón Tiempo máximo de ejecución: 5 días.

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

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

(Informar y describir el procedimiento para la cancelación de un sistema de tratamiento de datos personales.)[13]

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

a) Denominación
b) Motivo de la cancelación

B) PLAZOS Y CONDICIONES PARA EL BLOQUEO DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES:[14]

(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)

---

[13] 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.

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

Sistema de Préstamos y Adeudos (PRESTAD)

Permite el registro de préstamos realizados y adeudos generados en las diferentes áreas de la ENES Morelia, por parte de estudiantes o trabajadores. Este tipo de eventos podrán ser registrados y liberados por los trabajadores responsables de dichas áreas. El sistema permite el envío por correo electrónico de Constancias de No adeudo o Eventos (préstamos o adeudos) por resolver, según corresponda, por parte del coordinador de la licenciatura correspondiente. Permite la suspensión de usuarios derivado de la entrega tardía de un material.

ANEXO I: Documento de Seguridad de datos personales

ÍNDICE

1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Secretaría Técnica	
Identificador único*	EM016
Nombre del sistema*	Sistema de Préstamos y Adeudos (PRESTAD)
Datos personales (sensibles o no) contenidos en el sistema*:	Nombre, correo electrónico (personal o institucional), programa académico (estudiantes y trabajadores UNAM), número de trabajador (UNAM) o número de cuenta (estudiantes UNAM).
Responsable*:	Escuela Nacional de Estudios Superiores Unidad Morelia
Nombre*:	Dr. Santiago Cortés Hernández
Cargo*:	Secretario Técnico
Funciones*:	Decidir sobre el tratamiento automatizado de los datos personales, así como el contenido, finalidad y uso del sistema.
Obligaciones*:	- Decidir a qué usuarios se les da acceso al sistema con privilegios administrativos.

	- Decidir sobre la incorporación de nuevas funcionalidades en el sistema. - Vigilar que el sistema cumpla con todas las medidas de seguridad técnicas, físicas y administrativas.
	Encargados[1]:
(Nombre del Encargado 1*)	Mtro. José Alfredo Noriega Carmona
Cargo*:	Técnico Académico en Desarrollo de Software
Funciones*:	Realizar el proceso de software con la finalidad de atender las necesidades administrativas de la ENES Morelia, dicha actividad involucra la captación de datos personales de usuarios con la finalidad de brindar apoyo técnico y administrativo a los responsables en áreas susceptibles de generarse préstamos y/o adeudos de materiales.
Obligaciones*:	Procurar la protección de los datos personales contenidos en el sistema mediante la implementación de estrategias y mecanismos de seguridad en su desarrollo y mantenimiento.
	Usuarios:
(Nombre del Usuario 1*)	Alejandra Guadalupe Esquivel Guillén
Cargo*:	Responsable en Módulo PC Puma
Funciones*:	Gestionar préstamos y adeudos a la Comunidad Universitaria de la ENES Morelia
Obligaciones*:	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 desempeña en la Universidad mediante el uso del sistema.
(Nombre del Usuario 2*)	Víctor Hugo Coria González
Cargo*:	Responsable en Módulo PC Puma
Funciones*:	Gestionar préstamos y adeudos a la Comunidad Universitaria de la ENES Morelia
Obligaciones*:	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

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

	tenga conocimiento, con motivo de las funciones que desempeña en la Universidad mediante el uso del sistema.
(Nombre del Usuario 3*)	José Rodrigo Hernández Rangel
Cargo*:	Responsable en Módulo PC Puma
Funciones*:	Gestionar préstamos y adeudos a la Comunidad Universitaria de la ENES Morelia
Obligaciones*:	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 desempeña en la Universidad mediante el uso del sistema.
(Nombre del Usuario 4*)	Edison Piñon Bravo
Cargo*:	Responsable en Módulo PC Puma
Funciones*:	Gestionar préstamos y adeudos a la Comunidad Universitaria de la ENES Morelia
Obligaciones*:	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 desempeña en la Universidad mediante el uso del sistema.
(Nombre del Usuario 5*)	Lizeth García Salgado
Cargo*:	Responsable en Módulo PC Puma
Funciones*:	Gestionar préstamos y adeudos a la Comunidad Universitaria de la ENES Morelia
Obligaciones*:	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 desempeña en la Universidad mediante el uso del sistema.
(Nombre del Usuario 6*)	Sinhué A. R. Haro Corzo
Cargo*:	Responsable en Laboratorio de Física
Funciones*:	Gestionar préstamos y adeudos a la Comunidad Universitaria de la ENES Morelia

Obligaciones*:	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 desempeña en la Universidad mediante el uso del sistema.
(Nombre del Usuario 7*)	María Dolores Rodríguez Guzmán
Cargo*:	Responsable en la Coordinación de Atención y Servicios a la Comunidad
Funciones*:	Gestionar préstamos y adeudos a la Comunidad Universitaria de la ENES Morelia
Obligaciones*:	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 desempeña en la Universidad mediante el uso del sistema.
(Nombre del Usuario 8*)	Carlos Rodrigo Zalapa Cardiel
Cargo*:	Técnico Académico en la Secretaría Técnica
Funciones*:	Gestionar préstamos a trabajadores de la ENES Morelia.
Obligaciones*:	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 desempeña en la Universidad mediante el uso del sistema.

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

Secretaría Técnica	
Identificador único*	EM016
Nombre del sistema*	Sistema de Préstamos y Adeudos (PRESTAD)
Tipo de soporte[2]:*	Electrónico

[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.

Descripción[3]:*	Base de datos
Características del lugar donde se resguardan los soportes[4]:*	[redacted]

Eliminado: Información específica sobre el lugar donde se resguardan los soportes de la información.

Fundamentación: De conformidad con 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 los artículos 32 y 36 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

Motivación: En virtud de que estos datos hace identificable las formas en que es posible atacar o vulnerar nuestros sistemas de información que resguardan datos personales y 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.

[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.

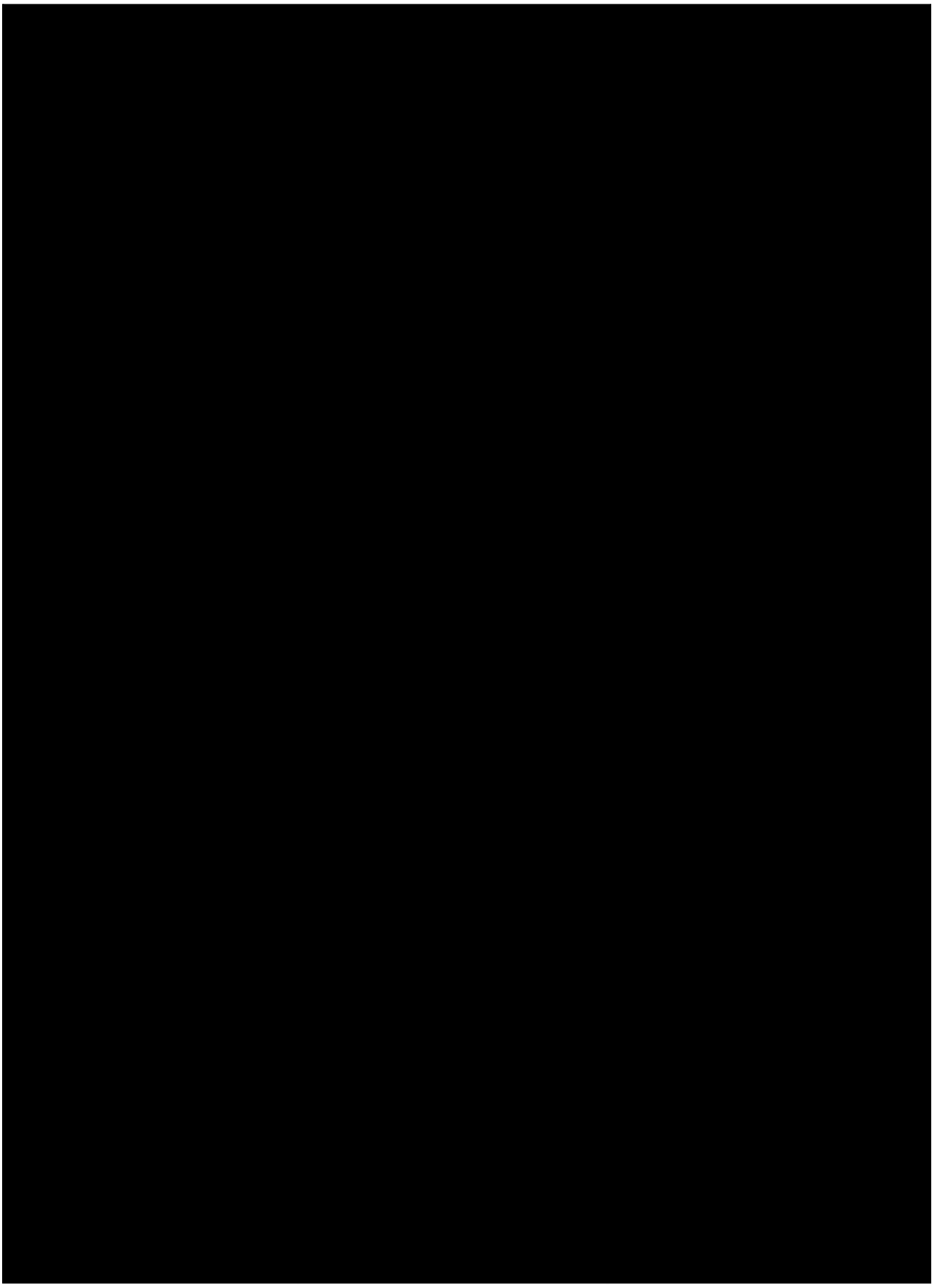
[4] Para describir las características del lugar donde se resguardan los soportes, se deberá considerar lo siguiente:

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



[redacted]

Eliminado: Análisis de riesgos.

Fundamentación: De conformidad con 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 los artículos 32 y 36 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

Motivación: En virtud de que estos datos hace identificable las formas en que es posible atacar o vulnerar nuestros sistemas de información que resguardan datos personales y 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.

4. ANÁLISIS DE BRECHA

[redacted]

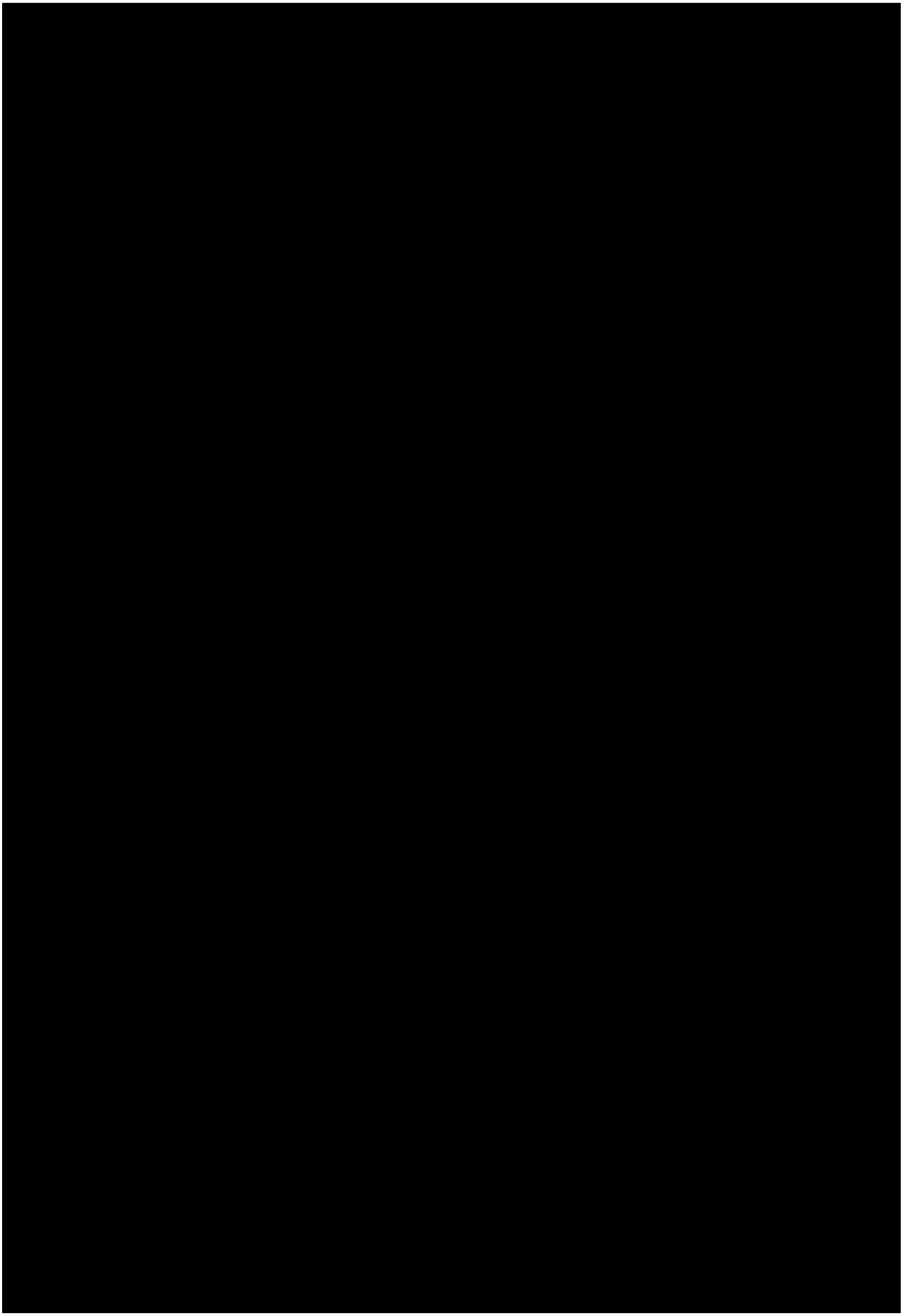
[redacted]

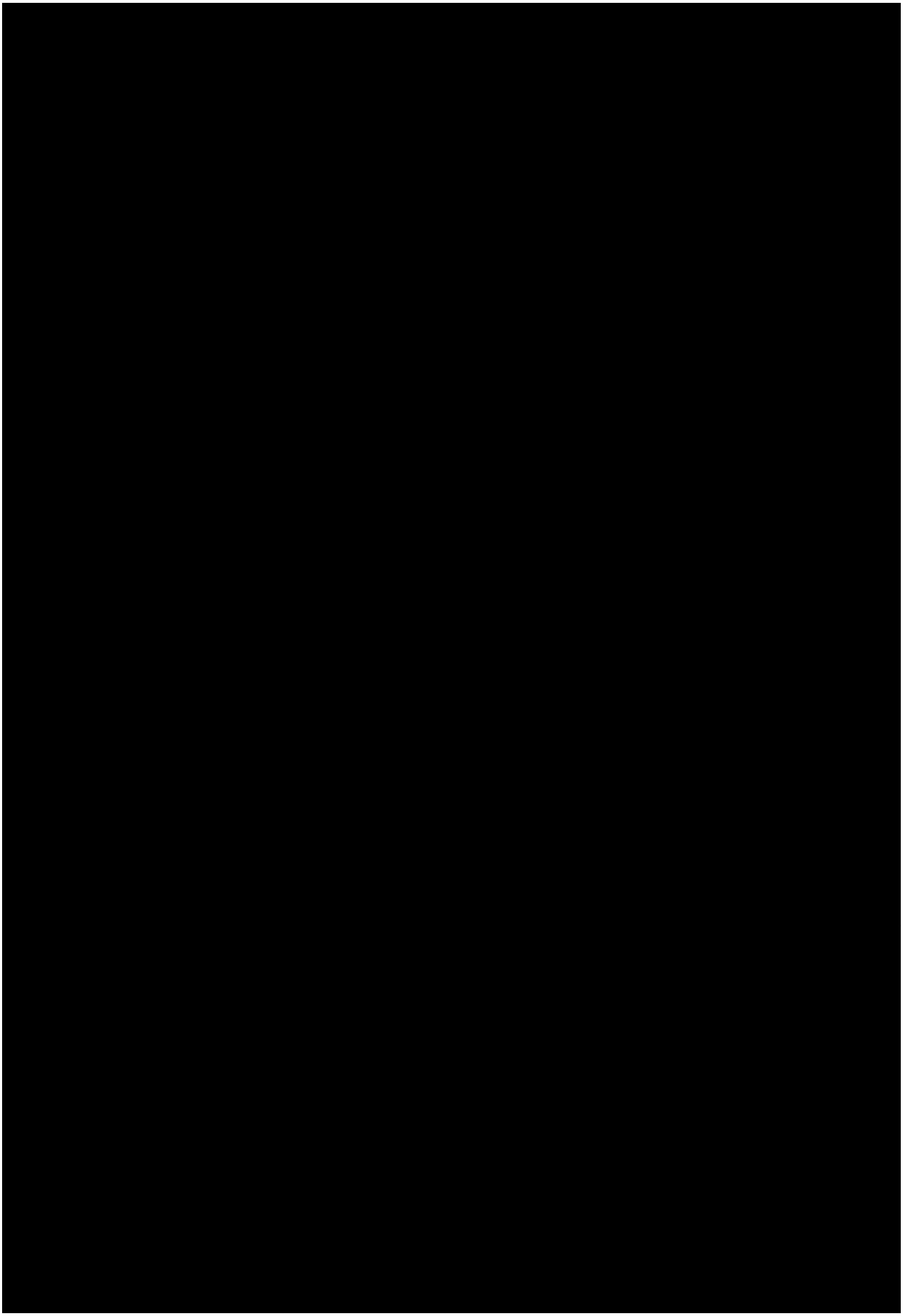
Eliminado: Análisis de brecha.

Fundamentación: De conformidad con 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 los artículos 32 y 36 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

Motivación: En virtud de que estos datos hace identificable las formas en que es posible atacar o vulnerar nuestros sistemas de información que resguardan datos personales y 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.

5. PLAN DE TRABAJO





Eliminado: Plan de trabajo.

Fundamentación: De conformidad con 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 los artículos 32 y 36 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

Motivación: En virtud de que estos datos hace identificable las formas en que es posible atacar o vulnerar nuestros sistemas de información que resguardan datos personales y 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.

6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

I. TRANSFERENCIAS DE DATOS PERSONALES

Secretaría Técnica*	
Identificador único*	EM016
(Nombre del sistema A1)*	Sistema de Préstamos y Adeudos (PRESTAD)
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:[5]	No se realizan transferencias de datos personales mediante el traslado de soportes físicos.
Transferencias mediante el traslado de soportes electrónicos:	No se realizan transferencias de datos personales mediante el traslado de soportes electrónicos.
Transferencias mediante el traslado sobre redes electrónicas:	No se realizan transferencias de datos personales mediante el traslado sobre redes electrónicas.

[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.

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

El Sistema de Préstamos y Adeudos (PRESTAD) no realiza tratamiento de datos personales con soportes físicos, ya que se encuentra en soporte electrónico mediante el uso de una base de datos.

1. Señalar las medidas de seguridad que ha implementado el área universitaria para el resguardo de los soportes físicos del sistema de manera que evite la alteración, pérdida o acceso no autorizado a los mismos.[6]
2. Señalar en un listado las personas (nombre, cargo, funciones y obligaciones) que tienen acceso a los soportes físicos del sistema.[7]

II. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

La información correspondiente al presente apartado es registrada de manera automática por el sistema, y se encuentra almacenada en el servidor.

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

[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:

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.

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
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 cuenta con un procedimiento de atención de incidentes.

1. Los datos que registra:

   a) La persona que resolvió el incidente;

   b) La metodología aplicada;[10]

---

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.

[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

c) Para soportes físicos: Los oficios, documentos, expedientes, estantes o archiveros, tanto los dañados como los recuperados, y

d) Para soportes electrónicos: Los campos, registros, tablas, bases de datos o archivos electrónicos, tanto dañados como recuperados, el nombre de los sistemas y la infraestructura afectada, indicar si el incidente afectó el servidor principal y los servidores de respaldo, etc.

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

V. ACCESO A LAS INSTALACIONES

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

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

Para las personas que acceden a sus instalaciones:

a) ¿Cómo las identifica?
No se cuenta con mecanismos de identificación.

b) ¿Cómo las autentifica?
No se cuenta con mecanismos de autenticación.

c) ¿Cómo les autoriza el acceso?
No se cuenta con mecanismos de control de acceso.

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

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

Para las personas que acceden a dichos espacios interiores:

---

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.

1. ¿Cómo las identifica?
   Se tiene definida una lista de acceso para el personal autorizado.
2. ¿Cómo las autentifica?
   Mediante credencial y número de trabajador.
3. ¿Cómo les autoriza el acceso?
   Si se encuentran en la lista de acceso autorizada, o si son proveedores acompañados por un empleado autorizado. Se les solicita se registren en la bitácora correspondiente.

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

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

Los usuarios que deseen realizar la actualización de sus datos personales deberán acudir a cualquier área de préstamos y solicitar al responsable la actualización de sus datos personales.

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

VII. PERFILES DE USUARIO Y CONTRASEÑAS

1. Modelo de control de acceso:

Está basado en roles.

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

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

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

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

4. Administración de perfiles de usuario y contraseñas:

a) ¿Quién da de alta nuevos perfiles?
   El encargado puede crear perfiles con rol: administrador.
   Los responsables de áreas (rol: administrador) pueden crear perfiles sin privilegios

administrativos.

b) ¿Quién autoriza la creación de nuevos perfiles?
El Secretario Técnico autoriza la creación de nuevos perfiles con rol: administrador.

c) ¿Se lleva registro de la creación de nuevos perfiles?
Desde el sistema es posible visualizar la creación de perfiles.

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

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

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

c) ¿Cómo se evita el acceso remoto no autorizado?
- Se cuenta con controles de acceso basados en roles y privilegios.
- El acceso remoto a los servidores se realiza mediante conexiones VPN habilitadas únicamente a los responsables de los sistemas.
- Implementación de captcha en el inicio de sesión del sistema.

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: _Semanal_

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 y de estado sólido

3. Cómo y dónde archiva esos medios, y Consultar los documentos: "Plan de respaldos ENES Morelia" y "Bitácora de control de los respaldos".

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

IX. PLAN DE CONTINGENCIA

1. Presentar el plan de contingencia con el cual garantiza la continuidad de la operación del sistema o informar si no lo tiene, pero se encuentra desarrollándolo.
Se cuenta con algunas medidas como las especificadas en el documento: "Medidas de seguridad en los periodos de inactividad o mantenimiento", pero no se tiene desarrollado el plan de contingencia.

2. Si cuenta con plan de contingencia y lo ha implementado, deberá indicar si realiza pruebas de eficiencia de este.
No se cuenta con plan de contingencia.

[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.

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

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.

No se cuenta con un sitio redundante.

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*		
Identificador único*	EM016	
Nombre del sistema*	Sistema de Préstamos y Adeudos (PRESTAD)	
Recurso*	**Descripción***	**Control***
Herramientas automatizadas	Se utilizan diversas herramientas para realizar pruebas de penetración y escaneo de puertos abiertos.	Las herramientas utilizadas están bajo el control y operación de personal de UNAM CERT. Responsables: Personal de la Coordinación de Seguridad de la Información - UNAM CERT.

[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.

Bitácora del sistema	Revisión aleatoria	Revisar de manera regular la bitácora con el fin de indagar si hubiera algún uso o comportamiento inusual en la aplicación mediante el análisis de excepciones. Responsable: Mtro. José Alfredo Noriega Carmona

7.2. Procedimiento para la revisión de las medidas de seguridad

Secretaría Técnica*		
Identificador único*	EM016	
Nombre del sistema*	Sistema de Préstamos y Adeudos (PRESTAD)	
Medida de seguridad*	**Procedimiento***	**Responsable***
Principio del menor privilegio	Revisiones periódicas de las cuentas de los usuarios del sistema.	El responsable de realizar la revisión es el Mtro. José Alfredo Noriega Carmona La duración de la revisión es un día hábil.
Plan de respaldos de información	Revisión y validación del historial de respaldos del sistema.	El responsable de realizar la revisión es el Mtro. José Alfredo Noriega Carmona La duración de la revisión es un día hábil.
Sincronizar la fecha y hora con el servidor NTP (Network Time Protocol) oficial de la UNAM	Revisiones periódicas de la hora y fecha del sistema.	El responsable de realizar la revisión es el Mtro. Froylan Hernández Rendón La duración de la revisión es un día hábil.

Instalar y mantener actualizado el software antimalware.	Revisión y actualización de la versión del software antivirus y de la base de datos.	El responsable de realizar la revisión es el Mtro. Froylan Hernández Rendón La duración de la revisión es un día hábil.
Instalar las actualizaciones de seguridad más recientes disponibles.	Revisión y actualizaciones del sistema operativo.	El responsable de realizar la revisión es el Mtro. Froylan Hernández Rendón La duración de la revisión es un día hábil.

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

Secretaría Técnica*		
Identificador único*	EM016	
Nombre del sistema*	Sistema de Préstamos y Adeudos (PRESTAD)	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***
Principio del menor privilegio	Se encontró que todas las cuentas de usuarios del sistema cuentan con los privilegios correspondientes.	El responsable de realizar la revisión es el Mtro. José Alfredo Noriega Carmona
Plan de respaldos de información	Se cuenta con respaldos actualizados de la información del sistema.	El responsable de realizar la revisión es el Mtro. José Alfredo Noriega Carmona
Sincronizar la fecha y hora con el servidor NTP (Network Time Protocol) oficial de la UNAM	La fecha y hora están sincronizadas con el servidor NTP de la UNAM.	El responsable de realizar la revisión es el Mtro. Froylan Hernández Rendón
Instalar y mantener actualizado el software antimalware.	El Software antivirus está actualizado.	El responsable de realizar la revisión es el Mtro. Froylan Hernández Rendón

Instalar las actualizaciones de seguridad más recientes disponibles.	El sistema operativo cuenta con las actualizaciones correspondientes.	El responsable de realizar la revisión es el Mtro. Froylan Hernández Rendón.

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

Secretaría Técnica*		
Identificador único*	EM016	
Nombre del sistema*	Sistema de Préstamos y Adeudos (PRESTAD)	
Medida de seguridad*	**Acciones***	**Responsable***
Uso de certificados SSL	Realizar la renovación anual del certificado SSL para el subdominio donde se encuentra el sistema.	El responsable de las acciones es el Mtro. Froylan Hernández Rendón.
Actualización del lenguaje de programación	Actualizar el lenguaje de programación a la última versión estable disponible a petición del responsable del sistema	El responsable de las acciones es el Mtro. Froylan Hernández Rendón.

8. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

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

Secretaría Técnica*	
Identificador único*	EM016

Nombre del sistema*	Sistema de Préstamos y Adeudos (PRESTAD)		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Capacitación para la Protección de Datos Personales	Curso en línea	25 horas. Fecha de inicio: 20 de noviembre de 2020. Fecha de término: 17 de enero de 2021	Público objetivo: Enlaces de Transparencia, Responsables de Seguridad de Datos Personales, Responsables de Tecnologías de la Información, así como funcionarios y empleados universitarios. Sin vigencia. Sin frecuencia de actualización.
Medidas de Seguridad Técnicas para la Protección de Datos Personales	Curso en línea	25 horas. Fecha de inicio: 8 de febrero de 2021. Fecha de término: 14 de marzo de 2021.	Público objetivo: Enlaces de Transparencia, Responsables de Seguridad de Datos Personales, Responsables de Tecnologías de la Información, así como funcionarios y empleados universitarios. Sin vigencia. Sin frecuencia de actualización.
Elaboración de Documento de Seguridad y Sistema de Gestión de Seguridad de Datos Personales de las áreas universitarias	Curso en línea	25 horas. Fecha de inicio: 25 de marzo de 2022 Fecha de término: 25 de marzo de 2022.	Público objetivo: Enlaces de Transparencia, Responsables de Seguridad de Datos Personales, Responsables de Tecnologías de la Información, así como funcionarios y empleados universitarios.

			Sin vigencia. Sin frecuencia de actualización.
La importancia de la protección de datos personales	Seminario en línea	1 hora. Fecha: 16 de junio de 2022.	Público en general. Sin vigencia. Sin frecuencia de actualización.

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

Secretaría Técnica*			
Identificador único*	EM016		
Nombre del sistema*	Sistema de Préstamos y Adeudos (PRESTAD)		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Indique actividad, tema, recursos para la difusión. Agregar un renglón por cada elemento	*Describa el tipo de elemento, sus objetivos y forma de impartición, publicación o distribución*	*Indique duración del elemento en horas, días, meses, su fecha de inicio y de término*	*Mencione público objetivo, vigencia del elemento y frecuencia de actualización*

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

9. MEJORA CONTINUA

9.1. Actualización y mantenimiento de sistemas de información

Secretaría Técnica*			
Identificador único*	EM016		
Nombre del sistema*	Sistema de Préstamos y Adeudos (PRESTAD)		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Actualización de tecnologías de desarrollo	1.Solicitar la actualización del lenguaje de programación en el servidor de pruebas. 3. Actualizar el framework de desarrollo de la aplicación y sus dependencias. 2. Realizar exhaustivas pruebas de funcionalidad en busca de errores, bugs o problemas de compatibilidad como consecuencia de las actualizaciones anteriores. 3. Corregir y/o refactorizar características del sistema. 4. Aplicar modificaciones realizadas en el servidor de pruebas y verificar el correcto funcionamiento. 5. Llevar a cabo todas las actualizaciones	12 meses	BackEnd de la aplicación: tecnologías de desarrollo.

	anteriores en el servidor de producción.		

9.2. Actualización y mantenimiento de equipo de cómputo

Secretaría Técnica*			
Identificador único*	EM016		
Nombre del sistema*	Sistema de Préstamos y Adeudos (PRESTAD)		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Indique actividad. Agregar un renglón por cada elemento	*Describa el tipo de actividad, sus objetivos e impacto la actualización o mantenimiento del equipo de cómputo*	*Indique duración en la ejecución de la actividad en horas, días, meses, su fecha de inicio y de término*	*Mencione los aspectos de equipo de cómputo que son resueltos, total o parcialmente, por la actividad.*

No se han asignado recursos para la actualización del equipo de cómputo.

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

Secretaría Técnica*	
Identificador único*	EM016

Nombre del sistema*	Sistema de Préstamos y Adeudos (PRESTAD)	
Proceso*	**Descripción***	**Responsable***
El formato de los archivos de respaldo de información corresponde a información en texto plano.	Se realiza una verificación regular de que el contenido de los respaldos de información es accesible y funcional.	Responsable del proceso: Mtro. José Alfredo Noriega Carmona Tiempo máximo de ejecución en días: 1
El proceso de respaldo de información se encuentra contenido en el documento "Plan de respaldos ENES Morelia".	El proceso se describe en el documento "Plan de respaldos ENES Morelia".	Responsable del proceso: Mtro. José Alfredo Noriega Carmona Tiempo máximo de ejecución en días: 1

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

Secretaría Técnica*		
Identificador único*	EM016	
(Nombre del sistema A1)*	Sistema de Préstamos y Adeudos (PRESTAD)	
Proceso*	**Descripción***	**Responsable***
El proceso se encuentra contenido en el documento "Borrado Seguro ENES Morelia"	El proceso se describe en el documento "Borrado Seguro ENES Morelia"	Responsable del proceso de borrado seguro: Mtro. José Alfredo Noriega Carmona Responsable de la disposición final de equipos o componentes

		de cómputo: Mtro. Froylán Hernández Rendón Tiempo máximo de ejecución: 5 días.

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

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

(Informar y describir el procedimiento para la cancelación de un sistema de tratamiento de datos personales.)[13]

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

a) Denominación
b) Motivo de la cancelación

B) PLAZOS Y CONDICIONES PARA EL BLOQUEO DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES:[14]

[13] 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.

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

(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)

Sistema INGRESSIO

La función de este sistema es llevar el control del registro de asistencia de los trabajadores de la ENES Morelia, para lo cual es necesario registrar en la base de datos, datos personales de los usuarios.

ANEXO I: Documento de Seguridad de datos personales

ÍNDICE

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

Secretaría Técnica	
Identificador único*	EM011 (ENES Morelia sistema 11)
Nombre del sistema*	**INGRESSIO**
Datos personales (sensibles o no) contenidos en el sistema*:	1. **Datos personales en general**: a. **Datos de identificación**: nombre completo (apellido paterno, apellido materno y nombre o nombres). b. **Datos laborales**: número de trabajador UNAM. c. **Datos académicos**: no se registran datos académicos. 2. **Datos personales sensibles**: huella digital.
Responsable*:	Escuela Nacional de Estudios Superiores Unidad Morelia
Nombre*:	**Dr. Santiago Cortés Hernández**
Cargo*:	**Secretario Técnico**
Funciones*:	Estar a cargo y decidir sobre el tratamiento automatizado de los datos personales, así como el contenido, finalidad y uso del sistema.
Obligaciones*:	- Decidir a qué usuarios se les da acceso al sistema con privilegios administrativos. - Decidir sobre la incorporación de nuevas funcionalidades en el sistema. - Vigilar que el sistema cumpla con todas las medidas de seguridad técnicas, físicas y administrativas.
	Encargados:

(Nombre del Encargado 1*)	**Mtro. Froylan Hernández Rendón**
Cargo*:	**Responsable de Cómputo y Tecnologías de Información**
Funciones*:	1. Administración y soporte técnico del sistema Ingressio. 2. Generar reportes de la información que requieren las áreas de la escuela.
Obligaciones*:	1. Cumplir con la obligación legal de resguardar los datos personales. 2. Mantener actualizado y funcionando correctamente el sistema informático INGRESSIO. 3. Generar respaldos de la información contenida. 4. Transferir información a las áreas que la requieran justificando debidamente su uso. 5. Resguardar la confidencialidad de los datos personales a los que se tiene acceso. 6. Actuar conscientemente para prevenir el posible robo o acceso no autorizado a los equipos en el exterior. 7. Leer el Contrato de Adhesión y firmarlo aceptando el entendimiento de las obligaciones que tiene respecto a la protección de los datos personales.
	Usuarios:
1. **RODRIGUEZ ECHEVARRIA ALEJANDRA**	ARODRIGUEZ (Tipo: ADMINISTRADOR)
Cargo*:	Asistente de la Secretaría Técnica
Funciones*:	1. Administrar datos personales de docentes y ayudantes de docencia. 2. Actualización y depuración de información en el sistema.
Obligaciones*:	1. Cumplir con la obligación legal de resguardar los datos

	personales. 2. Administrar la información contenida en el sistema. 3. Resguardar la confidencialidad de los datos personales a los que se tiene acceso. 4. Actuar conscientemente para prevenir el posible robo o acceso no autorizado a los equipos en el exterior. 5. Leer el Contrato de Adhesión y firmarlo aceptando el entendimiento de las obligaciones que tiene respecto a la protección de los datos personales.
2. BARAJAS GUTIERREZ DANIEL	DBARAJAS (Tipo: ADMINISTRADOR)
Cargo*:	Asistente de la Secretaría Académica
Funciones*:	1. Administrar datos personales de docentes y ayudantes de docencia. 2. Actualización y depuración de información en el sistema.
Obligaciones*:	1. Cumplir con la obligación legal de resguardar los datos personales. 2. Administrar la información contenida en el sistema. 3. Resguardar la confidencialidad de los datos personales a los que se tiene acceso. 4. Actuar conscientemente para prevenir el posible robo o acceso no autorizado a los equipos en el exterior. 5. Leer el Contrato de Adhesión y firmarlo aceptando el entendimiento de las obligaciones que tiene respecto a la protección de los datos personales.
3. HUERTA SALTO JAVIER	JHUERTA (Tipo: ADMINISTRADOR)
Cargo*:	Técnico Académico
Funciones*:	1. Administrar datos personales de docentes y ayudantes de docencia. 2. Actualización y depuración de información en el sistema.

Obligaciones*:	1. Cumplir con la obligación legal de resguardar los datos personales. 2. Administrar la información contenida en el sistema. 3. Resguardar la confidencialidad de los datos personales a los que se tiene acceso. 4. Actuar conscientemente para prevenir el posible robo o acceso no autorizado a los equipos en el exterior. 5. Leer el Contrato de Adhesión y firmarlo aceptando el entendimiento de las obligaciones que tiene respecto a la protección de los datos personales.

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

Secretaría Técnica	
Identificador único*	EM011
Nombre del sistema*	**INGRESSIO**
Tipo de soporte:*	Electrónico.
Descripción:*	Sistema utilizado para el control de asistencia del personal de la ENES unidad Morelia, mediante el registro de huella digital en lectores biométricos.
Características del lugar donde se resguardan los soportes:*	El sistema está alojado en un servidor que se encuentra instalado en el Data Center de la ENES.
(Nombre del sistema A2*)	
Tipo de soporte*:	Ambos (físico y electrónico).
Descripción*:	Base de Datos.
Características del lugar donde se resguardan los soportes*:	[redacted]

Eliminado: Información específica sobre el lugar donde se resguardan los soportes de la información.

Fundamentación: De conformidad con 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 los artículos 32 y 36 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

Motivación: En virtud de que estos datos hace identificable las formas en que es posible atacar o vulnerar nuestros sistemas de información que resguardan datos personales y 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.

3. ANÁLISIS DE RIESGOS

[redacted]

Eliminado: Análisis de riesgos.

Fundamentación: De conformidad con 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 los artículos 32 y 36 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

Motivación: En virtud de que estos datos hace identificable las formas en que es posible atacar o vulnerar nuestros sistemas de información que resguardan datos personales y 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.

4. ANÁLISIS DE BRECHA

[redacted]

Eliminado: Análisis de brecha.

Fundamentación: De conformidad con 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 los artículos 32 y 36 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

Motivación: En virtud de que estos datos hace identificable las formas en que es posible atacar o vulnerar nuestros sistemas de información que resguardan datos personales y 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.

5. PLAN DE TRABAJO

[redacted]

Eliminado: Plan de trabajo.

Fundamentación: De conformidad con 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 los artículos 32 y 36 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

Motivación: En virtud de que estos datos hace identificable las formas en que es posible atacar o vulnerar nuestros sistemas de información que resguardan datos personales y 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.

6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

I. TRANSFERENCIAS DE DATOS PERSONALES

Secretaría Técnica*	
Identificador único*	EM011
Nombre del sistema*	**INGRESSIO**
TRANSFERENCIAS DE DATOS PERSONALES	

Transferencias mediante el traslado de soportes físicos:[1]	No se realizan transferencias de datos personales mediante el traslado de soportes físicos.
Transferencias mediante el traslado de soportes electrónicos:	No se realizan transferencias de datos personales mediante el traslado de soportes electrónicos.
Transferencias mediante el traslado sobre redes electrónicas:	No se realizan transferencias de datos personales mediante el traslado sobre redes electrónicas.

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.[2]

Los soportes físicos (documentos impresos del Sistema de Gestión de Seguridad de Datos Personales y medios de respaldos de información) son resguardados bajo llave.

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

Santiago Cortés Hernández, Secretario Técnico. Su función es facilitar la información del sistema que requieren las diferentes áreas de las dependencia. Su obligación es gestionar los recursos para mantener actualizado el software y hardware, así como dar seguimiento al buen funcionamiento del sistema.

Froylan Hernández Rendón, Responsable de Cómputo. Su función es administrar y mantener el correcto funcionamiento del sistema, además de generar los reportes con la información que sea requerida. Su obligación es implementar las medidas de seguridad para la protección de datos personales contenidos en el sistema.

---

[1] **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.

[2] 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.

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

Alejandra Rodriguez Echevarria, Asistente. Su función es capturar la información de los usuarios en el sistema. Su obligación es tratar adecuadamente la información que procesa.

II. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

1. Los datos que se registran en las bitácoras:[4]

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

---

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

a) 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.

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;[5]
3. Lugar dónde almacena las bitácoras y por cuánto tiempo;
4. La manera en que asegura la integridad de las bitácoras, y
5. Respecto del análisis de las bitácoras:

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

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

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.

1. Los datos que registra:

   a) La persona que resolvió el incidente;

   b) La metodología aplicada;[6]

   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):

---

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

[6] **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.

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

Para las personas que acceden a sus instalaciones:

a) ¿Cómo las identifica?
No se cuenta con mecanismos de identificación.

b) ¿Cómo las autentifica?
No se cuenta con mecanismos de autenticación.

c) ¿Cómo les autoriza el acceso?
No se cuenta con mecanismos de control de acceso.

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

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

Para las personas que acceden a dichos espacios interiores:

1. ¿Cómo las identifica?
   Se tiene definida una lista de acceso para el personal autorizado.
2. ¿Cómo las autentifica?
   Mediante credencial y número de trabajador.
3. ¿Cómo les autoriza el acceso?
   Si se encuentran en la lista de acceso autorizada, o si son proveedores acompañados por un empleado autorizado. Se les solicita se registren en la bitácora correspondiente.

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

La información se actualiza cada semestre, debido a que es necesario que los profesores de nuevo ingreso registren su huella y sus datos en el sistema para poder registrar su asistencia.

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

VII. PERFILES DE USUARIO Y CONTRASEÑAS

1. Modelo de control de acceso:

Está basado en roles.

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

b) ¿Quién autoriza la creación de nuevos perfiles?

El Secretario Técnico

c) ¿Se lleva registro de la creación de nuevos perfiles?

No, solo se revisa en los archivos del sistema.

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

a) ¿Requieren los usuarios acceso remoto al equipo de cómputo que por lo general utilizan para trabajar con el sistema?

Si

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

Si

c) ¿Cómo se evita el acceso remoto no autorizado?

- Se cuenta con controles de acceso basados en roles y privilegios.
- El acceso remoto a los servidores se realiza mediante conexiones VPN habilitadas únicamente a los responsables de los sistemas.
- Implementación de captcha en el inicio de sesión del sistema.

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: Semestral
2. El tipo de medios (por ejemplo: cintas magnéticas, discos duros, CD-ROM, entre otros) que utiliza para almacenar las copias de seguridad;[7]

   Disco Duro

3. Cómo y dónde archiva esos medios:

   Se resguardan bajo llave en la oficina del administrador.

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

   El área universitaria.

IX. PLAN DE CONTINGENCIA

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

   Se cuenta con algunas medidas, pero no se tiene desarrollado el plan de contingencia.

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

   No se cuenta con plan de contingencia.

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

[7] 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.

a) El tipo de sitio (caliente, tibio o frío);[8]
b) Si el sitio es propio o subcontratado con un tercero;
c) Los procedimientos, el equipo y el personal que designa para poner en marcha tal sitio y
d) Tiempo que le lleva poner en marcha el sitio, según las pruebas de eficiencia.

No se cuenta con un sitio redundante.

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*		
Identificador único*	EM011	
Nombre del sistema*	**INGRESSIO**	
Recurso*	**Descripción***	**Control***
Auditoría Interna	Se utilizan diversas herramientas para realizar pruebas de penetración y escaneo de puertos abiertos.	El responsable del uso de las herramientas y ejecución de las pruebas es el administrador del sistema. Las herramientas utilizadas son de software libre y no requieren licenciamiento.

[8] 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.

7.2. Procedimiento para la revisión de las medidas de seguridad

Secretaría Técnica*		
Identificador único*	EM011	
Nombre del sistema*	**INGRESSIO**	
Medida de seguridad*	**Procedimiento***	**Responsable***
Principio del menor privilegio	Revisiones periódicas de las cuentas de los usuarios del sistema.	El responsable de realizar la revisión es el Mtro. Froylan Hernández Rendón La duración de la revisión es un día hábil.
Plan de respaldos de información	Revisión y validación del historial de respaldos del sistema.	El responsable de realizar la revisión es el Mtro. Froylan Hernández Rendón La duración de la revisión es un día hábil.
Sincronizar la fecha y hora con el servidor NTP (Network Time Protocol) oficial de la UNAM	Revisiones periódicas de la hora y fecha del sistema.	El responsable de realizar la revisión es el Mtro. Froylan Hernández Rendón La duración de la revisión es un día hábil.
Instalar y mantener actualizado el software antimalware.	Revisión y actualización de la versión del software antivirus y de la base de datos.	El responsable de realizar la revisión es el Mtro. Froylan Hernández Rendón La duración de la revisión es un día hábil.
Instalar las actualizaciones de seguridad más recientes disponibles.	Revisión y actualizaciones del sistema operativo.	El responsable de realizar la revisión es el Mtro. Froylan Hernández Rendón La duración de la revisión es un día hábil.

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

Secretaría Técnica*		
Identificador único*	EM011	
Nombre del sistema*	**INGRESSIO**	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***
Principio del menor privilegio	Se encontró que todas las cuentas de usuarios del sistema cuentan con los privilegios correspondientes.	El responsable de realizar la revisión es el Mtro. Froylan Hernández Rendón
Plan de respaldos de información	Se cuenta con respaldos actualizados de la información del sistema.	El responsable de realizar la revisión es el Mtro. Froylan Hernández Rendón
Sincronizar la fecha y hora con el servidor NTP (Network Time Protocol) oficial de la UNAM	La fecha y hora están sincronizadas con el servidor NTP de la UNAM.	El responsable de realizar la revisión es el Mtro. Froylan Hernández Rendón
Instalar y mantener actualizado el software antimalware.	El Software antivirus está actualizado.	El responsable de realizar la revisión es el Mtro. Froylan Hernández Rendón
Instalar las actualizaciones de seguridad más recientes disponibles.	El sistema operativo cuenta con las actualizaciones correspondientes.	El responsable de realizar la revisión es el Mtro. Froylan Hernández Rendón

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

Secretaría Técnica*

Identificador único*	EM011	
Nombre del sistema*	**INGRESSIO**	
Medida de seguridad*	**Acciones***	**Responsable***
Uso de certificados SSL	Debido a que el sistema no requiere de un servidor web para su funcionamiento en red, no se requiere el uso de certificados SSL.	El responsable de las acciones es el Mtro. Froylan Hernández Rendón.

8. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

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

Secretaría Técnica*			
Identificador único*	EM011		
Nombre del sistema*	**INGRESSIO**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Capacitación para la Protección de Datos Personales	Curso en línea	25 horas. Fecha de inicio: 20 de noviembre de 2020. Fecha de término: 17 de enero de 2021	Público objetivo: Enlaces de Transparencia, Responsables de Seguridad de Datos Personales, Responsables de Tecnologías de la Información, así como funcionarios y empleados universitarios.

			Sin vigencia. Sin frecuencia de actualización.
Medidas de Seguridad Técnicas para la Protección de Datos Personales	Curso en línea	25 horas. Fecha de inicio: 8 de febrero de 2021. Fecha de término: 14 de marzo de 2021.	Público objetivo: Enlaces de Transparencia, Responsables de Seguridad de Datos Personales, Responsables de Tecnologías de la Información, así como funcionarios y empleados universitarios. Sin vigencia. Sin frecuencia de actualización.
Elaboración de Documento de Seguridad y Sistema de Gestión de Seguridad de Datos Personales de las áreas universitarias	Curso en línea	25 horas. Fecha de inicio: 25 de marzo de 2022 Fecha de término: 25 de marzo de 2022.	Público objetivo: Enlaces de Transparencia, Responsables de Seguridad de Datos Personales, Responsables de Tecnologías de la Información, así como funcionarios y empleados universitarios. Sin vigencia. Sin frecuencia de actualización.
Solución de incidentes de Red	Curso en línea	20 horas. Fecha de inicio: 19 de abril de 2021 Fecha de término: 16 de mayo de 2021	Público objetivo: Enlaces de Transparencia, Responsables de Seguridad de Datos Personales, Responsables de Tecnologías de la Información, así como funcionarios y empleados universitarios. Sin vigencia. Sin frecuencia de actualización.

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

Secretaría Técnica*			
Identificador único*	EM011		
Nombre del sistema*	**INGRESSIO**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
No se cuenta con un programa de difusión de la protección de datos personales.			

9. MEJORA CONTINUA

9.1. Actualización y mantenimiento de sistemas de información

Secretaría Técnica*			
Identificador único*	EM011		
Nombre del sistema*	**INGRESSIO**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Al ser un Software comercial, no se cuenta con una póliza de mantenimiento ni			

actualizaciones para el mismo.			

9.2. Actualización y mantenimiento de equipo de cómputo

Secretaría Técnica*			
Identificador único*	EM011		
Nombre del sistema*	**INGRESSIO**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
No se han asignado recursos para la actualización del equipo de cómputo			

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

Secretaría Técnica*		
Identificador único*	EM011	
Nombre del sistema*	**INGRESSIO**	
Proceso*	**Descripción***	**Responsable***

Revisión de actualizaciones	Se revisa de manera periódica los cambios en los formatos de las bases de datos, código, etc. Para descartar problemas de compatibilidad entre los aplicativos.	Responsable del proceso: Froylan Hernández Rendón Tiempo de ejecución: 1 día
Para los respaldos de información se cuenta con el documento "Plan de Respaldos ENES Morelia"	El proceso se describe en el documento Plan de respaldos ENES Morelia	*Responsable del proceso: Froylan Hernández Rendón* *Tiempo de ejecución: 1 día*

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

Secretaría Técnica*		
Identificador único*	EM011	
Nombre del sistema*	**INGRESSIO**	
Proceso*	**Descripción***	**Responsable***
El proceso se encuentra contenido en el documento Borrado Seguro ENES Morelia	El proceso se describe en el documento Borrado Seguro ENES Morelia	*Responsable: Froylan Hernández Rendón* *Tiempo de ejecución: 3 días*

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

(Informar y describir el procedimiento para la cancelación de un sistema de tratamiento de datos personales.)[9]

Procedimiento

1.- El Secretario Técnico deberá solicitar la cancelación por escrito al encargado del sistema explicando los motivos y tiempo que deberá permanecer disponible para consulta.

2.-El responsable del sistema deberá realizar la suspensión de las credenciales de acceso al sistema o en su caso, bloquear el apartado inicio de sesión del mismo.

3.- El responsable del sistema deberá notificar al Secretario Técnico de las acciones realizadas para lograr la cancelación temporal del sistema.

4.- Una vez transcurrida la temporalidad en que el sistema quedó bloqueado, el encargado del sistema iniciará la eliminación segura del mismo siguiendo el procedimiento establecido en el documento Borrado seguro ENES Morelia.

5.- El responsable del sistema notificará al Secretario Técnico de que el sistema ha sido cancelado.

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

a) Denominación
b) Motivo de la cancelación

B) PLAZOS Y CONDICIONES PARA EL BLOQUEO DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES:[10]

(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

---

[9] 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.

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

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)

SISTEMA CRONOS

Sistema web que almacena datos personales de los académicos (profesores/as de tiempo completo, ayudantes de profesor, funcionarios administrativos y docentes invitados de otras instituciones externas e internas de la UNAM) para administrar el banco de horas que, semestre a semestre se captura para asignar los horarios del periodo ordinario y exámenes extraordinarios de un semestre lectivo.

Asimismo, se almacena la planta física (aulas virtuales, salones físicos, laboratorios, etc.) de la ENES Unidad Morelia con el fin de asignar (en modo presencial) y administrar los horarios de cada una de las 13 licenciaturas que imparte actualmente la escuela.

También se tiene registro de todos las licenciaturas, posgrados y cursos extracurriculares (formación complementaria, áreas deportivas, mediateca) para administrar los ya mencionados bancos de horas y horarios ya que de este sistema se desprenden otros procesos de carga automática para otros sistemas que operan en la escuela.

ANEXO I: Documento de Seguridad de datos personales

ÍNDICE

INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Secretaría Técnica	
Identificador único*	EM001
Nombre del sistema*	CRONOS (Banco de horas y horarios)
Datos personales (sensibles o no) contenidos en el sistema*:	● Datos personales del académico(a): o Nombre completo (apellido paterno, apellido materno, nombre). o Sexo o Nacionalidad o RFC o CURP o Número de trabajador o Último grado académico o Nombramiento (General) o Domicilio o Teléfono o Correo electrónico *Actualmente únicamente se utiliza en este sistema el correo electrónico de contacto, teléfono ni domicilio no se almacena.
Responsable*:	Escuela Nacional de Estudios Superiores Unidad Morelia
Nombre*:	Dr. Santiago Cortés Hernández
Cargo*:	Secretario Técnico
Funciones*:	Decidir sobre el tratamiento automatizado de los datos personales, así como el contenido, finalidad y uso del sistema.
Obligaciones*:	- Decidir a qué usuarios se le da acceso al sistema con privilegios administrativos. - Decidir sobre la incorporación de nuevas funcionalidades en el sistema. - Vigilar que el sistema cumpla con todas las medidas de seguridad técnicas, físicas y administrativas.
	Encargados[1]:
(Nombre del Encargado 1*)	Lic. Gustavo Cano Salazar

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

Cargo*:	Técnico Académico, responsable del Depto. de Sistemas Informáticos de la ENES Unidad Morelia.
Funciones*:	Análisis, diseño, implementación, mantenimiento, documentación, soporte y capacitación de usuarios, sobre los diversos sistemas informáticos a su cargo en operación de la ENES Unidad Morelia.
Obligaciones*:	● Vigilar la operación correcta del sistema durante el periodo de mayor uso de este (inicios y fin de cada semestre). ● Registrar, actualizar, eliminar datos según requerimiento por escrito de la Secretaría Técnica y/o los usuarios que utilizan el sistema. ● Monitorear la protección de los datos personales contenidos en el sistema mediante la implementación de estrategias y mecanismos de seguridad en su desarrollo y mantenimiento, a nivel interno y externo.
	Usuarios:
(Nombre del Usuario 1*)	Dr. Hernando Alonso Rodríguez Correa
Cargo*:	Secretario Académico / Profesor de Carrera Asociado “C”.
Funciones*:	Revisar el proceso de registro y/o actualización de banco de horas y horarios por parte de los Coordinadores de Área.
Obligaciones*:	Cumplir con la obligación legal de resguardar los datos personales de los académicos/as registrados para impartir clase y/o coadyuvar en la asignación de materias.
(Nombre del Usuario 2*)	Dra. María del Río Francos.
Cargo*:	Coordinadora de Área 1 (Físico-Matemáticas y de las Ingenierías)
Funciones*:	● Captura de banco de horas de académicos(as) para semestre lectivo (área del conocimiento correspondiente). ● Captura de horarios del académico(a) del semestre lectivo. ● Solicitud vía correo electrónico de registro de profesores(as) invitados en sistema y/o agregarlo(a) a una licenciatura. *Nota: El registro de profesores de asignatura, tiempos completos y ayudantes se hacen vía otro sistema que opera con este (Ver: Sistema de contratación Temporal de profesores de asignatura, interinos y ayudantes).
Obligaciones*:	Cumplir con la obligación legal de resguardar los datos personales de los académicos/as registrados para impartir clase y/o coadyuvar en la asignación de materias

	(ayudantes).
(Nombre del Usuario 3*)	Dra. Lucero Sevillano García-Mayeya.
Cargo*:	Coordinadora de Área 2: Ciencias Biológicas y de la Salud
Funciones*:	● Captura de banco de horas de académicos(as) para semestre lectivo (área del conocimiento correspondiente). ● Captura de horarios del académico(a) del semestre lectivo. ● Solicitud vía correo electrónico de registro de profesores(as) invitados en sistema y/o agregarlo(a) a una licenciatura. *Nota: El registro de profesores de asignatura, tiempos completos y ayudantes se hacen vía otro sistema que opera con este (Ver: Sistema de contratación Temporal de profesores de asignatura, interinos y ayudantes).
Obligaciones*:	Cumplir con la obligación legal de resguardar los datos personales de los académicos/as registrados para impartir clase y/o coadyuvar en la asignación de materias (ayudantes).
(Nombre del Usuario 4*)	Dra. Nuri Celene Fuerte Álvarez
Cargo*:	Coordinadora de Área 3: Ciencias Sociales.
Funciones*:	● Captura de banco de horas de académicos(as) para semestre lectivo (área del conocimiento correspondiente). ● Captura de horarios del académico(a) del semestre lectivo. ● Solicitud vía correo electrónico de registro de profesores(as) invitados en sistema y/o agregarlo(a) a una licenciatura. *Nota: El registro de profesores de asignatura, tiempos completos y ayudantes se hacen vía otro sistema que opera con este (Ver: Sistema de contratación Temporal de profesores de asignatura, interinos y ayudantes).
Obligaciones*:	Cumplir con la obligación legal de resguardar los datos personales de los académicos/as registrados para impartir clase y/o coadyuvar en la asignación de materias (ayudantes).
(Nombre del Usuario 5*)	Mtra. Beatriz Alejandra Pimentel Ávila
Cargo*:	Coordinadora del Área 4: Humanidades y Artes.
Funciones*:	● Captura de banco de horas de académicos(as) para semestre lectivo (área del conocimiento correspondiente). ● Captura de horarios del académico(a) del semestre

	lectivo. ● Solicitud vía correo electrónico de registro de profesores(as) invitados en sistema y/o agregarlo(a) a una licenciatura. *Nota: El registro de profesores de asignatura, tiempos completos y ayudantes se hacen vía otro sistema que opera con este (Ver: Sistema de contratación Temporal de profesores de asignatura, interinos y ayudantes).
Obligaciones*:	Cumplir con la obligación legal de resguardar los datos personales de los académicos/as registrados para impartir clase y/o coadyuvar en la asignación de materias (ayudantes).
(Nombre del Usuario 6*)	Mtra. Verónica de los Ángeles López Hernández
Cargo*:	Responsable SUAyED de la ENES Unidad Morelia.
Funciones*:	● Captura de banco de horas de académicos(as) para semestre lectivo (de la Lic. en Admón de Arch. y Gest. Doc. Mod. a Distancia.). ● Captura de horarios del académico(a) del semestre lectivo. ● Solicitud vía correo electrónico de registro de profesores(as) invitados en sistema y/o agregarlo(a) a una licenciatura. *Nota: El registro de profesores de asignatura, tiempos completos y ayudantes se hacen vía otro sistema que opera con este (Ver: Sistema de contratación Temporal de profesores de asignatura, interinos y ayudantes).
Obligaciones*:	Cumplir con la obligación legal de resguardar los datos personales de los académicos/as registrados para impartir clase y/o coadyuvar en la asignación de materias (ayudantes).
Obligaciones*:	Cumplir con la obligación legal de resguardar los datos personales de los académicos/as registrados para impartir clase y/o coadyuvar en la asignación de materias (ayudantes).
(Nombre del Usuario 7*)	Mtra. Melba Selene Cardoso Gómez
Cargo*:	Coordinadora del Departamento de Idiomas.
Funciones*:	● Captura de banco de horas de académicos(as) para semestre lectivo (asignaturas de inglés de cada plan de estudio de las licenciaturas de la ENES Unidad Morelia). ● Captura de horarios del académico(a) del semestre lectivo. ● Solicitud vía correo electrónico de registro de profesores(as) invitados en sistema y/o agregarlo(a) a

	una licenciatura. *Nota: El registro de profesores de asignatura, tiempos completos y ayudantes se hacen vía otro sistema que opera con este (Ver: Sistema de contratación Temporal de profesores de asignatura, interinos y ayudantes).
Obligaciones*:	● Cumplir con la obligación legal de resguardar los datos personales de los académicos/as registrados para impartir clase y/o coadyuvar en la asignación de materias (ayudantes).
(Nombre del Usuario 8*)	Mtra. Bertha Karina Godina Sepúlveda
Cargo*:	Coordinadora Centro de Auto acceso y Mediateca.
Funciones*:	● Captura de banco de horas de académicos(as) para semestre lectivo (área idiomas complementarios a inglés y Mediateca). ● Solicitud vía correo electrónico de registro de profesores(as) invitados en sistema y/o agregarlo(a) a una licenciatura. *Nota: El registro de profesores de asignatura, tiempos completos y ayudantes se hacen vía otro sistema que opera con este (Ver: Sistema de contratación Temporal de profesores de asignatura, interinos y ayudantes).
Obligaciones*:	● Cumplir con la obligación legal de resguardar los datos personales de los académicos/as registrados para impartir clase y/o coadyuvar en la asignación de materias (ayudantes).
(Nombre del Usuario 9*)	Lic. María Dolores Rodríguez Guzmán
Cargo*:	Coordinadora de Atención a la Comunidad
Funciones*:	● Captura de banco de horas de académicos(as) para semestre lectivo (área de actividades deportivas). ● Solicitud vía correo electrónico de registro de profesores(as) invitados en sistema y/o agregarlo(a) a una licenciatura. *Nota: El registro de profesores de asignatura, tiempos completos y ayudantes se hacen vía otro sistema que opera con este (Ver: Sistema de contratación Temporal de profesores de asignatura, interinos y ayudantes).
Obligaciones*:	● Cumplir con la obligación legal de resguardar los datos personales de los académicos/as registrados para impartir clase y/o coadyuvar en la asignación de materias (ayudantes).

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

Secretaría Técnica	
Identificador único*	EM001
Nombre del sistema*	CRONOS (Sistema de Banco de Horas y Horarios)
Tipo de soporte[2]:*	Electrónico
Descripción[3]:*	Para almacenamiento de datos se utiliza un Sistema Gestor de Bases de Datos relacional y para informes ejecutivos y reportes se generan archivos separados por comas, archivos de la suite de Microsoft y formato de documentos portátiles.
[redacted]	

Eliminado: Información específica sobre el lugar donde se resguardan los soportes de la información.

Fundamentación: De conformidad con 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 los artículos 32 y 36 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

Motivación: En virtud de que estos datos hace identificable las formas en que es posible atacar o vulnerar nuestros sistemas de información que resguardan datos personales y 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.

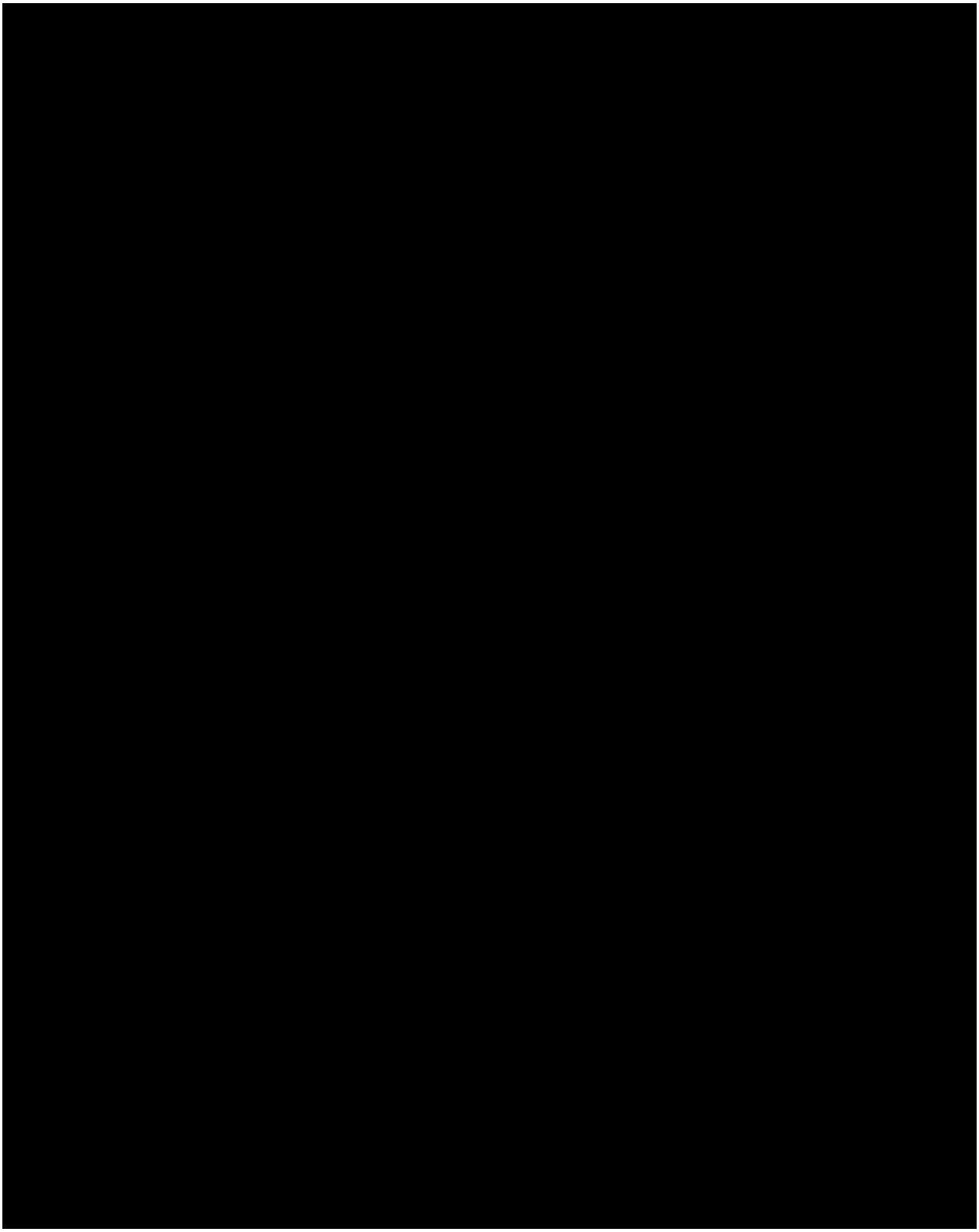
[2] En caso de que el área universitaria prevea cambiar el tipo de soporte que utiliza el sistema de tratamiento de datos personales por ejemplo de físico a electrónico o en el supuesto de que prevea en el futuro utilizar ambos tipos de soportes, deberá indicarse en este rubro.

[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



[redacted]

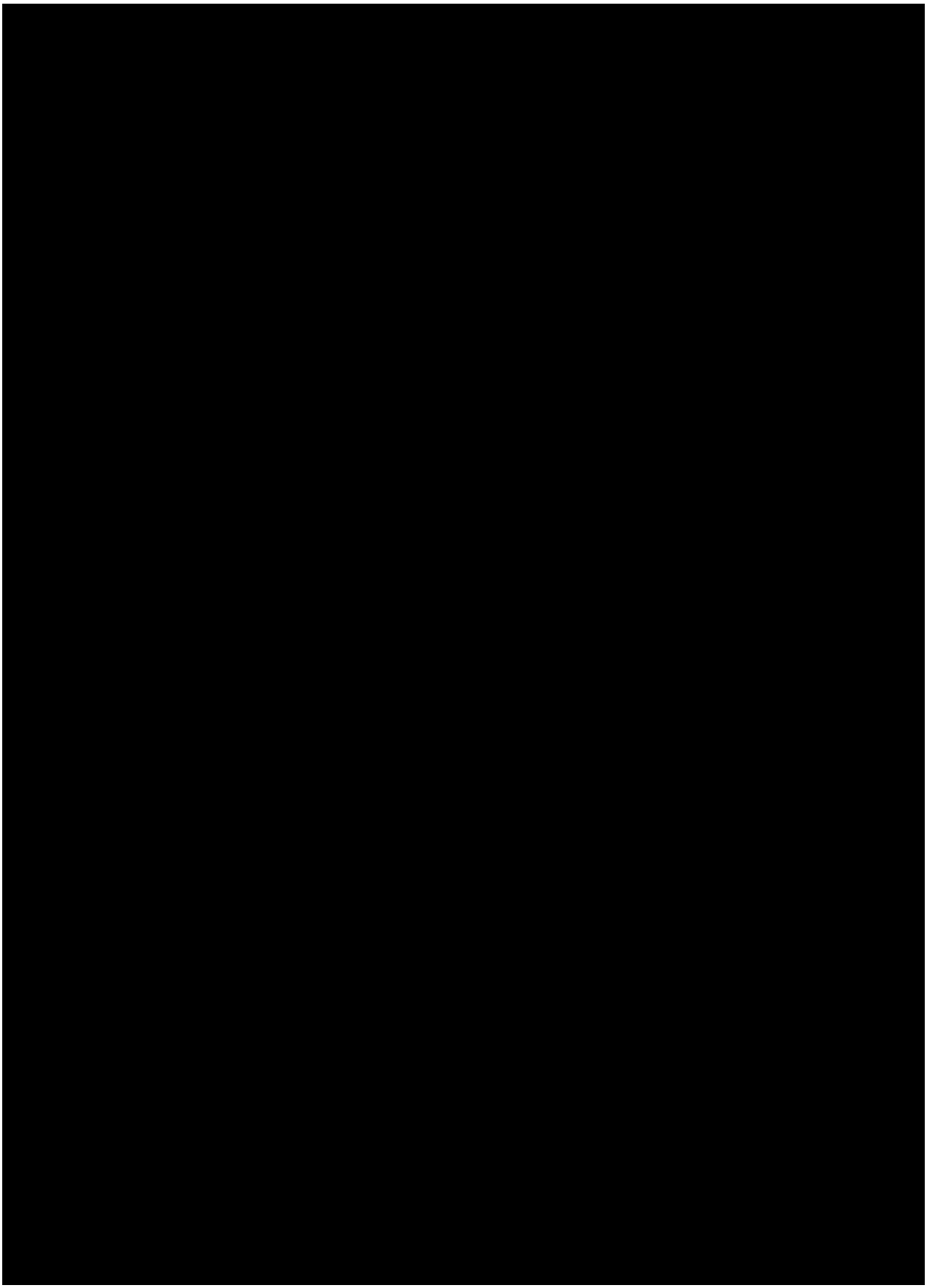
Eliminado: Análisis de riesgos.

Fundamentación: De conformidad con 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 los artículos 32 y 36 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

Motivación: En virtud de que estos datos hace identificable las formas en que es posible atacar o vulnerar nuestros sistemas de información que resguardan datos personales y 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.

4. ANÁLISIS DE BRECHA

[redacted]



[redacted]

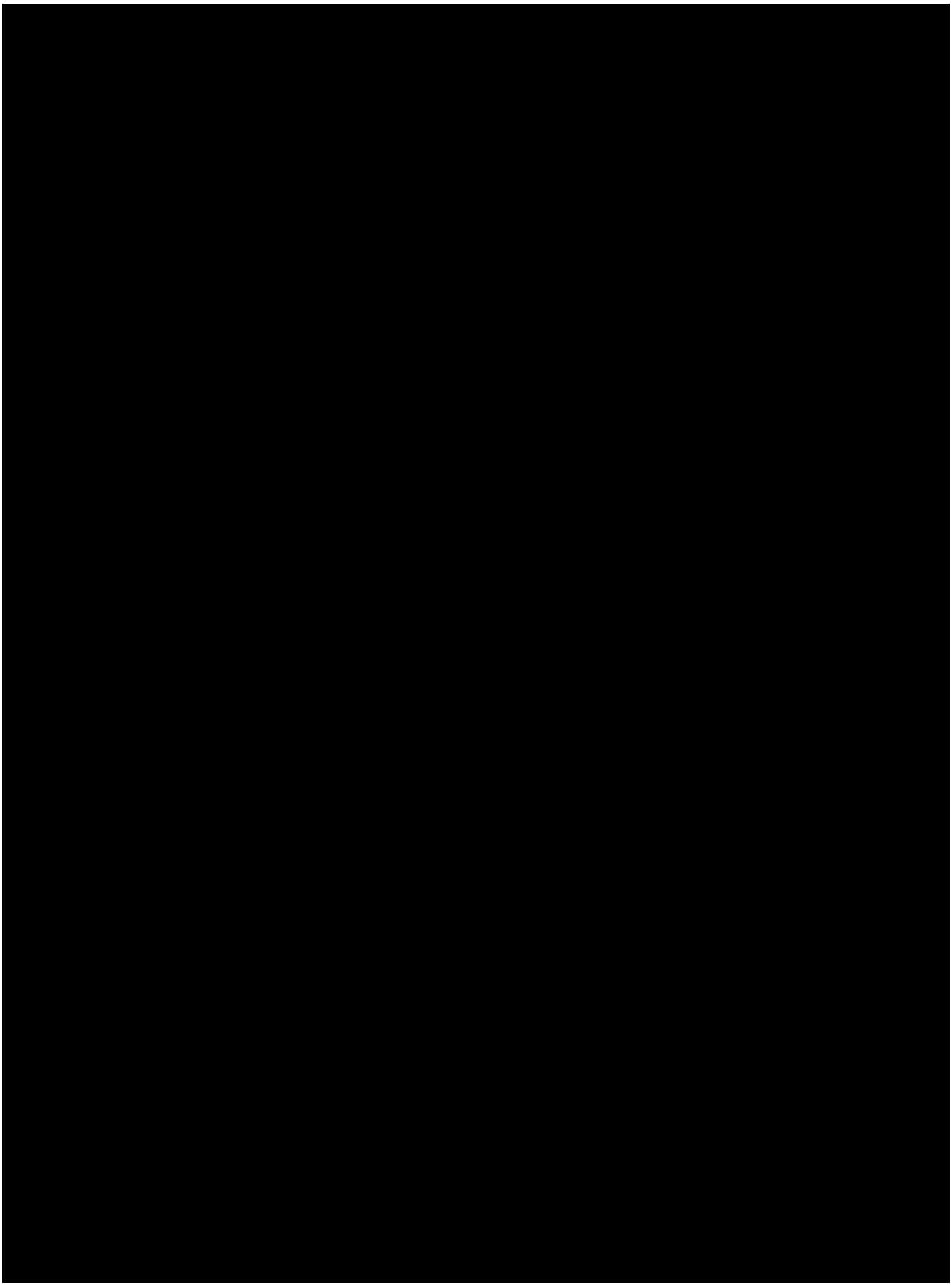
Eliminado: Análisis de brecha.

Fundamentación: De conformidad con 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 los artículos 32 y 36 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

Motivación: En virtud de que estos datos hace identificable las formas en que es posible atacar o vulnerar nuestros sistemas de información que resguardan datos personales y 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.

5. PLAN DE TRABAJO

[redacted]



[redacted]

Eliminado: Plan de trabajo.

Fundamentación: De conformidad con 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 los artículos 32 y 36 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

Motivación: En virtud de que estos datos hace identificable las formas en que es posible atacar o vulnerar nuestros sistemas de información que resguardan datos personales y 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.

6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

I. TRANSFERENCIAS DE DATOS PERSONALES

Secretaría Técnica*	
Identificador único*	EM001
(Nombre del sistema A1)*	CRONOS (Sistema de Banco de Horas y Horarios)
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:[5]	No se realizan transferencias de datos personales mediante el traslado de soportes físicos.
Transferencias mediante el traslado de soportes electrónicos:	Para el presente sistema la transferencia de datos personales se hace a través del usuario ADMINISTRADOR, Secretaría Académica y Coordinadores con el privilegio de descarga de informes ejecutivos y/o reportes en archivos de la suite de Microsoft y de formato de documentos portátiles.
Transferencias mediante el traslado sobre redes electrónicas:	Actualmente no se cuenta con una infraestructura privada de almacenamiento (nube) en la ENES Unidad Morelia.

[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.

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]
2. Señalar en un listado las personas (nombre, cargo, funciones y obligaciones) que tienen acceso a los soportes físicos del sistema.[7]

El sistema CRONOS no realiza transferencia de datos personales en soportes físicos ya que todo el resguardo de los datos se hace mediante soporte electrónico mediante el uso de bases de datos relacionales y su descarga a través de hojas de cálculo y archivos de formato portátil.

II. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

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

[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:

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

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

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.

El sistema CRONOS actualmente no cuenta con un registro de bitácoras de acceso y operación cotidiana.

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 cuenta con un procedimiento de atención de incidentes.

---

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.

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:

a) ¿Cómo las identifica?

No se cuenta con mecanismos de identificación.

b) ¿Cómo las autentifica?

No se cuenta con mecanismos de autenticación.

c) ¿Cómo les autoriza el acceso?

No se cuenta con mecanismos de control de acceso.

---

[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.

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

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

Para las personas que acceden a dichos espacios interiores:

1. ¿Cómo las identifica?
   Se tiene definida una lista de acceso para el personal autorizado.
2. ¿Cómo las autentifica?
   Mediante credencial y número de trabajador.
3. ¿Cómo les autoriza el acceso?
   Si se encuentran en la lista de acceso autorizada, o si son proveedores acompañados por un empleado autorizado. Se les solicita se registren en la bitácora correspondiente.

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

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

En caso de detectar error y/o realizar alguna actualización de datos personales del académico se tienen dos procedimientos:

El procedimiento lo realiza únicamente el administrador del sistema, donde mediante un correo electrónico escrito a la cuenta del responsable del sistema de tratamiento de datos personales se indica la corrección y/o actualización del o los datos personales a procesar y una vez realizado, el responsable responde a vuelta de correo electrónico el ajuste realizado y solicita la verificación del mismo en sistema de los datos actualizados o corregidos.

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

VII. PERFILES DE USUARIO Y CONTRASEÑAS

1. Modelo de control de acceso:

Basado en perfiles o privilegios de acceso (permisos).

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?
Únicamente las contraseñas.

4. Administración de perfiles de usuario y contraseñas:

a) ¿Quién da de alta nuevos perfiles?
El Responsable del sistema a su cargo. Lic. Gustavo Cano Salazar.

b) ¿Quién autoriza la creación de nuevos perfiles?
El Secretario Técnico autoriza la creación de nuevos perfiles con privilegios administrativos.

c) ¿Se lleva registro de la creación de nuevos perfiles?
Mediante control interno del Departamento de Sistemas Informáticos y a través del sistema.

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

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

b) ¿Requiere el administrador acceso remoto al equipo donde reside el sistema para realizar tareas de mantenimiento?
Si, con acceso mediante VPN.

c) ¿Cómo se evita el acceso remoto no autorizado?

- Se cuenta con controles de acceso basados en roles y privilegios.
- El acceso remoto a los servidores se realiza mediante conexiones VPN habilitadas únicamente a los responsables de los sistemas.
- Implementación de captcha en el inicio de sesión del sistema.

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

1. Señalar si realiza respaldos
   a) Completos_X_, diferenciales ___ o incrementales__X_;
   b) De forma automática ____ o Manual _X_,
   c) Periodicidad con que los realiza: _Semestral_

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 externo.
3. Cómo y dónde archiva esos medios, y Consultar los documentos: Plan de respaldos ENES Morelia y Bitácora de control de los respaldos.
4. Quién es el responsable de realizar estas operaciones (el área universitaria o un tercero). El responsable (encargado) del sistema a su cargo.

IX. PLAN DE CONTINGENCIA

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

   Se cuenta con algunas medidas como las especificadas en el documento: Medidas de seguridad en los periodos de inactividad o mantenimiento, pero no se tiene desarrollado el plan de contingencia.
2. Si cuenta con plan de contingencia y lo ha implementado, deberá indicar si realiza pruebas de eficiencia de este.

   No se cuenta con plan de contingencia.
3. Informar si cuenta con un sitio redundante (alterno) y señalar lo siguiente:
   a) El tipo de sitio (caliente, tibio o frío);[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.

Actualmente la ENES Unidad Morelia, no cuenta con sitio redundante para cubrir los incisos anteriores.

[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.

[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.

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*		
Identificador único*	EM001	
Nombre del sistema*	CRONOS (Sistema de Banco de Horas y Horarios)	
Recurso*	**Descripción***	**Control***
Reportes especiales de datos almacenados en el sistema.	Al solicitar reportes que no se encuentran en el sistema y su descarga en soporte electrónico, estos se generan y se descargan mediante un vínculo que vence en determinado tiempo para su descarga.	Evitar adjuntar archivos por correo electrónico porque es un servicio de terceros (Google). Una vez vencido el plazo de descarga (max. 24 horas) es imposible volver a descargar el soporte electrónico solicitado,
Reportes especiales de datos almacenados en el sistema en soportes electrónicos adjuntos por correo electrónico.	Solicitud de reportes especiales entregados en un soporte electrónico específico y que se piden se adjunten por correo electrónico.	Se utiliza programa de distribución libre para cifrar el archivo y personalmente se indica la contraseña para descifrarlo en el equipo de cómputo del usuario para utilizar el archivo que fue adjuntado por correo electrónico.

7.2 Procedimiento para la revisión de las medidas de seguridad

Secretaría Técnica*

Identificador único*	EM001	
Nombre del sistema*	CRONOS (Sistema de Banco de Horas y Horarios)	
Medida de seguridad*	**Procedimiento***	**Responsable***
Principio del menor privilegio	Otorgar el acceso al usuario autorizado por la Secretaría técnica de acuerdo con el permiso requerido.	Encargado del sistema. Lic. Gustavo Cano Salazar. (01 día hábil).
Respaldos del sistema y base de datos.	Generación de archivos de respaldo tanto del sistema web como de la base de datos y control de bitácoras de respaldo.	Encargado del sistema. Lic. Gustavo Cano Salazar. (01 día hábil).
Sincronizar la fecha y hora con el servidor NTP (Network Time Protocol) oficial de la UNAM	Revisiones periódicas de la hora y fecha del servidor donde se encuentra el sistema.	Mtro. Froylán Hernández Rendón (01 día hábil).
Instalar y mantener actualizado el software antimalware.	Revisión y actualización de la versión del software antivirus y de la base de datos.	Mtro. Froylán Hernández Rendón (01 día hábil).
Instalar las actualizaciones de seguridad más recientes disponibles.	Revisión y actualizaciones del sistema operativo.	Mtro. Froylán Hernández Rendón (02 días hábiles).

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

Secretaría Técnica*		
Identificador único*	EM001	
Nombre del sistema*	CRONOS (Sistema de Banco de Horas y Horarios)	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***
Principio del menor privilegio	Se encontró que todas las cuentas de usuarios del	Encargado del sistema. Lic. Gustavo Cano Salazar.

	sistema cuentan con los permisos correspondientes.	
Respaldo del sistema y base de datos.	Se cuenta con respaldos actualizados de la información del sistema.	Encargado del sistema. Lic. Gustavo Cano Salazar.
Sincronizar la fecha y hora con el servidor NTP (Network Time Protocol) oficial de la UNAM	La fecha y hora están sincronizadas con el servidor NTP de la UNAM.	Mtro. Froylán Hernández Rendón.
Instalar y mantener actualizado el software antimalware.	El Software antivirus está actualizado.	Mtro. Froylán Hernández Rendón.
Instalar las actualizaciones de seguridad más recientes disponibles.	El sistema operativo cuenta con las actualizaciones correspondientes.	Mtro. Froylán Hernández Rendón.

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

Secretaría Técnica*		
Identificador único*	EM001	
Nombre del sistema*	CRONOS (Banco de Horas y Horarios)	
Medida de seguridad*	**Acciones***	**Responsable***
Uso de certificados SSL	Implementar el protocolo “HTTPS” en el sistema. Realizar la renovación anual del certificado SSL para el subdominio donde se encuentra el sistema.	Mtro. Froylán Hernández Rendón

8 PROGRAMA ESPECÍFICO DE CAPACITACIÓN

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

Secretaría Técnica*			
Identificador único*	EM001		
Nombre del sistema*	CRONOS (Sistema de Banco de Horas y Horarios)		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Capacitación para la Protección de Datos Personales	Curso en línea	25 horas. Fecha de inicio: 20 de noviembre de 2020. Fecha de término: 17 de enero de 2021	Público objetivo: Enlaces de Transparencia, Responsables de Seguridad de Datos Personales, Responsables de Tecnologías de la Información, así como funcionarios y empleados universitarios. Sin vigencia. Sin frecuencia de actualización.
Medidas de Seguridad Técnicas para la Protección de Datos Personales	Curso en línea	25 horas. Fecha de inicio: 8 de febrero de 2021. Fecha de término: 14 de marzo de 2021.	Público objetivo: Enlaces de Transparencia, Responsables de Seguridad de Datos Personales, Responsables de Tecnologías de la Información, así como funcionarios y empleados universitarios. Sin vigencia. Sin frecuencia de actualización.

Elaboración de Documento de Seguridad y Sistema de Gestión de Seguridad de Datos Personales de las áreas universitarias	Curso en línea	25 horas. Fecha de inicio: 25 de marzo de 2022 Fecha de término: 25 de marzo de 2022.	Público objetivo: Enlaces de Transparencia, Responsables de Seguridad de Datos Personales, Responsables de Tecnologías de la Información, así como funcionarios y empleados universitarios. Sin vigencia. Sin frecuencia de actualización.
La importancia de la protección de datos personales	Seminario en línea	1 hora. Fecha: 16 de junio de 2022.	Público en general. Sin vigencia. Sin frecuencia de actualización.

8.2 Programa de difusión de la protección a los datos personales

Secretaría Técnica*			
Identificador único*	EM001		
Nombre del sistema*	CRONOS (Sistema de Banco de Horas y Horarios)		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Indique actividad, tema, recursos para la difusión. Agregar un renglón por cada elemento	*Describa el tipo de elemento, sus objetivos y forma de impartición, publicación o distribución*	*Indique duración del elemento en horas, días, meses, su fecha de inicio y de término*	*Mencione público objetivo, vigencia del elemento y frecuencia de actualización*

Actualmente, no se cuenta con un programa de difusión de la protección de datos personales.

9 MEJORA CONTINUA

9.1 Actualización y mantenimiento de sistemas de información

Secretaría Técnica*			
Identificador único*	EM001		
Nombre del sistema*	CRONOS (Sistema de Banco de Horas y Horarios)		
Actividad*	**Descripción***	**Duración ***	**Cobertura***
Actualización de tecnologías de desarrollo	1.Solicitud de actualización de la arquitectura de desarrollo del sistema. 2. Corregir y/o actualizar módulos del sistema. 3. Pruebas unitarias e integrales de las actualizaciones realizadas al sistema. 4. Actualización de archivos de sistema y/o sentencias de bases de datos en servidor de producción.	12 meses	“Back-end” del sistema.

9.2 Actualización y mantenimiento de equipo de cómputo

Secretaría Técnica*	
Identificador único*	EM001

Nombre del sistema*	CRONOS (Sistema de banco de horas y horarios).		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Indique actividad. Agregar un renglón por cada elemento	*Describa el tipo de actividad, sus objetivos e impacto la actualización o mantenimiento del equipo de cómputo*	*Indique duración en la ejecución de la actividad en horas, días, meses, su fecha de inicio y de término*	*Mencione los aspectos de equipo de cómputo que son resueltos, total o parcialmente, por la actividad.*

Actualmente, no se han asignado recursos para la actualización del equipo de cómputo.

9.3 Procesos para la conservación, preservación y respaldos de información

Secretaría Técnica*		
Identificador único*	EM001	
Nombre del sistema*	CRONOS (Sistema de banco de horas y horarios).	
Proceso*	**Descripción***	**Responsable***
Poner en fase de “mantenimiento” del sistema.	Se coloca un mensaje en la parte de acceso al sistema con un aviso de “mantenimiento” y de ser posible la fecha de “regreso” a la operación del sistema.	Encargado del sistema: Lic. Gustavo Cano Salazar. (01 día hábil).
Ingresar remotamente al servidor.	Acceso mediante SSH al servidor de manera remota para realizar el respaldo de ambos componentes (script	Encargado del sistema: Lic. Gustavo Cano Salazar. (01 día hábil).

	del sistema y de la base de datos)	
Descarga de respaldos del sistema a soporte físico electrónico.	Descarga directa al Disco Duro externo proporcionado por secretaría técnica con los respaldos realizados del sistema.	Encargado del sistema: Lic. Gustavo Cano Salazar. (01 día hábil).
Salida del servidor y de fase de “mantenimiento” en el sistema.	Quitar el mensaje del modo mantenimiento del sistema y salida completa del servidor.	Encargado del sistema: Lic. Gustavo Cano Salazar. (01 día hábil).
El proceso de respaldo de información se encuentra contenido en el documento: Plan de respaldos ENES Morelia	El proceso se describe en el documento: Plan de respaldos ENES Morelia	Encargado del sistema: Lic. Gustavo Cano Salazar. (01 día hábil).

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

Secretaría Técnica*		
Identificador único*	EM001	
(Nombre del sistema A1)*	CRONOS (Sistema de banco de horas y horarios)	
Proceso*	**Descripción***	**Responsable***
Borrado de datos mediante sistema (jnterfaz).	En la interfaz se tienen habilitadas opciones de “Actualizar y/o borrar datos” para los usuarios del sistema.	Encargado del sistema: Lic. Gustavo Cano Salazar.

Borrado de datos dentro del Sistema Gestor de Base de Datos.	Aplicación de transacciones y ejecución de instrucciones SQL para actualización y/o borrado de datos. Una vez completada la transacción aplicar la instrucción correspondiente para conservar o borrar definitivamente los datos.	Encargado del sistema: Lic. Gustavo Cano Salazar.
El proceso se encuentra contenido en el documento: Borrado Seguro ENES Morelia	El proceso se describe en el documento: Borrado Seguro ENES Morelia	Borrado seguro: Encargado del sistema: Lic. Gustavo Cano Salazar. Responsable de la disposición final de equipos o componentes de cómputo: Mtro. Froylán Hernández Rendón Tiempo máximo de ejecución: 05 días hábiles.

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

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

(Informar y describir el procedimiento para la cancelación de un sistema de tratamiento de datos personales.)[13]

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

a) Denominación
b) Motivo de la cancelación

B) PLAZOS Y CONDICIONES PARA EL BLOQUEO DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES:[14]

(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)

PROCEDIMIENTO PARA LA SUPRESIÓN DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

[13] 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.

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

SISTEMA ESCOLARES

Sistema web que realiza los procesos de inscripción en línea de los alumnos(as) que estudian una licenciatura en la ENES Unidad Morelia de la UNAM, tanto en sistema escolarizado como a distancia. Abarca los dos tipos de periodos que se manejan en el semestre en la UNAM (ordinario y extraordinario), obteniendo al final, un comprobante de inscripción en algún tipo de periodo en que el alumno(a) haya realizado el registro de al menos una asignatura en el semestre lectivo.

Este sistema se comunica con el sistema anterior (CRONOS) ya que se realiza la exportación de datos de profesores, horarios para su registro en el presente sistema y que los alumnos(as) puedan inscribir las materias a cursar y/o presentar exámenes en tiempo extraordinario.

Este sistema resguarda principalmente todos los datos personales del alumno(a) y algunos datos personales del profesor para que se identifique mediante este sistema las relaciones grupo-asignatura-profesor.

Asimsimo, dependiendo del rol o tipo de usuario dentro del sistema se verán algunos datos personales del alumno (principalmente) con el fin de atender los diferentes procesos que se llevan a cabo en el Departamento de Servicios Escolares de la Escuela.

ANEXO I: Documento de Seguridad de datos personales

ÍNDICE

INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Secretaría Técnica	
Identificador único*	EM002
Nombre del sistema*	ESCOLARES
Datos personales (sensibles o no) contenidos en el sistema*:	● Datos personales del alumno(a): o Nombre completo (apellido paterno, apellido materno, nombre) o Número de cuenta o Nacionalidad o Tipo de discapacidad o Si se encuentra en reclusión o Si realizó examen en el extranjero o Entidad federativa de procedencia o Sexo o Fecha de nacimiento o CURP o Domicilio (Calle, número exterior e interior, colonia, entidad, delegación o municipio, código postal) o Teléfono 1 (fijo o móvil) o Teléfono 2 (fijo o móvil) o Correo electrónico. o Número de seguridad social (IMSS) o Nombre completo del beneficiario o Teléfono del beneficiario o Nombre del Padre o Tutor responsable o Teléfono móvil del padre o tutor responsable o Nombre de la madre o Teléfono móvil de la madre. o Tipo de sangre. o Alergias o Si tiene trabajo ● Datos académicos del alumno(a): o Licenciatura o Plan de estudios o Generación o Aplicación de art 22 o Comprobante de inscripción del alumno(a) o Status del alumno. ● Datos personales del académico(a) o Nombre completo (apellido paterno, apellido materno, nombre) o RFC

	○ CURP ○ Sexo ○ Grado académico ○ Número de trabajador ○ Nacionalidad ○ Nombramiento ○ Contraseña
Responsable*:	Escuela Nacional de Estudios Superiores Unidad Morelia
Nombre*:	Dr. Santiago Cortés Hernández
Cargo*:	Secretario Técnico
Funciones*:	Decidir sobre el tratamiento automatizado de los datos personales, así como el contenido, finalidad y uso del sistema.
Obligaciones*:	- Decidir a qué usuarios se le da acceso al sistema con privilegios administrativos. - Decidir sobre la incorporación de nuevas funcionalidades en el sistema. - Vigilar que el sistema cumpla con todas las medidas de seguridad técnicas, físicas y administrativas.
	Encargados[1]:
(Nombre del Encargado 1*)	Lic. Gustavo Cano Salazar
Cargo*:	Técnico Académico, responsable del Depto. de Sistemas Informáticos de la ENES Unidad Morelia.
Funciones*:	Análisis, diseño, implementación, mantenimiento, documentación, soporte y capacitación de usuarios, sobre los diversos sistemas informáticos a su cargo en operación de la ENES Unidad Morelia.
Obligaciones*:	● Vigilar la operación correcta del sistema durante el periodo de mayor uso de este (inicios y fin de cada semestre). ● Registrar, actualizar, eliminar datos según requerimiento por escrito de la Secretaría Técnica y/o los usuarios que utilizan el sistema. ● Monitorear la protección de los datos personales contenidos en el sistema mediante la implementación de estrategias y mecanismos de seguridad en su desarrollo y mantenimiento, a nivel interno y externo.
	Usuarios:

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

(Nombre del Usuario 1*)	Lic. Alejandro Rebollar Villagómez.
Cargo*:	Jefe del Depto. de Servicios Escolares (Administrativo)
Funciones*:	Vigilar, dirigir y controlar los procesos de trámites que se realizan en el Departamento de Servicios Escolares a través de sus colaboradores consultando para ello, los datos personales y/o académicos de los alumnos de la ENES Unidad Morelia.
Obligaciones*:	Cumplir con la obligación legal de resguardar los datos personales de los alumnos(as) registrados en el sistema utilizando la información con fines administrativos.
(Nombre del Usuario 2*)	Mtro. Mauricio Ríos Rojas
Cargo*:	Oficinista del Departamento de Servicios Escolares.
Funciones*:	▪ Consulta de datos personales del alumno(a) para trámite de constancias de estudios y credenciales del plantel. ▪ Consulta de datos académicos del alumno(a) para trámites diversos del departamento. ▪ Apertura de sistema informático extemporáneo para permitir registro de asignaturas del semestre. ▪ Visualización de listados de alumnos(as) inscritos para apoyo académico a profesores/as.
Obligaciones*:	Cumplir con la obligación legal de resguardar los datos personales de los alumnos(as) registrados en el sistema utilizando la información con fines administrativos.
(Nombre del Usuario 3*)	Lic. Verónica Janette Chávez Hernández.
Cargo*:	Oficinista del Departamento de Servicios Escolares.
Funciones*:	▪ Consulta de datos personales del alumno(a) para trámite de constancias de estudios y credenciales del plantel. ▪ Consulta de datos académicos del alumno(a) para trámites de certificados de estudios. ▪ Apertura de sistema informático extemporáneo para permitir registro de asignaturas del semestre. ▪ Visualización de listados de alumnos(as) inscritos para apoyo académico a profesores/as.
Obligaciones*:	Cumplir con la obligación legal de resguardar los datos personales de los alumnos(as) registrados en el sistema utilizando la información con fines administrativos.

(Nombre del Usuario 4*)	Lic. Silvia Ramírez Flores
Cargo*:	Asistente del Departamento de Servicios Escolares
Funciones*:	▪ Consulta de datos personales del alumno(a) para trámite de constancias de estudios y credenciales del plantel. ▪ Consulta de datos académicos del alumno(a) para trámites de programas de becas. ▪ Apertura de sistema informático extemporáneo para permitir registro de asignaturas del semestre. ▪ Visualización de listados de alumnos(as) inscritos para apoyo académico a profesores/as.
Obligaciones*:	Cumplir con la obligación legal de resguardar los datos personales de los alumnos(as) registrados en el sistema utilizando la información con fines administrativos.
(Nombre del Usuario 5*)	Mtro. Agustín Martínez Morales
Cargo*:	Administrativo del área de Titulaciones.
Funciones*:	▪ Consulta de datos personales del alumno(a) para trámite de constancias de estudios y credenciales del plantel. ▪ Consulta de datos académicos del alumno(a) para trámites y seguimiento a titulaciones. ▪ Apertura de sistema informático extemporáneo para permitir registro de asignaturas del semestre. ▪ Visualización de listados de alumnos(as) inscritos para apoyo académico a profesores/as.
Obligaciones*:	Cumplir con la obligación legal de resguardar los datos personales de los alumnos(as) registrados en el sistema utilizando la información con fines administrativos.
(Nombre del Usuario 6*)	Coordinadores de Área.
Cargo*:	Coordinadores de las licenciaturas según área de conocimientos.
Funciones*:	● Visualización de asignaturas exportadas desde sistema CRONOS. ● Listas de inscritos exportados a archivos PDF para apoyo a los académicos. ● Estos Coordinadores de Área NO visualizan ningún dato personal tanto de los alumnos como de los académicos. ● Estos Coordinadores de Área son los mismos descritos

	en el sistema anterior (CRONOS).
Obligaciones*:	Cumplir con la obligación legal de resguardar los datos personales de los alumnos(as) y académicos/as registrados para impartir clase y/o coadyuvar en la asignación de materias (ayudantes).
(Nombre del Usuario 7*)	Coordinadores de Licenciatura
Cargo*:	Coordinación de profesores y asignaturas de la licenciatura que apoyan.
Funciones*:	● Visualización de asignaturas exportadas desde sistema CRONOS. ● Listas de inscritos exportados a formato de documento portátil para apoyo a los académicos. ● Estos Coordinadores de Licenciatura NO visualizan ningún dato personal tanto de los alumnos como de los académicos. ● Solo se visualizan las asignaturas correspondientes a la Coordinación de Licenciatura que manejan y son puestos que van rotando generalmente cada año.
Obligaciones*:	Cumplir con la obligación legal de resguardar los datos personales de los alumnos(as) y académicos/as registrados para impartir clase y/o coadyuvar en la asignación de materias (ayudantes).

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

Secretaría Técnica	
Identificador único*	EM002
Nombre del sistema*	ESCOLARES
Tipo de soporte[2]:*	Electrónico
Descripción[3]:*	Para almacenamiento de datos se utiliza un Sistema Gestor de Bases de Datos relacional y para informes ejecutivos y reportes se generan archivos separados por comas, hojas de cálculo y formato de documento portátil.

[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.

[redacted]

Eliminado: Información específica sobre el lugar donde se resguardan los soportes de la información.

Fundamentación: De conformidad con 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 los artículos 32 y 36 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

Motivación: En virtud de que estos datos hace identificable las formas en que es posible atacar o vulnerar nuestros sistemas de información que resguardan datos personales y 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.

3. ANÁLISIS DE RIESGOS

[redacted]

[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.

[redacted]

Eliminado: Análisis de riesgos.

Fundamentación: De conformidad con 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 los artículos 32 y 36 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

Motivación: En virtud de que estos datos hace identificable las formas en que es posible atacar o vulnerar nuestros sistemas de información que resguardan datos personales y 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.

[redacted]

4. ANÁLISIS DE BRECHA

[redacted]

[redacted]

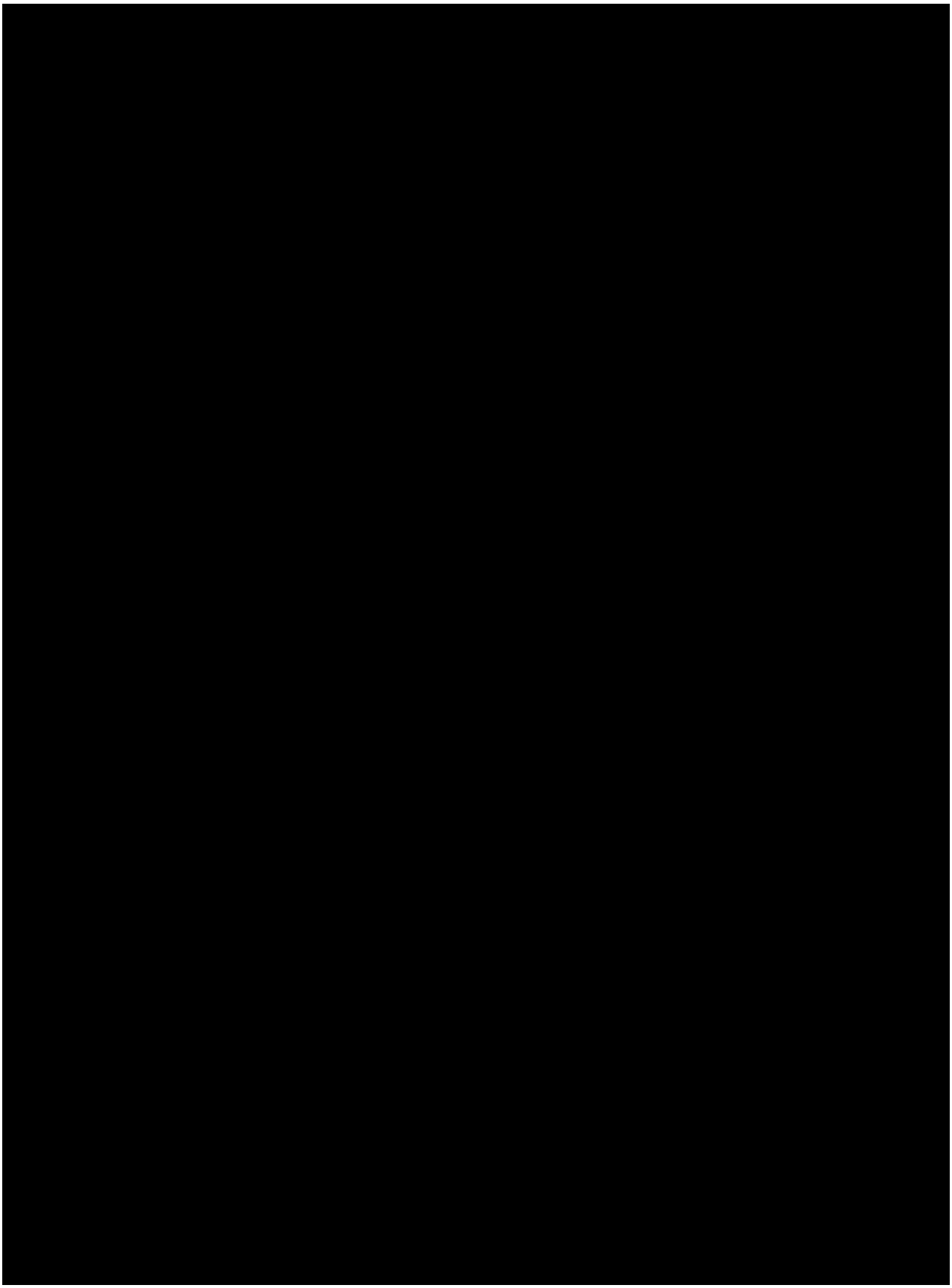
Eliminado: Análisis de brecha.

Fundamentación: De conformidad con 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 los artículos 32 y 36 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

Motivación: En virtud de que estos datos hace identificable las formas en que es posible atacar o vulnerar nuestros sistemas de información que resguardan datos personales y 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.

5. PLAN DE TRABAJO

[redacted]



[redacted]

Eliminado: Plan de trabajo.

Fundamentación: De conformidad con 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 los artículos 32 y 36 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

Motivación: En virtud de que estos datos hace identificable las formas en que es posible atacar o vulnerar nuestros sistemas de información que resguardan datos personales y 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.

6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

I. TRANSFERENCIAS DE DATOS PERSONALES

Secretaría Técnica*	
Identificador único*	EM002
(Nombre del sistema A1)*	ESCOLARES
TRANSFERENCIAS DE DATOS PERSONALES	

Transferencias mediante el traslado de soportes físicos:[5]	No se realizan transferencias de datos personales mediante el traslado de soportes físicos.
Transferencias mediante el traslado de soportes electrónicos:	La transferencia de datos personales se hace a través del usuario ADMINISTRADOR, Colaboradores (Área y Licenciatura) con el privilegio de descarga de informes ejecutivos y/o reportes en formato de documento portátil y hoja de cálculo (según el permiso).
Transferencias mediante el traslado sobre redes electrónicas:	Actualmente no se cuenta con una infraestructura privada de almacenamiento (nube) en la ENES Unidad Morelia.

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]
2. Señalar en un listado las personas (nombre, cargo, funciones y obligaciones) que tienen acceso a los soportes físicos del sistema.[7]

El sistema ESCOLARES no realiza transferencia de datos personales en soportes físicos ya que todo el resguardo de los datos se hace mediante soporte electrónico mediante el uso de bases de datos relacionales y su descarga a través de hojas de cálculo formato de documentos portables.

II. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

[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.

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

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

[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:

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.

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
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.

El sistema ESCOLARES, actualmente cuenta con una bitácora parcial donde se almacena cierta actividad de los usuarios que ingresan al sistema, pero que de manera general, no cubren con la información necesaria que indique a detalle la actividad del usuario dentro del sistema.

III. REGISTRO DE INCIDENTES:

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

No se cuenta con un procedimiento de atención de incidentes.

1. Los datos que registra:
   a) La persona que resolvió el incidente;
   b) La metodología aplicada;[10]

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

[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.

c) Para soportes físicos: Los oficios, documentos, expedientes, estantes o archiveros, tanto los dañados como los recuperados, y

d) Para soportes electrónicos7: Los campos, registros, tablas, bases de datos o archivos electrónicos, tanto dañados como recuperados, el nombre de los sistemas y la infraestructura afectada, indicar si el incidente afectó el servidor principal y los servidores de respaldo, etc.

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

V. ACCESO A LAS INSTALACIONES

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

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

Para las personas que acceden a sus instalaciones:

a) ¿Cómo las identifica?
No se cuenta con mecanismos de identificación.

b) ¿Cómo las autentifica?
No se cuenta con mecanismos de autenticación.

c) ¿Cómo les autoriza el acceso?
No se cuenta con mecanismos de control de acceso.

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

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

Para las personas que acceden a dichos espacios interiores:

1. ¿Cómo las identifica?
   Se tiene definida una lista de acceso para el personal autorizado.
2. ¿Cómo las autentifica?
   Mediante credencial y número de trabajador.
3. ¿Cómo les autoriza el acceso?
   Si se encuentran en la lista de acceso autorizada, o si son proveedores acompañados

por un empleado autorizado. Se les solicita se registren en la bitácora correspondiente.

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

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

Para actualizar los datos del estudiante se tienen dos opciones:

1) Como administrador del sistema, buscar al alumno ya sea por apellidos, nombre o número de cuenta y una vez encontrado seleccionar la opción “Consultar Datos Personales”, el cual es un formato editable de los mismos para proceder a su corrección.
2) Como estudiante de la escuela, puede entrar a su sesión en este sistema y mediante la opción “Mis Datos” puede hacer el mismo procedimiento.

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

VII. PERFILES DE USUARIO Y CONTRASEÑAS

1. Modelo de control de acceso:

Basado en perfiles o privilegios de acceso (permisos).

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?
Únicamente las contraseñas.

4. Administración de perfiles de usuario y contraseñas:

a) ¿Quién da de alta nuevos perfiles?
El Responsable del sistema a su cargo. Lic. Gustavo Cano Salazar.

b) ¿Quién autoriza la creación de nuevos perfiles?
El Secretario Técnico autoriza la creación de nuevos perfiles con privilegios administrativos.

c) ¿Se lleva registro de la creación de nuevos perfiles?
Mediante control interno del Departamento de Sistemas Informáticos y a través del sistema.

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

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

b) ¿Requiere el administrador acceso remoto al equipo donde reside el sistema para realizar tareas de mantenimiento?
Si, con acceso mediante VPN y SSH.

c) ¿Cómo se evita el acceso remoto no autorizado?

- Se cuenta con controles de acceso basados en roles y privilegios.
- El acceso remoto a los servidores se realiza mediante conexiones VPN habilitadas únicamente a los responsables de los sistemas.
- Implementación de captcha en el inicio de sesión del sistema.

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

1. Señalar si realiza respaldos

a) Completos_X_, diferenciales ___ o incrementales__X_;

b) De forma automática ____ o Manual _X_,

c) Periodicidad con que los realiza: _Semestral_

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 externo.

3. Cómo y dónde archiva esos medios, y Consultar los documentos: Plan de respaldos ENES Morelia y Bitácora de control de los respaldos.

4. Quién es el responsable de realizar estas operaciones (el área universitaria o un tercero). El responsable (encargado) del sistema a su cargo.

IX. PLAN DE CONTINGENCIA

[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.

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.

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

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

   No se cuenta con plan de contingencia.

3. Informar si cuenta con un sitio redundante (alterno) y señalar lo siguiente:
   a) El tipo de sitio (caliente, tibio o frío);[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.

Actualmente la ENES Unidad Morelia, no cuenta con sitio redundante para cubrir los incisos anteriores.

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*	
Identificador único*	EM002

[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.

Nombre del sistema*	ESCOLARES	
Recurso*	**Descripción***	**Control***
Reportes especiales de datos almacenados en el sistema.	Al solicitar reportes que no se encuentran en el sistema y su descarga en soporte electrónico, estos se generan y se descargan mediante un vínculo que vence en determinado tiempo para su descarga.	Evitar adjuntar archivos por correo electrónico porque es un servicio de terceros (Google). Una vez vencido el plazo de descarga (max. 24 horas) es imposible volver a descargar el soporte electrónico solicitado.
Reportes especiales de datos almacenados en el sistema en soportes electrónicos adjuntos por correo electrónico.	Solicitud de reportes especiales entregados en un soporte electrónico específico (hoja de cálculo, archivo separado por comas, texto plano, archivos portables, etc.) y que se piden se adjunten por correo electrónico.	Se utiliza el programa de software libre para cifrar el archivo y personalmente se indica la contraseña para descifrar en el equipo de cómputo del usuario para utilizar el archivo que fue adjuntado por correo electrónico.

7.2 Procedimiento para la revisión de las medidas de seguridad

Secretaría Técnica*		
Identificador único*	EM002	
Nombre del sistema*	ESCOLARES	
Medida de seguridad*	**Procedimiento***	**Responsable***
Principio del menor privilegio	Otorgar el acceso al usuario autorizado por la Secretaría	Encargado del sistema. Lic. Gustavo Cano Salazar. (01 día hábil).

	técnica de acuerdo con el permiso requerido.	
Respaldos del sistema y base de datos.	Generación de archivos de respaldo tanto del sistema web como de la base de datos y control de bitácoras de respaldo.	Encargado del sistema. Lic. Gustavo Cano Salazar. (01 día hábil).
Sincronizar la fecha y hora con el servidor NTP (Network Time Protocol) oficial de la UNAM	Revisiones periódicas de la hora y fecha del servidor donde se encuentra el sistema.	Mtro. Froylan Hernández Rendón (01 día hábil).
Instalar y mantener actualizado el software antimalware.	Revisión y actualización de la versión del software antivirus y de la base de datos.	Mtro. Froylan Hernández Rendón (01 día hábil).
Instalar las actualizaciones de seguridad más recientes disponibles.	Revisión y actualizaciones del sistema operativo.	Mtro. Froylan Hernández Rendón (02 días hábiles).

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

Secretaría Técnica*		
Identificador único*	EM002	
Nombre del sistema*	ESCOLARES	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***
Principio del menor privilegio	Se encontró que todas las cuentas de usuarios del sistema cuentan con los permisos correspondientes.	Encargado del sistema. Lic. Gustavo Cano Salazar.
Respaldo del sistema y base de datos.	Se cuenta con respaldos actualizados de la información del sistema.	Encargado del sistema. Lic. Gustavo Cano Salazar.
Sincronizar la fecha y hora con el servidor NTP (Network Time Protocol) oficial de la UNAM	La fecha y hora están sincronizadas con el servidor NTP de la UNAM.	Mtro. Froylán Hernández Rendón.

Instalar y mantener actualizado el software antimalware.	El Software antivirus está actualizado.	Mtro. Froylán Hernández Rendón.
Instalar las actualizaciones de seguridad más recientes disponibles.	El sistema operativo cuenta con las actualizaciones correspondientes.	Mtro. Froylán Hernández Rendón.

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

Secretaría Técnica*		
Identificador único*	EM002	
Nombre del sistema*	ESCOLARES	
Medida de seguridad*	**Acciones***	**Responsable***
Uso de certificados SSL	Implementar el protocolo “HTTPS” en el sistema. Realizar la renovación anual del certificado SSL para el subdominio donde se encuentra el sistema.	Mtro. Froylán Hernández Rendón

8 PROGRAMA ESPECÍFICO DE CAPACITACIÓN

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

Secretaría Técnica*	
Identificador único*	EM002

Nombre del sistema*	ESCOLARES		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Capacitación para la Protección de Datos Personales	Curso en línea	25 horas. Fecha de inicio: 20 de noviembre de 2020. Fecha de término: 17 de enero de 2021	Público objetivo: Enlaces de Transparencia, Responsables de Seguridad de Datos Personales, Responsables de Tecnologías de la Información, así como funcionarios y empleados universitarios. Sin vigencia. Sin frecuencia de actualización.
Medidas de Seguridad Técnicas para la Protección de Datos Personales	Curso en línea	25 horas. Fecha de inicio: 8 de febrero de 2021. Fecha de término: 14 de marzo de 2021.	Público objetivo: Enlaces de Transparencia, Responsables de Seguridad de Datos Personales, Responsables de Tecnologías de la Información, así como funcionarios y empleados universitarios. Sin vigencia. Sin frecuencia de actualización.
Elaboración de Documento de Seguridad y Sistema de Gestión de Seguridad de Datos	Curso en línea	25 horas. Fecha de inicio: 25 de marzo de 2022	Público objetivo: Enlaces de Transparencia, Responsables de Seguridad de Datos Personales, Responsables de

Personales de las áreas universitarias		Fecha de término: 25 de marzo de 2022.	Tecnologías de la Información, así como funcionarios y empleados universitarios. Sin vigencia. Sin frecuencia de actualización.
La importancia de la protección de datos personales	Seminario en línea	1 hora. Fecha: 16 de junio de 2022.	Público en general. Sin vigencia. Sin frecuencia de actualización.

8.2 Programa de difusión de la protección a los datos personales

Secretaría Técnica*			
Identificador único*	EM002		
Nombre del sistema*	ESCOLARES		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Indique actividad, tema, recursos para la difusión. Agregar un renglón por cada elemento	*Describa el tipo de elemento, sus objetivos y forma de impartición, publicación o distribución*	*Indique duración del elemento en horas, días, meses, su fecha de inicio y de término*	*Mencione público objetivo, vigencia del elemento y frecuencia de actualización*

Actualmente, no se cuenta con un programa de difusión de la protección de datos personales.

9 MEJORA CONTINUA

9.1 Actualización y mantenimiento de sistemas de información

Secretaría Técnica*			
Identificador único*	EM002		
Nombre del sistema*	ESCOLARES		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Actualización de tecnologías de desarrollo	1.Solicitud de actualización de la arquitectura de desarrollo del sistema de datos personales. 2. Corregir y/o actualizar módulos del sistema. 3. Pruebas unitarias e integrales de las actualizaciones realizadas al sistema. 4. Actualización de archivos de sistema y/o sentencias de bases de datos en servidor de producción.	12 meses	“Back-end” del sistema.

9.2 Actualización y mantenimiento de equipo de cómputo

Secretaría Técnica*			
Identificador único*	EM002		
Nombre del sistema*	ESCOLARES		
Actividad*	**Descripción***	**Duración***	**Cobertura***

Indique actividad. Agregar un renglón por cada elemento	*Describa el tipo de actividad, sus objetivos e impacto la actualización o mantenimiento del equipo de cómputo*	*Indique duración en la ejecución de la actividad en horas, días, meses, su fecha de inicio y de término*	*Mencione los aspectos de equipo de cómputo que son resueltos, total o parcialmente, por la actividad.*

Actualmente, no se han asignado recursos para la actualización del equipo de cómputo.

9.3 Procesos para la conservación, preservación y respaldos de información

Secretaría Técnica*		
Identificador único*	EM002	
Nombre del sistema*	ESCOLARES	
Proceso*	**Descripción***	**Responsable***
Poner en fase de “mantenimiento” del sistema.	Se coloca un mensaje en la parte de acceso al sistema con un aviso de “mantenimiento” y de ser posible la fecha de “regreso” a la operación del sistema.	Encargado del sistema: Lic. Gustavo Cano Salazar. (01 día hábil).
Ingresar remotamente al servidor.	Acceso al servidor de manera remota para realizar el respaldo de ambos componentes (script del sistema y de la base de datos)	Encargado del sistema: Lic. Gustavo Cano Salazar. (01 día hábil).
Descarga de respaldos del sistema a soporte físico electrónico.	Descarga directa al Disco Duro externo proporcionado por secretaría técnica con los	Encargado del sistema: Lic. Gustavo Cano Salazar. (01 día hábil).

	respaldos realizados del sistema.	
Salida del servidor y de fase de “mantenimiento” en el sistema.	Quitar el mensaje del modo mantenimiento del sistema y salida completa del servidor.	Encargado del sistema: Lic. Gustavo Cano Salazar. (01 día hábil).
El proceso de respaldo de información se encuentra contenido en el documento Plan de respaldos ENES Morelia	El proceso se describe en el documento Plan de respaldos ENES Morelia	Encargado del sistema: Lic. Gustavo Cano Salazar. (01 día hábil).

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

Secretaría Técnica*		
Identificador único*	EM002	
(Nombre del sistema A1)*	ESCOLARES	
Proceso*	**Descripción***	**Responsable***
Borrado de datos mediante sistema (jnterfaz).	En la interfaz se tienen habilitadas opciones de “Actualizar y/o borrar datos” para los usuarios del sistema.	Encargado del sistema: Lic. Gustavo Cano Salazar.
Borrado de datos dentro del Sistema Gestor de Base de Datos.	Aplicación de transacciones y ejecución de instrucciones SQL para actualización y/o borrado de datos. Una vez completada la transacción aplicar la instrucción correspondiente para	Encargado del sistema: Lic. Gustavo Cano Salazar.

	conservar o borrar definitivamente los datos.	
El proceso se encuentra contenido en el documento Borrado Seguro ENES Morelia	El proceso se describe en el documento Borrado Seguro ENES Morelia	Borrado seguro: Encargado del sistema: Lic. Gustavo Cano Salazar. Responsable de la disposición final de equipos o componentes de cómputo: Mtro. Froylán Hernández Rendón Tiempo máximo de ejecución: 05 días hábiles.

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

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

(Informar y describir el procedimiento para la cancelación de un sistema de tratamiento de datos personales.)[13]

[13] 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

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

a) Denominación
b) Motivo de la cancelación

B) PLAZOS Y CONDICIONES PARA EL BLOQUEO DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES:[14]

(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)

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.

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

SISTEMA CODR (COMISIÓN DE RECURSOS)

Sistema web que permite el registro de solicitudes a convocatorias (emitidas por el personal que conforma la Comisión de Recursos):

- Viáticos
- Eventos académicos (gastos de intercambio)
- Necesidades de docencia para coordinadores
- Materiales y equipos menores

Una vez que las solicitudes han sido registradas, el sistema permite realizar las evaluaciones correspondientes por el área administrativa. Permite la emisión de oficios para que los académicos puedan ejercer los recursos que le fueron autorizados. Además, es posible autorizar temporalmente a profesores de asignatura, ayudantes o invitados para que puedan realizar solicitudes a convocatorias.

El sistema también permite el registro de licencias nacionales e internacionales por parte de académicos de la ENES Morelia.

ANEXO I: Documento de Seguridad de datos personales

ÍNDICE

INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Secretaría Técnica	
Identificador único*	EM009
Nombre del sistema*	CODR (Comisión de Recursos)
Datos personales (sensibles o no) contenidos en el sistema*:	● Datos personales del académico(a): o Nombre completo (apellido paterno, apellido materno, nombre). o Número de trabajador o Correo electrónico y nombres completos de personas invitadas externas a la ENES Morelia, UNAM. que participan en eventos académicos.
Responsable*:	Escuela Nacional de Estudios Superiores Unidad Morelia
Nombre*:	Dr. Santiago Cortés Hernández
Cargo*:	Secretario Técnico
Funciones*:	Decidir sobre el tratamiento automatizado de los datos personales, así como el contenido, finalidad y uso del sistema.
Obligaciones*:	- Decidir a qué usuarios se le da acceso al sistema con privilegios administrativos. - Decidir sobre la incorporación de nuevas funcionalidades en el sistema. - Vigilar que el sistema cumpla con todas las medidas de seguridad técnicas, físicas y administrativas.
	Encargados[1]:
(Nombre del Encargado 1*)	Mtro. José Alfredo Noriega Carmona
Cargo*:	Técnico Académico en Desarrollo de Software
Funciones*:	Mantenimiento, documentación, soporte y capacitación de usuarios sobre el uso del sistema.
Obligaciones*:	● Vigilar la operación correcta del sistema. ● Monitorear la protección de los datos personales contenidos en el sistema mediante la implementación de estrategias y mecanismos de seguridad en su desarrollo y mantenimiento.

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

	Usuarios:
(Nombre del Usuario 1*)	Mtro. José Alfredo Noriega Carmona
Cargo*:	Técnico Académico en Desarrollo de Software
Funciones*:	Revisar el proceso de registro y/o actualización de banco de horas y horarios por parte de los Coordinadores de Área.
Obligaciones*:	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 desempeña en la Universidad mediante el uso del sistema.
(Nombre del Usuario 2*)	Dra. María del Río Francos
Cargo*:	Coordinadora de Área 1 (Físico-Matemáticas y de las Ingenierías)
Funciones*:	Realizar el registro de solicitudes a convocatorias en curso.
Obligaciones*:	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 desempeña en la Universidad mediante el uso del sistema.
(Nombre del Usuario 3*)	Dra. Lucero Sevillano García-Mayeya.
Cargo*:	Coordinadora de Área 2: Ciencias Biológicas y de la Salud
Funciones*:	Realizar el registro de solicitudes a convocatorias en curso.
Obligaciones*:	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 desempeña en la Universidad mediante el uso del sistema.
(Nombre del Usuario 4*)	Dra. Nuri Celene Fuerte Álvarez
Cargo*:	Coordinadora de Área 3: Ciencias Sociales.
Funciones*:	Realizar el registro de solicitudes a convocatorias en curso.
Obligaciones*:	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 desempeña en la Universidad mediante el uso del sistema.
(Nombre del Usuario 5*)	Mtra. Beatriz Alejandra Pimentel Ávila
Cargo*:	Coordinadora de Área 4: Humanidades y Artes.
Funciones*:	Realizar el registro de solicitudes a convocatorias en curso.

Obligaciones*:	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 desempeña en la Universidad mediante el uso del sistema.
(Nombre del Usuario 6*)	Dra. Claudia Briones Jurado
Cargo*:	Coordinador de la Licenciatura en Ciencia de Materiales Sustentables
Funciones*:	Realizar el registro de solicitudes a convocatorias en curso.
Obligaciones*:	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 desempeña en la Universidad mediante el uso del sistema.
(Nombre del Usuario 7*)	Dr. Sinhué A. R. Haro Corzo
Cargo*:	Coordinador de la Licenciatura en Geociencias
Funciones*:	Realizar el registro de solicitudes a convocatorias en curso.
Obligaciones*:	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 desempeña en la Universidad mediante el uso del sistema.
(Nombre del Usuario 8*)	Dr. Luis Miguel García Velázquez
Cargo*:	Coordinador de la Licenciatura en Tecnologías para la Información en Ciencias
Funciones*:	Realizar el registro de solicitudes a convocatorias en curso.
Obligaciones*:	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 desempeña en la Universidad mediante el uso del sistema.
(Nombre del Usuario 9*)	Dr. Ignacio Torres García
Cargo*:	Coordinador de la Licenciatura en Ciencias Agroforestales
Funciones*:	Realizar el registro de solicitudes a convocatorias en curso.
Obligaciones*:	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 desempeña en la Universidad mediante el uso del sistema.
(Nombre del Usuario 10*)	M. en C. Ana Claudia Nepote González
Cargo*:	Coordinador de la Licenciatura en Ciencias Ambientales
Funciones*:	Realizar el registro de solicitudes a convocatorias en curso.
Obligaciones*:	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 desempeña en la Universidad mediante el uso del sistema.
(Nombre del Usuario 11*)	Dr. Carlos Anaya Merchant
Cargo*:	Coordinador de la Licenciatura en Ecología
Funciones*:	Realizar el registro de solicitudes a convocatorias en curso.
Obligaciones*:	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 desempeña en la Universidad mediante el uso del sistema.
(Nombre del Usuario 12*)	Dra. Karina Vázquez Bernal
Cargo*:	Coordinador de la Licenciatura en Geohistoria
Funciones*:	Realizar el registro de solicitudes a convocatorias en curso.
Obligaciones*:	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 desempeña en la Universidad mediante el uso del sistema.
(Nombre del Usuario 13*)	Dra. Marcela Morales Magaña
Cargo*:	Coordinador de la Licenciatura en Estudios Sociales y Gestión Local
Funciones*:	Realizar el registro de solicitudes a convocatorias en curso.
Obligaciones*:	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 desempeña en la Universidad mediante el uso del sistema.
(Nombre del Usuario 14*)	Dr. Ignacio Silva Cruz
Cargo*:	Coordinador de la Licenciatura en Administración de Archivos y Gestión Documental

Funciones*:	Realizar el registro de solicitudes a convocatorias en curso.
Obligaciones*:	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 desempeña en la Universidad mediante el uso del sistema.
(Nombre del Usuario 15*)	Lic. Joel Astreo González López
Cargo*:	Coordinador de la Licenciatura en Arte y Diseño
Funciones*:	Realizar el registro de solicitudes a convocatorias en curso.
Obligaciones*:	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 desempeña en la Universidad mediante el uso del sistema.
(Nombre del Usuario 16*)	Mtra. María Guadalupe Matus Ramírez
Cargo*:	Coordinador de la Licenciatura en Historia del Arte
Funciones*:	Realizar el registro de solicitudes a convocatorias en curso.
Obligaciones*:	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 desempeña en la Universidad mediante el uso del sistema.
(Nombre del Usuario 17*)	Dr. Antonio Río Torres-Murciano
Cargo*:	Coordinador de la Licenciatura en Literatura Intercultural
Funciones*:	Realizar el registro de solicitudes a convocatorias en curso.
Obligaciones*:	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 desempeña en la Universidad mediante el uso del sistema.
(Nombre del Usuario 18*)	Dr. Rodrigo Sigal Sefchovich
Cargo*:	Coordinador de la Licenciatura en Música y Tecnología Artística
Funciones*:	Realizar el registro de solicitudes a convocatorias en curso.
Obligaciones*:	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 desempeña en la Universidad mediante el uso del sistema.
(Nombre del Usuario 19*)	Dr. Luis Alejandro Pérez Ortiz
Cargo*:	Coordinador del Posgrado en Antropología
Funciones*:	Realizar el registro de solicitudes a convocatorias en curso.
Obligaciones*:	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 desempeña en la Universidad mediante el uso del sistema.
(Nombre del Usuario 20*)	Lic. Ana Gabriela Vargas Gómez
Cargo*:	Secretaria Administrativa
Funciones*:	Realizar la gestión de solicitudes realizadas a convocatorias emitidas desde la Comisión de Recursos.
Obligaciones*:	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 desempeña en la Universidad mediante el uso del sistema.

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

Secretaría Técnica	
Identificador único*	EM009
Nombre del sistema*	CODR (Comisión de Recursos)
Tipo de soporte[2]:*	Electrónico
Descripción[3]:*	Para almacenamiento de datos se utiliza un Sistema Gestor de Bases de Datos relacional y para informes ejecutivos y reportes se generan archivos de la suite de Microsoft.

[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.

Características del lugar donde se resguardan los soportes[4]:*	[redacted]

Eliminado: Información específica sobre el lugar donde se resguardan los soportes de la información.

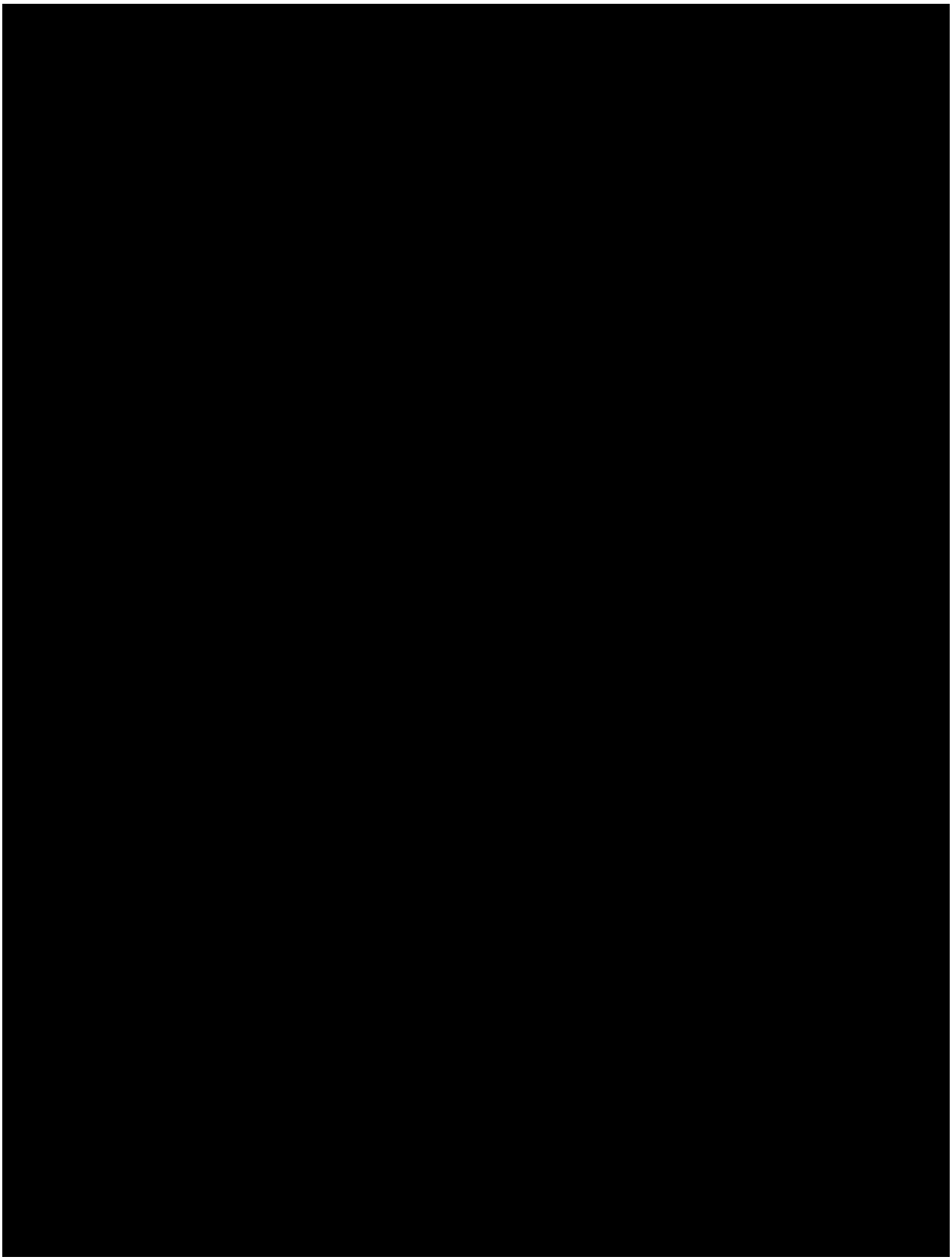
Fundamentación: De conformidad con los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública, así como los artículos 32 y 36 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

Motivación: En virtud de que estos datos hace identificable las formas en que es posible atacar o vulnerar nuestros sistemas de información que resguardan datos personales y 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.

[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



[redacted]

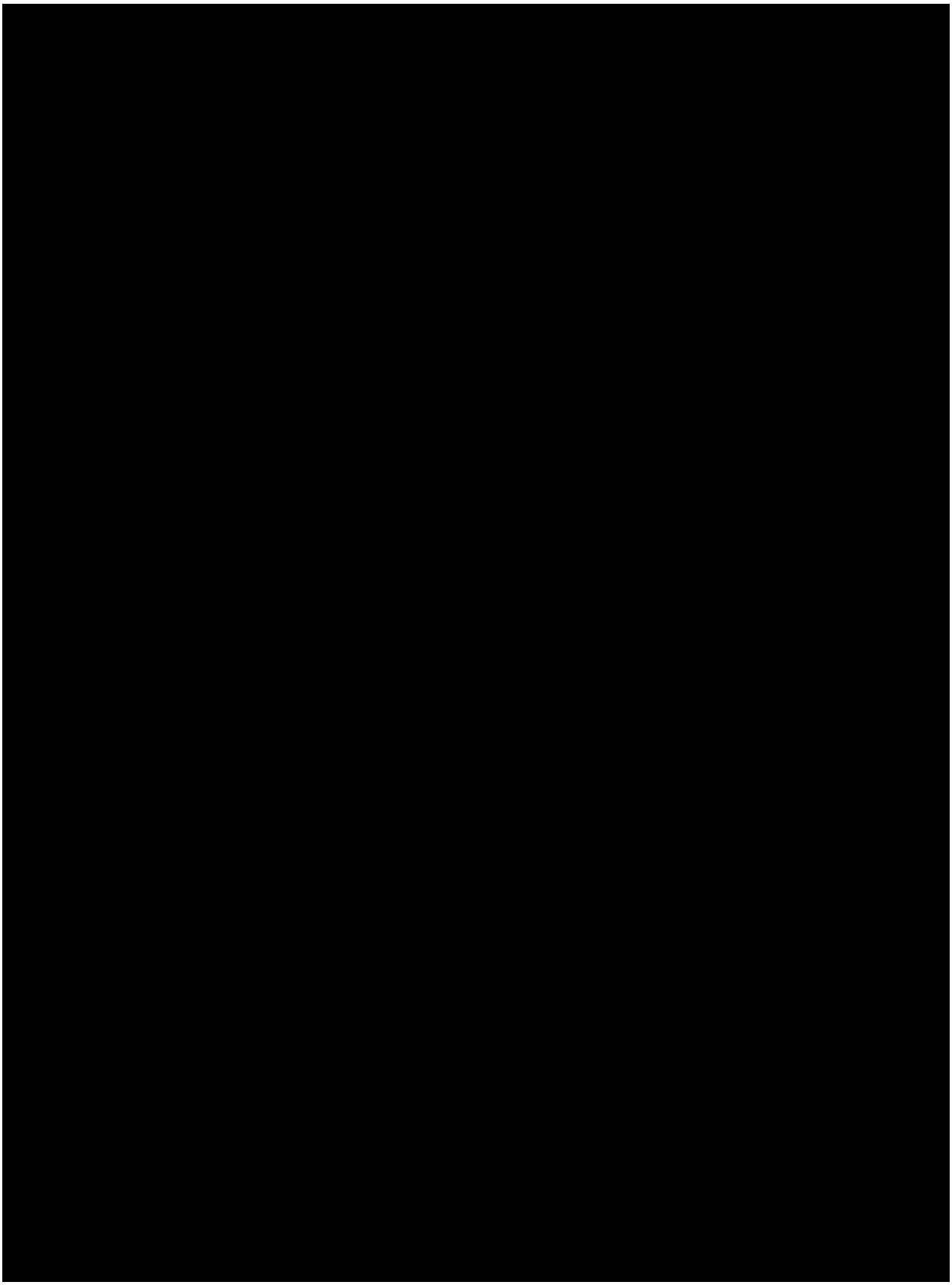
Eliminado: Análisis de riesgos.

Fundamentación: De conformidad con 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 los artículos 32 y 36 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

Motivación: En virtud de que estos datos hace identificable las formas en que es posible atacar o vulnerar nuestros sistemas de información que resguardan datos personales y 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.

4. ANÁLISIS DE BRECHA

[redacted]



[redacted]

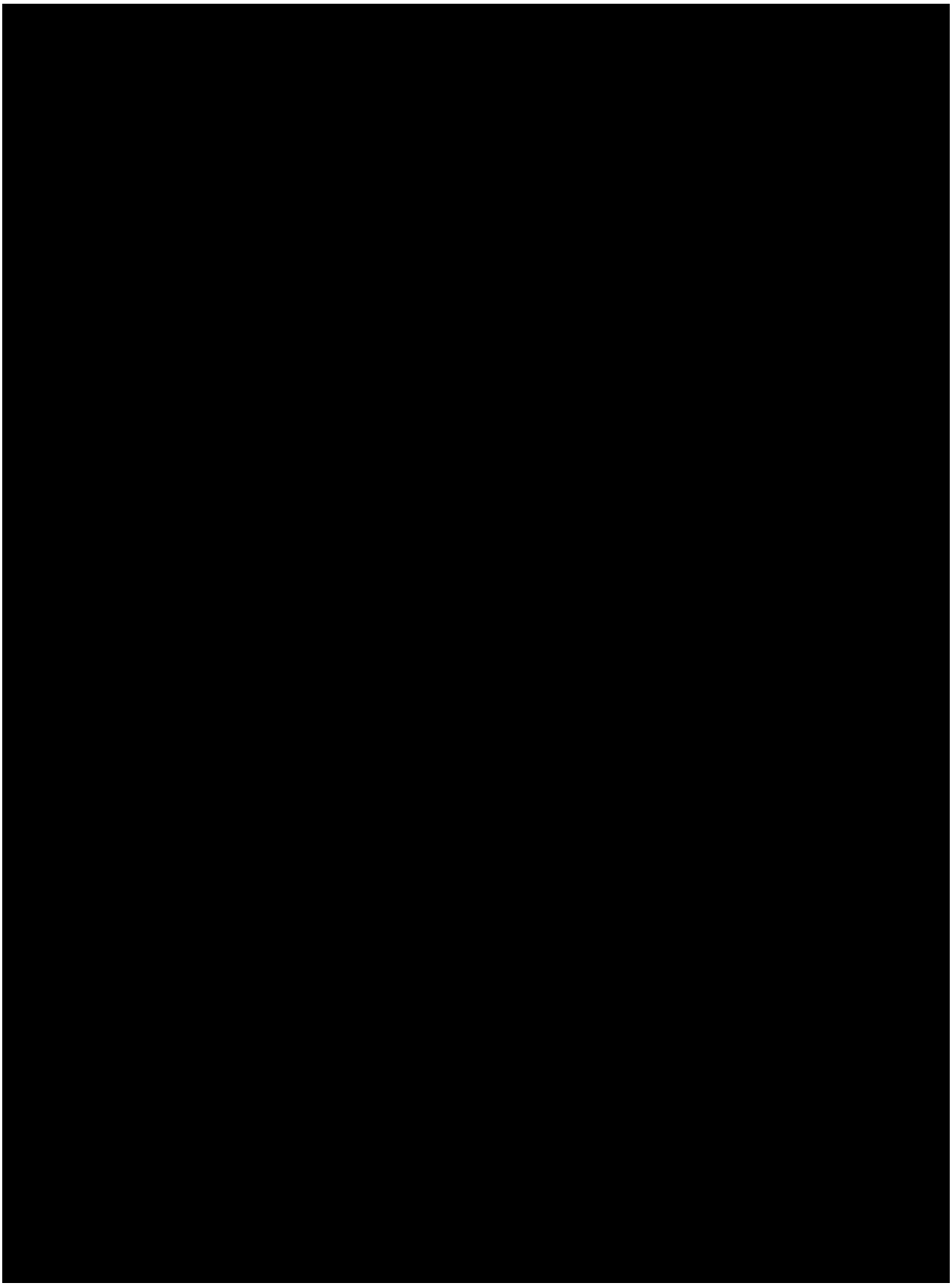
Eliminado: Análisis de brecha.

Fundamentación: De conformidad con 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 los artículos 32 y 36 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

Motivación: En virtud de que estos datos hace identificable las formas en que es posible atacar o vulnerar nuestros sistemas de información que resguardan datos personales y 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.

5. PLAN DE TRABAJO

[redacted]



[redacted]

Eliminado: Plan de trabajo.

Fundamentación: De conformidad con 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 los artículos 32 y 36 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

Motivación: En virtud de que estos datos hace identificable las formas en que es posible atacar o vulnerar nuestros sistemas de información que resguardan datos personales y 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.

6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

I. TRANSFERENCIAS DE DATOS PERSONALES

Secretaría Técnica*	
Identificador único*	EM009
(Nombre del sistema A1)*	CODR (Comisión de Recursos)
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:[5]	No se realizan transferencias de datos personales mediante el traslado de soportes físicos.
Transferencias mediante el traslado de soportes electrónicos:	No se realizan transferencias de datos personales mediante el traslado de soportes electrónicos.
Transferencias mediante el traslado sobre redes electrónicas:	No se realizan transferencias de datos personales mediante el traslado sobre redes electrónicas.

I. RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON

[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.

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]

2. Señalar en un listado las personas (nombre, cargo, funciones y obligaciones) que tienen acceso a los soportes físicos del sistema.[7]

El sistema no realiza tratamiento de datos personales con soportes físicos, ya que se encuentra en soporte electrónico mediante el uso de una base de datos.

II. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

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

[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:

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.

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

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.

El sistema actualmente no cuenta con un registro de bitácoras de acceso y operación cotidiana.

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 cuenta con un procedimiento de atención de incidentes.

1. Los datos que registra:

a) La persona que resolvió el incidente;

b) La metodología aplicada;[10]

---

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.

[10] **Ejemplo de procedimiento en caso de presentarse un incidente:**

c) Para soportes físicos: Los oficios, documentos, expedientes, estantes o archiveros, tanto los dañados como los recuperados, y

d) Para soportes electrónicos: Los campos, registros, tablas, bases de datos o archivos electrónicos, tanto dañados como recuperados, el nombre de los sistemas y la infraestructura afectada, indicar si el incidente afectó el servidor principal y los servidores de respaldo, etc.

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

V. ACCESO A LAS INSTALACIONES

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

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

Para las personas que acceden a sus instalaciones:

a) ¿Cómo las identifica?

No se cuenta con mecanismos de identificación.

b) ¿Cómo las autentifica?

No se cuenta con mecanismos de autenticación.

c) ¿Cómo les autoriza el acceso?

No se cuenta con mecanismos de control de acceso.

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

---

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.

¿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?
   Se tiene definida una lista de acceso para el personal autorizado.
2. ¿Cómo las autentifica?
   Mediante credencial y número de trabajador.
3. ¿Cómo les autoriza el acceso?
   Si se encuentran en la lista de acceso autorizada, o si son proveedores acompañados por un empleado autorizado. Se les solicita se registren en la bitácora correspondiente.

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

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

En caso de detectar error y/o realizar alguna actualización de datos personales del académico se tienen dos procedimientos:

1) Si es profesor de asignatura/ayudante, mediante el sistema de contrataciones temporales de profesores de asignatura, interinos y ayudantes se realiza dicha actualización en la opción “Mi perfil” y posteriormente mediante proceso automatizado estos datos actualizados se “realimentan” en el presente sistema.
2) Para académicos de tiempo completo, técnicos académicos e invitados, la actualización de datos personales se hace a través de medio escrito (correo electrónico) ya sea del interesado o a través de su Coordinador de Área y/o Licenciatura al Lic. Gustavo Cano Salazar, señalando el sistema donde se encuentra el ajuste a realizar y éste procede a realizarlo.

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

VII. PERFILES DE USUARIO Y CONTRASEÑAS

1. Modelo de control de acceso:

Basado en perfiles o privilegios de acceso (permisos).

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?
Únicamente las contraseñas.

4. Administración de perfiles de usuario y contraseñas:

a) ¿Quién da de alta nuevos perfiles?
El Responsable del sistema a su cargo. Lic. Gustavo Cano Salazar.

b) ¿Quién autoriza la creación de nuevos perfiles?
El Secretario Técnico autoriza la creación de nuevos perfiles con privilegios administrativos.

c) ¿Se lleva registro de la creación de nuevos perfiles?
Mediante control interno del Departamento de Sistemas Informáticos y a través del sistema.

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

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

b) ¿Requiere el administrador acceso remoto al equipo donde reside el sistema para realizar tareas de mantenimiento?
Si, con acceso mediante VPN.

c) ¿Cómo se evita el acceso remoto no autorizado?

- Se cuenta con controles de acceso basados en roles y privilegios.
- El acceso remoto a los servidores se realiza mediante conexiones VPN habilitadas únicamente a los responsables de los sistemas.
- Implementación de captcha en el inicio de sesión del sistema.

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: _Semestral_

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 externo.
3. Cómo y dónde archiva esos medios, y Consultar los documentos: "Plan de respaldos ENES Morelia" y "Bitácora de control de los respaldos".
4. Quién es el responsable de realizar estas operaciones (el área universitaria o un tercero). El área universitaria.

IX. PLAN DE CONTINGENCIA

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

   Se cuenta con algunas medidas como las especificadas en el documento: "Medidas de seguridad en los periodos de inactividad o mantenimiento", pero no se tiene desarrollado el plan de contingencia.
2. Si cuenta con plan de contingencia y lo ha implementado, deberá indicar si realiza pruebas de eficiencia de este.

   No se cuenta con plan de contingencia.
3. Informar si cuenta con un sitio redundante (alterno) y señalar lo siguiente:
   a) El tipo de sitio (caliente, tibio o frío);[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.

Actualmente la ENES Unidad Morelia, no cuenta con sitio redundante para cubrir los incisos anteriores.

[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.

[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.

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*		
Identificador único*	EM009	
Nombre del sistema*	CODR (Comisión de Recursos)	
Recurso*	**Descripción***	**Control***
Reportes especiales de datos almacenados en el sistema.	Al solicitar reportes que no se encuentran en el sistema y su descarga en soporte electrónico, estos se generan y se descargan mediante un vínculo que vence en determinado tiempo para su descarga.	Evitar adjuntar archivos por correo electrónico porque es un servicio de terceros (Google). Una vez vencido el plazo de descarga (max. 24 horas) es imposible volver a descargar el soporte electrónico solicitado,
Reportes especiales de datos almacenados en el sistema en soportes electrónicos adjuntos por correo electrónico.	Solicitud de reportes especiales entregados en un soporte electrónico específico y que se piden se adjunten por correo electrónico.	Se utiliza programa de distribución libre para cifrar el archivo y personalmente se indica la contraseña para descifrarlo en el equipo de cómputo del usuario para utilizar el archivo que fue adjuntado por correo electrónico.

7.2 Procedimiento para la revisión de las medidas de seguridad

Secretaría Técnica*		
Identificador único*	EM009	
Nombre del sistema*	CODR (Comisión de Recursos)	
Medida de seguridad*	**Procedimiento***	**Responsable***
Principio del menor privilegio	Otorgar el acceso al usuario autorizado por la Secretaría técnica de acuerdo con el permiso requerido.	Lic. Gustavo Cano Salazar (01 día hábil).
Respaldos del sistema y base de datos.	Generación de archivos de respaldo tanto del sistema web como de la base de datos y control de bitácoras de respaldo.	Lic. Gustavo Cano Salazar. (01 día hábil).
Sincronizar la fecha y hora con el servidor NTP (Network Time Protocol) oficial de la UNAM	Revisiones periódicas de la hora y fecha del servidor donde se encuentra el sistema.	Mtro. Froylán Hernández Rendón (01 día hábil).
Instalar y mantener actualizado el software antimalware.	Revisión y actualización de la versión del software antivirus y de la base de datos.	Mtro. Froylán Hernández Rendón (01 día hábil).
Instalar las actualizaciones de seguridad más recientes disponibles.	Revisión y actualizaciones del sistema operativo.	Mtro. Froylán Hernández Rendón (02 días hábiles).

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

Secretaría Técnica*		
Identificador único*	EM009	
Nombre del sistema*	CODR (Comisión de Recursos)	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***

Principio del menor privilegio	Se encontró que todas las cuentas de usuarios del sistema cuentan con los permisos correspondientes.	Lic. Gustavo Cano Salazar.
Respaldo del sistema y base de datos.	Se cuenta con respaldos actualizados de la información del sistema.	Lic. Gustavo Cano Salazar.
Sincronizar la fecha y hora con el servidor NTP (Network Time Protocol) oficial de la UNAM	La fecha y hora están sincronizadas con el servidor NTP de la UNAM.	Mtro. Froylán Hernández Rendón.
Instalar y mantener actualizado el software antimalware.	El Software antivirus está actualizado.	Mtro. Froylán Hernández Rendón.
Instalar las actualizaciones de seguridad más recientes disponibles.	El sistema operativo cuenta con las actualizaciones correspondientes.	Mtro. Froylán Hernández Rendón.

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

Secretaría Técnica*		
Identificador único*	EM009	
Nombre del sistema*	CODR (Comisión de Recursos)	
Medida de seguridad*	**Acciones***	**Responsable***
Uso de certificados SSL	Implementar el protocolo “HTTPS” en el sistema. Realizar la renovación anual del certificado SSL para el subdominio donde se encuentra el sistema.	Mtro. Froylán Hernández Rendón

8 PROGRAMA ESPECÍFICO DE CAPACITACIÓN

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

Secretaría Técnica*			
Identificador único*	EM009		
Nombre del sistema*	CODR (Comisión de Recursos)		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Capacitación para la Protección de Datos Personales	Curso en línea	25 horas. Fecha de inicio: 20 de noviembre de 2020. Fecha de término: 17 de enero de 2021	Público objetivo: Enlaces de Transparencia, Responsables de Seguridad de Datos Personales, Responsables de Tecnologías de la Información, así como funcionarios y empleados universitarios. Sin vigencia. Sin frecuencia de actualización.
Medidas de Seguridad Técnicas para la Protección de Datos Personales	Curso en línea	25 horas. Fecha de inicio: 8 de febrero de 2021. Fecha de término: 14 de marzo de 2021.	Público objetivo: Enlaces de Transparencia, Responsables de Seguridad de Datos Personales, Responsables de Tecnologías de la Información, así como funcionarios y empleados universitarios.

			Sin vigencia. Sin frecuencia de actualización.
Elaboración de Documento de Seguridad y Sistema de Gestión de Seguridad de Datos Personales de las áreas universitarias	Curso en línea	25 horas. Fecha de inicio: 25 de marzo de 2022 Fecha de término: 25 de marzo de 2022.	Público objetivo: Enlaces de Transparencia, Responsables de Seguridad de Datos Personales, Responsables de Tecnologías de la Información, así como funcionarios y empleados universitarios. Sin vigencia. Sin frecuencia de actualización.
La importancia de la protección de datos personales	Seminario en línea	1 hora. Fecha: 16 de junio de 2022.	Público en general. Sin vigencia. Sin frecuencia de actualización.

8.2 Programa de difusión de la protección a los datos personales

Secretaría Técnica*			
Identificador único*	EM009		
Nombre del sistema*	CODR (Comisión de Recursos)		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Indique actividad, tema, recursos para la difusión. Agregar	*Describa el tipo de elemento, sus objetivos y forma*	*Indique duración del elemento en horas, días,*	*Mencione público objetivo, vigencia del*

un renglón por cada elemento	*de impartición, publicación o distribución*	*meses, su fecha de inicio y de término*	*elemento y frecuencia de actualización*

Actualmente, no se cuenta con un programa de difusión de la protección de datos personales.

9 MEJORA CONTINUA

9.1 Actualización y mantenimiento de sistemas de información

Secretaría Técnica*			
Identificador único*	EM009		
Nombre del sistema*	CODR (Comisión de Recursos)		
Actividad*	**Descripción***	**Duración ***	**Cobertura***
Actualización de tecnologías de desarrollo	1.Solicitud de actualización de la arquitectura de desarrollo del sistema. 2. Corregir y/o actualizar módulos del sistema. 3. Pruebas unitarias e integrales de las actualizaciones realizadas al sistema. 4. Actualización de archivos de sistema y/o sentencias de bases de datos en servidor de producción.	12 meses	“Back-end” del sistema.

9.2 Actualización y mantenimiento de equipo de cómputo

Secretaría Técnica*			
Identificador único*	EM009		
Nombre del sistema*	CODR (Comisión de Recursos).		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Indique actividad. Agregar un renglón por cada elemento	*Describa el tipo de actividad, sus objetivos e impacto la actualización o mantenimiento del equipo de cómputo*	*Indique duración en la ejecución de la actividad en horas, días, meses, su fecha de inicio y de término*	*Mencione los aspectos de equipo de cómputo que son resueltos, total o parcialmente, por la actividad.*

Actualmente, no se han asignado recursos para la actualización del equipo de cómputo.

9.3 Procesos para la conservación, preservación y respaldos de información

Secretaría Técnica*		
Identificador único*	EM009	
Nombre del sistema*	CODR (Comisión de Recursos).	
Proceso*	**Descripción***	**Responsable***
Poner en fase de “mantenimiento” del sistema.	Se coloca un mensaje en la parte de acceso al sistema con un aviso de “mantenimiento” y de ser posible la fecha de “regreso” a la operación del sistema.	Mtro. José Alfredo Noriega Carmona vía el Lic. Gustavo Cano Salazar. (01 día hábil).

Ingresar remotamente al servidor.	Acceso mediante SSH al servidor de manera remota para realizar el respaldo de ambos componentes (script del sistema y de la base de datos)	Mtro. José Alfredo Noriega Carmona vía el Lic. Gustavo Cano Salazar. (01 día hábil).
Descarga de respaldos del sistema a soporte físico electrónico.	Descarga directa al Disco Duro externo proporcionado por secretaría técnica con los respaldos realizados del sistema.	Lic. Gustavo Cano Salazar. (01 día hábil).
Salida del servidor y de fase de “mantenimiento” en el sistema.	Quitar el mensaje del modo mantenimiento del sistema y salida completa del servidor.	Mtro. José Alfredo Noriega Carmona vía el Lic. Gustavo Cano Salazar. (01 día hábil).
El proceso de respaldo de información se encuentra contenido en el documento “Plan de respaldos ENES Morelia”.	El proceso se describe en el documento “Plan de respaldos ENES Morelia”.	Lic. Gustavo Cano Salazar. (01 día hábil).

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

Secretaría Técnica*		
Identificador único*	EM009	
(Nombre del sistema A1)*	CODR (Comisión de Recursos)	
Proceso*	**Descripción***	**Responsable***

El proceso se encuentra contenido en el documento “Borrado Seguro ENES Morelia”.	El proceso se describe en el documento “Borrado Seguro ENES Morelia”.	Borrado seguro: Encargado del sistema: Mtro. José Alfredo Noriega Carmona vía el Lic. Gustavo Cano Salazar. Responsable de la disposición final de equipos o componentes de cómputo: Mtro. Froylán Hernández Rendón Tiempo máximo de ejecución: 05 días hábiles.

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

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

(Informar y describir el procedimiento para la cancelación de un sistema de tratamiento de datos personales.)[13]

[13] 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.

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

a) Denominación
b) Motivo de la cancelación

B) PLAZOS Y CONDICIONES PARA EL BLOQUEO DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES:[14]

(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)

PROCEDIMIENTO PARA LA SUPRESIÓN DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

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

SIAENES (SISTEMA DE INFORME ANUAL DE ACADÉMICOS DE TIEMPO COMPLETO)

Sistema web que almacena todos informes anuales de todos los académicos(as) de tiempo completo de la ENES Unidad Morelia que son:

- Investigadores(as)
- Profesores(as) de Carrera
- Técnicos(as) académicos(as)

En donde dependiendo de cada tipo de contratación de estos tres niveles académicos de la UNAM que son: Artículo 51, Interinos y Definitivos(as) deben hacer este procedimiento de forma obligatoria para entregar a la Secretaría de Investigación y Posgrado el informe en formato PDF que se obtiene de este sistema y también obtener los indicadores que se requieran para medir y/o saber la productividad del nivel académico de tiempo completo de la escuela.

Se señala que este sistema se conecta y retroalimenta del sistema principal CRONOS mencionado anteriormente para obtener algunos datos personales del académico para que se encuentren presentes y visibles e identificar en el informe al académico que está reportando las actividades realizadas en un periodo específico.

ANEXO I: Documento de Seguridad de datos personales

ÍNDICE

INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Secretaría Técnica	
Identificador único*	EM004
Nombre del sistema*	SIAENES (Sistema de Informe Anual de Académicos de Tiempo Completo)
Datos personales (sensibles o no) contenidos en el sistema*:	● Datos personales del académico(a) ○ Nombre completo (apellido paterno, apellido materno, nombre ○ RFC ○ CURP ○ Sexo ○ Número de trabajador ○ Lugar de nacimiento ○ Nombramiento ○ Fecha de nacimiento ○ Nacionalidad ○ Estado civil ○ Domicilio particular completo ○ Teléfono(s) ○ Correo electrónico ○ Fecha de ingreso a la UNAM ○ Fecha de ingreso a la ENES Morelia ○ Teléfono oficina ○ Estímulo SNI ○ PRIDE ○ PAIPA ○ PEII ○ Nombramiento
Responsable*:	Escuela Nacional de Estudios Superiores Unidad Morelia
Nombre*:	Dr. Santiago Cortés Hernández
Cargo*:	Secretario Técnico
Funciones*:	Decidir sobre el tratamiento automatizado de los datos personales, así como el contenido, finalidad y uso del sistema.
Obligaciones*:	- Decidir a qué usuarios se le da acceso al sistema con privilegios administrativos. - Decidir sobre la incorporación de nuevas funcionalidades en el sistema. - Vigilar que el sistema cumpla con todas las medidas de

	seguridad técnicas, físicas y administrativas.
	Encargados[1]:
(Nombre del Encargado 1*)	Lic. Gustavo Cano Salazar
Cargo*:	Técnico Académico, responsable del Depto. de Sistemas Informáticos de la ENES Unidad Morelia.
Funciones*:	Análisis, diseño, implementación, mantenimiento, documentación, soporte y capacitación de usuarios, sobre los diversos sistemas informáticos a su cargo en operación de la ENES Unidad Morelia.
Obligaciones*:	● Vigilar la operación correcta del sistema durante el periodo de mayor uso de este (inicios y fin de cada semestre). ● Registrar, actualizar, eliminar datos según requerimiento por escrito de la Secretaría Técnica y/o los usuarios que utilizan el sistema. ● Monitorear la protección de los datos personales contenidos en el sistema mediante la implementación de estrategias y mecanismos de seguridad en su desarrollo y mantenimiento, a nivel interno y externo.
	Usuarios:
(Nombre del Usuario 1*)	Dra. Mercedes Martínez González
Cargo*:	Secretaria de Investigación y posgrado / Profesora de carrera asociada “C” de tiempo completo. Definitiva
Funciones*:	Revisar los informes ingresados en el sistema para monitorear la productividad académica de los investigadores, profesores y técnicos académicos(as) de la ENES Unidad Morelia.
Obligaciones*:	Cumplir con la obligación legal de resguardar los datos personales de los académicos(as) registrados en el sistema utilizando la información con fines administrativos.
(Nombre del Usuario 2*)	Profesor(a) / Técnico(a) de Tiempo Completo
Cargo*:	Académico(a) de la ENES Unidad Morelia.
Funciones*:	▪ Ingresar al sistema anualmente mediante número de trabajador y RFC con homoclave. ▪ Actualizar los datos personales (si aplica) en el formato prellenado. ▪ Ingresar los rubros del informe de acuerdo con el nombramiento que realizó en un periodo específico (generalmente a su contrato elaborado indicado

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

	este periodo). ▪ Entregar en archivo PDF obtenido del sistema el informe a entregar con el periodo reportado.
Obligaciones*:	Resguardar sus propios datos personales sin conceder el acceso a este sistema a otra persona que no sea el académico autorizado.

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

Secretaría Técnica	
Identificador único*	EM004
Nombre del sistema*	SIAENES (Sistema de Informe Anual de Académicos de Tiempo Completo)
Tipo de soporte[2]:*	Electrónico
Descripción[3]:*	Para almacenamiento de datos se utiliza un Sistema Gestor de Bases de Datos Relacional y para informes ejecutivos y reportes se generan archivos separados por comas, hojas de cálculo y formato de documentos portables.
[redacted]	

[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.

[redacted]

Eliminado: Información específica sobre el lugar donde se resguardan los soportes de la información.

Fundamentación: De conformidad con 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 los artículos 32 y 36 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

Motivación: En virtud de que estos datos hace identificable las formas en que es posible atacar o vulnerar nuestros sistemas de información que resguardan datos personales y 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.

3. ANÁLISIS DE RIESGOS

[redacted]

[redacted]

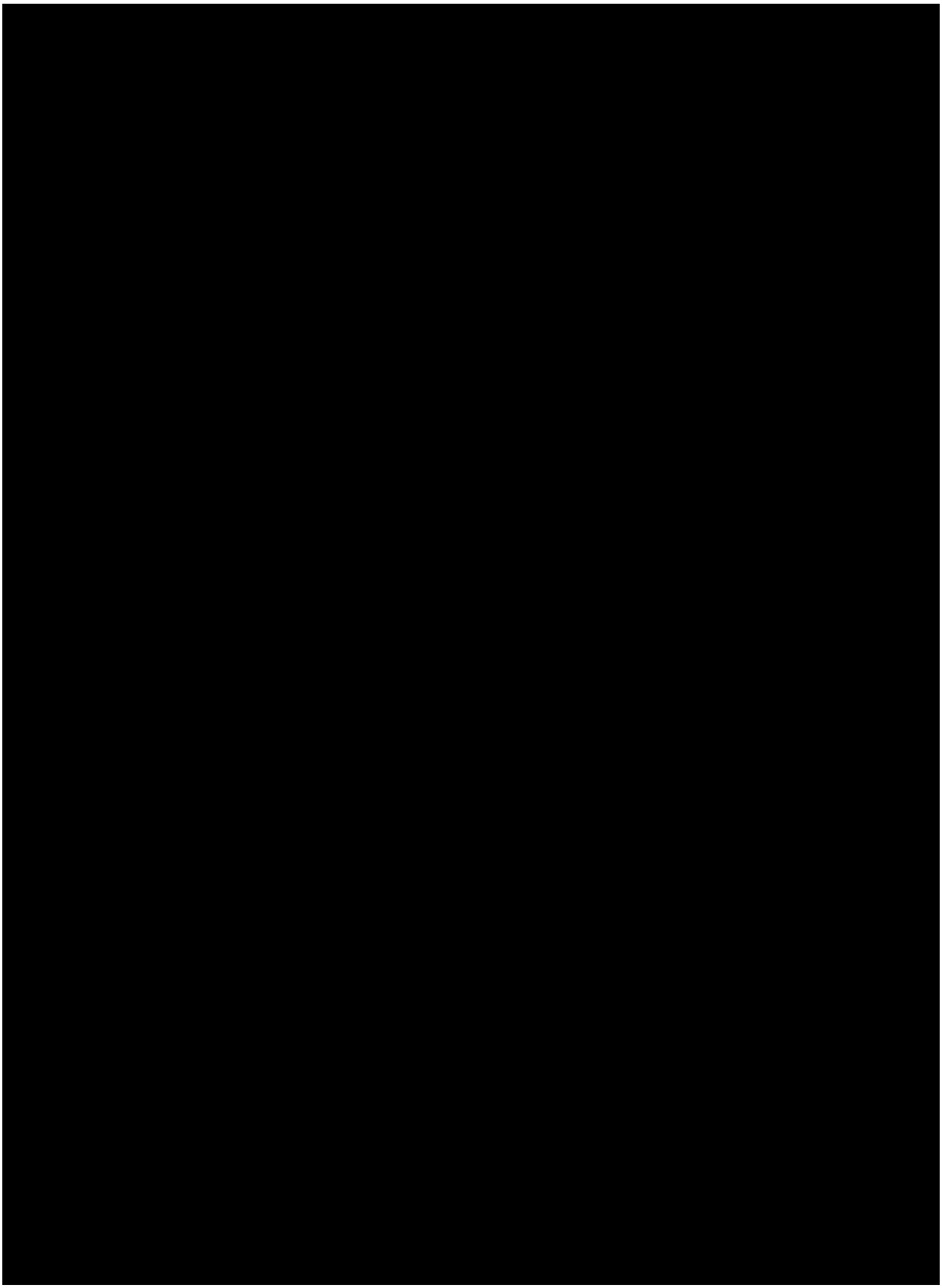
Eliminado: Análisis de riesgos.

Fundamentación: De conformidad con 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 los artículos 32 y 36 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

Motivación: En virtud de que estos datos hace identificable las formas en que es posible atacar o vulnerar nuestros sistemas de información que resguardan datos personales y 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.

4. ANÁLISIS DE BRECHA

[redacted]



[redacted]

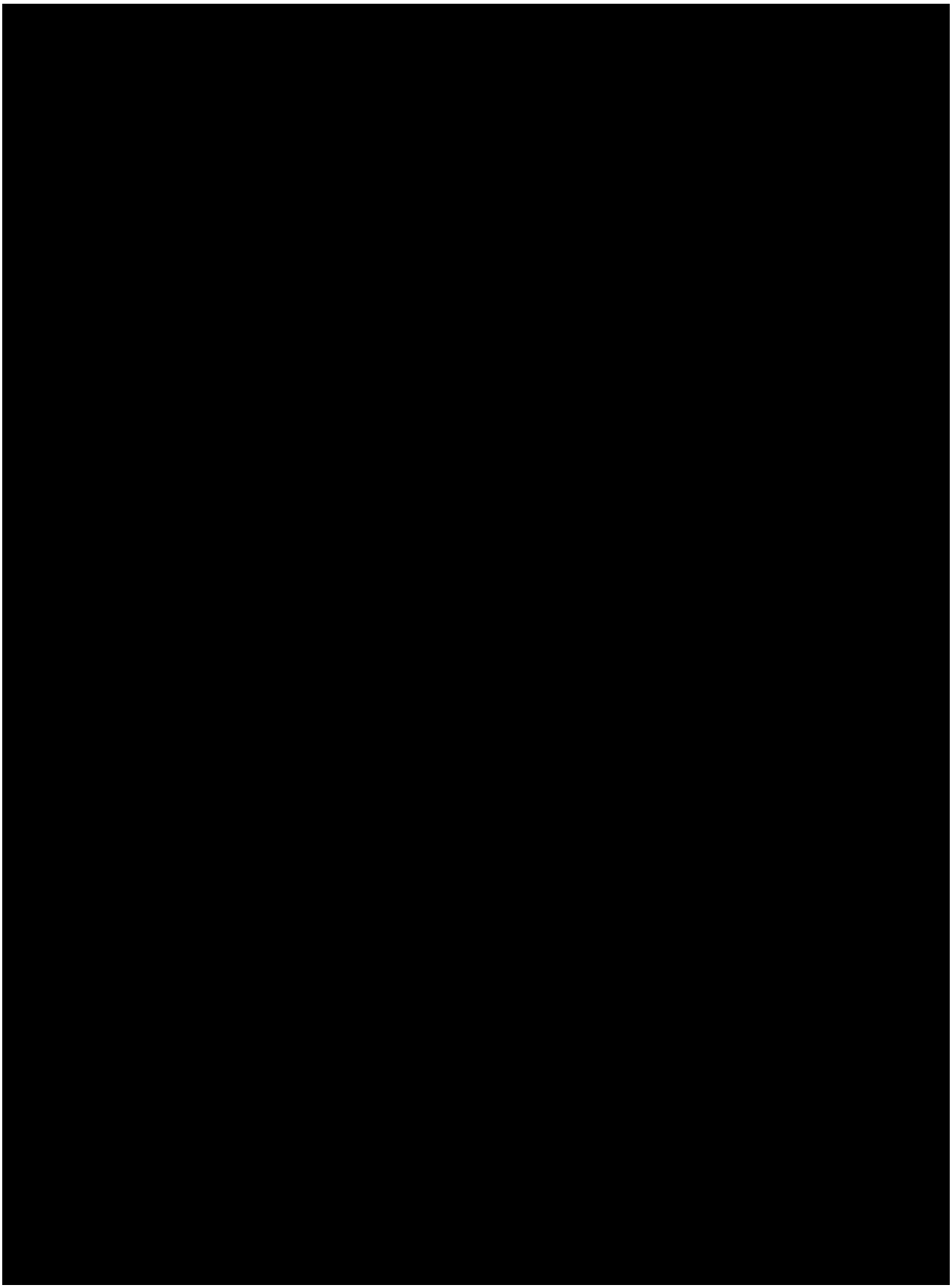
Eliminado: Análisis de brecha.

Fundamentación: De conformidad con 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 los artículos 32 y 36 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

Motivación: En virtud de que estos datos hace identificable las formas en que es posible atacar o vulnerar nuestros sistemas de información que resguardan datos personales y 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.

5. PLAN DE TRABAJO

[redacted]



[redacted]

Eliminado: Plan de trabajo.

Fundamentación: De conformidad con 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 los artículos 32 y 36 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

Motivación: En virtud de que estos datos hace identificable las formas en que es posible atacar o vulnerar nuestros sistemas de información que resguardan datos personales y 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.

6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

I. TRANSFERENCIAS DE DATOS PERSONALES

Secretaría Técnica*	
Identificador único*	EM004
(Nombre del sistema A1)*	SIAENES (Sistema de Informe Anual de Académicos de Tiempo Completo)
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:[5]	No se realizan transferencias de datos personales mediante el traslado de soportes físicos.
Transferencias mediante el traslado de soportes electrónicos:	La transferencia de datos personales e informes se hace a través del usuario ADMINISTRADOR (Secretaría de Investigación y Posgrado) mediante exportación de datos a hojas de cálculo y formato de documentos portables. Los académicos de tiempo completo, descargan su informe ingresado anualmente mediante exportación a formato de documento portable.

[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.

Transferencias mediante el traslado sobre redes electrónicas:	Actualmente no se cuenta con una infraestructura privada de almacenamiento (nube) en la ENES Unidad Morelia.

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]
2. Señalar en un listado las personas (nombre, cargo, funciones y obligaciones) que tienen acceso a los soportes físicos del sistema.[7]

El SIAENES (Sistema de Informe Anual de Académicos de Tiempo Completo) no realiza transferencia de datos personales en soportes físicos ya que todo el resguardo de los datos se hace mediante soporte electrónico mediante el uso de bases de datos relacionales y su descarga a través de hojas de cálculo y formato de documentos portables.

II. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

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

[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:

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.

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

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.

El SIAENES (Sistema de Informe Anual de Académicos de Tiempo Completo), actualmente no cuenta con una bitácora donde se almacena cierta actividad de los usuarios que ingresan al sistema, ni la actividad que realizan.

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

---

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.

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 cuenta con un procedimiento de atención de incidentes.

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 electrónicos7: 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.

a) ¿Cómo las identifica?

No se cuenta con mecanismos de identificación.

b) ¿Cómo las autentifica?

No se cuenta con mecanismos de autenticación.

c) ¿Cómo les autoriza el acceso?

No se cuenta con mecanismos de control de acceso.

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

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

Para las personas que acceden a dichos espacios interiores:

1. ¿Cómo las identifica?
   Se tiene definida una lista de acceso para el personal autorizado.
2. ¿Cómo las autentifica?
   Mediante credencial y número de trabajador.
3. ¿Cómo les autoriza el acceso?
   Si se encuentran en la lista de acceso autorizada, o si son proveedores acompañados por un empleado autorizado. Se les solicita se registren en la bitácora correspondiente.

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

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

El personal académico de tiempo completo, puede actualizar sus datos personales desde la opción “Datos personales” dentro de los rubros que debe completar para presentar su informe.

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

VII. PERFILES DE USUARIO Y CONTRASEÑAS

1. Modelo de control de acceso:

Basado en perfiles o privilegios de acceso (permisos).

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?
Únicamente las contraseñas.

4. Administración de perfiles de usuario y contraseñas:

a) ¿Quién da de alta nuevos perfiles?
El Responsable del sistema a su cargo. Lic. Gustavo Cano Salazar.

b) ¿Quién autoriza la creación de nuevos perfiles?
El Secretario Técnico autoriza la creación de nuevos perfiles con privilegios administrativos.

c) ¿Se lleva registro de la creación de nuevos perfiles?
Mediante control interno del Departamento de Sistemas Informáticos y a través del sistema.

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

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

b) ¿Requiere el administrador acceso remoto al equipo donde reside el sistema para realizar tareas de mantenimiento?
Si, con acceso mediante VPN y SSH.

c) ¿Cómo se evita el acceso remoto no autorizado?

- Se cuenta con controles de acceso basados en roles y privilegios.
- El acceso remoto a los servidores se realiza mediante conexiones VPN habilitadas únicamente a los responsables de los sistemas.
- Implementación de captcha en el inicio de sesión del sistema.

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

1. Señalar si realiza respaldos

a) Completos_X_, diferenciales ___ o incrementales__X_;

b) De forma automática ____ o Manual _X_,

c) Periodicidad con que los realiza: _Semestral_

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 externo.

3. Cómo y dónde archiva esos medios, y consultar los documentos: Plan de respaldos ENES Morelia y Bitácora de control de los respaldos.

4. Quién es el responsable de realizar estas operaciones (el área universitaria o un tercero). El responsable (encargado) del sistema a su cargo.

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.

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

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

No se cuenta con plan de contingencia.

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

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

Actualmente la ENES Unidad Morelia, no cuenta con sitio redundante para cubrir los incisos anteriores.

---

[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.

[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.

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*		
Identificador único*	EM004	
Nombre del sistema*	SIAENES (Sistema de Informe Anual de Académicos de Tiempo Completo)	
Recurso*	**Descripción***	**Control***
Reportes especiales de datos almacenados en el sistema.	Al solicitar reportes que no se encuentran en el sistema y su descarga en soporte electrónico, estos se generan y se descargan mediante un vínculo que vence en determinado tiempo para su descarga.	Evitar adjuntar archivos por correo electrónico porque es un servicio de terceros (Google). Una vez vencido el plazo de descarga (max. 24 horas) es imposible volver a descargar el soporte electrónico solicitado.
Reportes especiales de datos almacenados en el sistema en soportes electrónicos adjuntos por correo electrónico.	Solicitud de reportes especiales entregados en un soporte electrónico específico (hoja de cálculo, texto plano, formato de documento portable, etc.) y que se piden se adjunten por correo electrónico.	Se utiliza un programa de software libre para cifrar el archivo y personalmente se indica la contraseña para descifrar en el equipo de cómputo del usuario para utilizar el archivo que fue adjuntado por correo electrónico.

7.2 Procedimiento para la revisión de las medidas de seguridad

Secretaría Técnica*		
Identificador único*	EM004	
Nombre del sistema*	SIAENES (Sistema de Informe Anual de Académicos de Tiempo Completo)	
Medida de seguridad*	**Procedimiento***	**Responsable***
Principio del menor privilegio	Otorgar el acceso al usuario autorizado por la Secretaría técnica de acuerdo con el permiso requerido.	Encargado del sistema. Lic. Gustavo Cano Salazar. (01 día hábil).
Respaldos del sistema y base de datos.	Generación de archivos de respaldo tanto del sistema web como de la base de datos y control de bitácoras de respaldo.	Encargado del sistema. Lic. Gustavo Cano Salazar. (01 día hábil).
Sincronizar la fecha y hora con el servidor NTP (Network Time Protocol) oficial de la UNAM	Revisiones periódicas de la hora y fecha del servidor donde se encuentra el sistema.	Mtro. Froylan Hernández Rendón (01 día hábil).
Instalar y mantener actualizado el software antimalware.	Revisión y actualización de la versión del software antivirus y de la base de datos.	Mtro. Froylan Hernández Rendón (01 día hábil).
Instalar las actualizaciones de seguridad más recientes disponibles.	Revisión y actualizaciones del sistema operativo.	Mtro. Froylan Hernández Rendón (02 días hábiles).

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

Secretaría Técnica*	
Identificador único*	EM004

Nombre del sistema*	SIAENES (Sistema de Informe Anual de Académicos de Tiempo Completo)	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***
Principio del menor privilegio	Se encontró que todas las cuentas de usuarios del sistema cuentan con los permisos correspondientes.	Encargado del sistema. Lic. Gustavo Cano Salazar.
Respaldo del sistema y base de datos.	Se cuenta con respaldos actualizados de la información del sistema.	Encargado del sistema. Lic. Gustavo Cano Salazar.
Sincronizar la fecha y hora con el servidor NTP (Network Time Protocol) oficial de la UNAM	La fecha y hora están sincronizadas con el servidor NTP de la UNAM.	Mtro. Froylán Hernández Rendón.
Instalar y mantener actualizado el software antimalware.	El Software antivirus está actualizado.	Mtro. Froylán Hernández Rendón.
Instalar las actualizaciones de seguridad más recientes disponibles.	El sistema operativo cuenta con las actualizaciones correspondientes.	Mtro. Froylán Hernández Rendón.

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

Secretaría Técnica*		
Identificador único*	EM004	
Nombre del sistema*	SIAENES (Sistema de Informe Anual de Académicos de Tiempo Completo)	
Medida de seguridad*	**Acciones***	**Responsable***
Uso de certificados SSL	Implementar el protocolo “HTTPS” en el sistema.	Mtro. Froylán Hernández Rendón

	Realizar la renovación anual del certificado SSL para el subdominio donde se encuentra el sistema.	

8 PROGRAMA ESPECÍFICO DE CAPACITACIÓN

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

Secretaría Técnica*			
Identificador único*	EM004		
Nombre del sistema*	SIAENES (Sistema de Informe Anual de Académicos de Tiempo Completo)		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Capacitación para la Protección de Datos Personales	Curso en línea	25 horas. Fecha de inicio: 20 de noviembre de 2020. Fecha de término: 17 de enero de 2021	Público objetivo: Enlaces de Transparencia, Responsables de Seguridad de Datos Personales, Responsables de Tecnologías de la Información, así como funcionarios y empleados universitarios. Sin vigencia. Sin frecuencia de actualización.
Medidas de Seguridad Técnicas para la Protección de Datos Personales	Curso en línea	25 horas.	Público objetivo: Enlaces de Transparencia, Responsables de Seguridad de Datos Personales,

		Fecha de inicio: 8 de febrero de 2021. Fecha de término: 14 de marzo de 2021.	Responsables de Tecnologías de la Información, así como funcionarios y empleados universitarios. Sin vigencia. Sin frecuencia de actualización.
Elaboración de Documento de Seguridad y Sistema de Gestión de Seguridad de Datos Personales de las áreas universitarias	Curso en línea	25 horas. Fecha de inicio: 25 de marzo de 2022 Fecha de término: 25 de marzo de 2022.	Público objetivo: Enlaces de Transparencia, Responsables de Seguridad de Datos Personales, Responsables de Tecnologías de la Información, así como funcionarios y empleados universitarios. Sin vigencia. Sin frecuencia de actualización.
La importancia de la protección de datos personales	Seminario en línea	1 hora. Fecha: 16 de junio de 2022.	Público en general. Sin vigencia. Sin frecuencia de actualización.

8.2 Programa de difusión de la protección a los datos personales

Secretaría Técnica*	
Identificador único*	EM004

Nombre del sistema*	SIAENES (Sistema de Informe Anual de Académicos de Tiempo Completo)		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Indique actividad, tema, recursos para la difusión. Agregar un renglón por cada elemento	*Describa el tipo de elemento, sus objetivos y forma de impartición, publicación o distribución*	*Indique duración del elemento en horas, días, meses, su fecha de inicio y de término*	*Mencione público objetivo, vigencia del elemento y frecuencia de actualización*

Actualmente, no se cuenta con un programa de difusión de la protección de datos personales.

9 MEJORA CONTINUA

9.1 Actualización y mantenimiento de sistemas de información

Secretaría Técnica*			
Identificador único*	EM004		
Nombre del sistema*	SIAENES (Sistema de Informe Anual de Académicos de Tiempo Completo)		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Actualización de tecnologías de desarrollo	1.Solicitud de actualización de la arquitectura de desarrollo del sistema de datos personales. 2. Corregir y/o actualizar módulos del sistema. 3. Pruebas unitarias e integrales de las actualizaciones realizadas al sistema.	12 meses	“Back-end” del sistema.

	4. Actualización de archivos de sistema y/o sentencias de bases de datos en servidor de producción.		

9.2 Actualización y mantenimiento de equipo de cómputo

Secretaría Técnica*			
Identificador único*	EM004		
Nombre del sistema*	SIAENES (Sistema de Informe Anual de Académicos de Tiempo Completo)		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Indique actividad. Agregar un renglón por cada elemento	*Describa el tipo de actividad, sus objetivos e impacto la actualización o mantenimiento del equipo de cómputo*	*Indique duración en la ejecución de la actividad en horas, días, meses, su fecha de inicio y de término*	*Mencione los aspectos de equipo de cómputo que son resueltos, total o parcialmente, por la actividad.*

Actualmente, no se han asignado recursos para la actualización del equipo de cómputo.

9.3 Procesos para la conservación, preservación y respaldos de información

Secretaría Técnica*	
Identificador único*	EM004

Nombre del sistema*	SIAENES (Sistema de Informe Anual de Académicos de Tiempo Completo)	
Proceso*	**Descripción***	**Responsable***
Poner en fase de “mantenimiento” del sistema.	Se coloca un mensaje en la parte de acceso al sistema con un aviso de “mantenimiento” y de ser posible la fecha de “regreso” a la operación del sistema.	Encargado del sistema: Lic. Gustavo Cano Salazar. (01 día hábil).
Ingresar remotamente al servidor.	Acceso al servidor de manera remota para realizar el respaldo de ambos componentes (script del sistema y de la base de datos)	Encargado del sistema: Lic. Gustavo Cano Salazar. (01 día hábil).
Descarga de respaldos del sistema a soporte físico electrónico.	Descarga directa al Disco Duro externo proporcionado por secretaría técnica con los respaldos realizados del sistema.	Encargado del sistema: Lic. Gustavo Cano Salazar. (01 día hábil).
Salida del servidor y de fase de “mantenimiento” en el sistema.	Quitar el mensaje del modo mantenimiento del sistema y salida completa del servidor.	Encargado del sistema: Lic. Gustavo Cano Salazar. (01 día hábil).
El proceso de respaldo de información se encuentra contenido en el documento: Plan de respaldos ENES Morelia	El proceso se describe en el documento: Plan de respaldos ENES Morelia	Encargado del sistema: Lic. Gustavo Cano Salazar. (01 día hábil).

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

Secretaría Técnica*		
Identificador único*	EM004	
(Nombre del sistema A1)*	SIAENES (Sistema de Informe Anual de Académicos de Tiempo Completo)	
Proceso*	**Descripción***	**Responsable***
Borrado de datos mediante sistema (jnterfaz).	En la interfaz se tienen habilitadas opciones de “Actualizar y/o borrar datos” para los usuarios del sistema.	Encargado del sistema: Lic. Gustavo Cano Salazar.
Borrado de datos dentro del Sistema Gestor de Base de Datos.	Aplicación de transacciones y ejecución de instrucciones SQL para actualización y/o borrado de datos. Una vez completada la transacción aplicar la instrucción correspondiente para conservar o borrar definitivamente los datos.	Encargado del sistema: Lic. Gustavo Cano Salazar.
El proceso se encuentra contenido en el documento: Borrado Seguro ENES Morelia	El proceso se describe en el documento: Borrado Seguro ENES Morelia	Borrado seguro: Encargado del sistema: Lic. Gustavo Cano Salazar. Responsable de la disposición final de equipos o componentes de cómputo: Mtro. Froylán Hernández Rendón Tiempo máximo de ejecución: 05 días hábiles.

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

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

(Informar y describir el procedimiento para la cancelación de un sistema de tratamiento de datos personales.)[13]

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

a) Denominación
b) Motivo de la cancelación

B) PLAZOS Y CONDICIONES PARA EL BLOQUEO DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES:[14]

(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)

---

[13] 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.

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

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

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

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

(Describir las técnicas para la eliminación física del sistema)

SISTEMA DE CONTRATACIÓN TEMPORAL DE PROFESORES DE ASIGNATURA, INTERINOS Y AYUDANTES DE PROFESOR

Sistema web que administra el proceso de contratación de profesores y ayudantes a nivel asignatura, es decir, de aquellos profesores(as) que son seleccionados únicamente para impartir asignaturas específicas y/o coadyuvar con los profesores titulares de las 13 licenciaturas de la ENES Unidad Morelia en modalidad escolarizada y a distancia; asimismo, de las asignaturas de posgrados, formación complementaria, mediateca y actividades deportivas.

Este sistema está “conectado” al sistema CRONOS (Banco de Horas y Horarios) para intercomunicarse mutuamente cuando una vez aprobadas las contrataciones por Consejo Técnico de la escuela, se haga el registro automatizado de los profesores y/o ayudantes en las licenciaturas, posgrados y programas extracurriculares de la escuela para que en el proceso ya mencionado del otro sistema se haga el registro de bancos de horas y horarios del semestre lectivo.

ANEXO I: Documento de Seguridad de datos personales

ÍNDICE

INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Secretaría Técnica	
Identificador único*	EM005
Nombre del sistema*	Sistema de contratación temporal de profesores de asignatura, interinos y ayudantes de profesor
Datos personales (sensibles o no) contenidos en el sistema*:	● Datos personales de candidato(a) cuando se registra en el sistema (aplica para actualización). o Primer apellido o Segundo apellido o Nombre(s) o Sexo o Domicilio completo o Correo electrónico o Teléfono particular o Teléfono celular o RFC con homoclave o CURP o Institución de procedencia o Número de trabajador UNAM (en caso de que ya cuente con dicho dato) o Grado máximo de estudios o Responder si cuenta con beca o Tipo de beca (si cuenta con una) o Área en la que se desempeña o Intereses académicos o Experiencia docente o Currículum Vitae (Archivo PDF)
Responsable*:	Escuela Nacional de Estudios Superiores Unidad Morelia
Nombre*:	Dr. Santiago Cortés Hernández
Cargo*:	Secretario Técnico
Funciones*:	Decidir sobre el tratamiento automatizado de los datos personales, así como el contenido, finalidad y uso del sistema.
Obligaciones*:	- Decidir a qué usuarios se le da acceso al sistema con privilegios administrativos. - Decidir sobre la incorporación de nuevas funcionalidades en el sistema. - Vigilar que el sistema cumpla con todas las medidas de seguridad técnicas, físicas y administrativas.

	Encargados[1]:
(Nombre del Encargado 1*)	Lic. Gustavo Cano Salazar
Cargo*:	Técnico Académico, responsable del Depto. de Sistemas Informáticos de la ENES Unidad Morelia.
Funciones*:	Análisis, diseño, implementación, mantenimiento, documentación, soporte y capacitación de usuarios, sobre los diversos sistemas informáticos a su cargo en operación de la ENES Unidad Morelia.
Obligaciones*:	● Vigilar la operación correcta del sistema durante el periodo de mayor uso de este (inicios y fin de cada semestre). ● Registrar, actualizar, eliminar datos según requerimiento por escrito de la Secretaría Técnica y/o los usuarios que utilizan el sistema. ● Monitorear la protección de los datos personales contenidos en el sistema mediante la implementación de estrategias y mecanismos de seguridad en su desarrollo y mantenimiento, a nivel interno y externo.
	Usuarios:
(Nombre del Usuario 1*)	Dr. Hernando Alonso Rodríguez Correa
Cargo*:	Secretario Académico / Profesor de carrera asociado “C”.
Funciones*:	Vigilar, dirigir y controlar los procesos de contratación que se llevan a cabo semestralmente en la ENES Unidad Morelia, verificando que se lleven a cabo cada una de las etapas que componen este sistema a que se realicen en tiempo y forma.
Obligaciones*:	Cumplir con la obligación legal de resguardar los datos personales de los candidatos(as) registrados en el sistema utilizando la información solo con fines administrativos.
(Nombre del Usuario 2*)	Lic. Daniel Barajas Gutiérrez
Cargo*:	Asistente de la Secretaría Académica
Funciones*:	▪ Consulta de candidatos registrados en el sistema (todos aquellos que hayan sido contratados o no. Visualiza datos personales y consultar el CV adjunto en formato de documento portable por el candidato(a). ▪ Consulta de solicitudes de contratación realizadas por los Coordinadores de Área. ▪ Consulta y descarga de oficios de contratación

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

	(formato de documento portable) generados por sistema y de acuerdo con las aprobaciones realizadas en sesiones de Consejo Técnico por la asistente del máximo órgano colegiado de la escuela. ▪ Consulta y descarga de contrataciones organizadas en hoja de cálculo que requiere le Jefatura de Personal de la escuela para realizar el proceso de contrataciones.
Obligaciones*:	Cumplir con la obligación legal de resguardar los datos personales de los candidatos(as) registrados en el sistema utilizando la información solo con fines administrativos.
(Nombre del Usuario 3*)	Lic. Katia Marcela Méndez Flores
Cargo*:	Secretaria Auxiliar del H. Consejo Técnico
Funciones*:	▪ Consulta y descarga de solicitudes de contratación de candidatos aprobados por comité académico de cada licenciatura en hoja de cálculo. ▪ Consulta y aprobación de solicitudes de la convocatoria actual para revisión posterior de oficio único. ▪ Consulta y aprobación de bajas de contratación por casos especiales de la convocatoria actual. ▪ Consulta y descarga en formato de documento portable, las actas de comité académico de cada licenciatura, posgrado y/o programa extracurricular generado por cada una de las licenciaturas a través del coordinador de área. ▪ Generación del oficio único de contratación en formato de documento portable una vez realizadas las aprobaciones de Consejo Técnico a través del sistema. ▪ Consulta de todos los oficios únicos generados a través del sistema y con posibilidad de descarga en formato de documento portable.
Obligaciones*:	Cumplir con la obligación legal de resguardar los datos personales de los candidatos(as) registrados en el sistema y de los oficios generados tanto en soporte físico como electrónico utilizando la información con fines administrativos.
(Nombre del Usuario 4*)	Mtro. Sergio Ruíz Ávalos

Cargo*:	Jefe de Personal de la ENES Unidad Morelia
Funciones*:	▪ Oficio de justificación de actividades que es un documento que se genera en el sistema en soporte electrónico de documento portable. Se requiere únicamente para ayudantes de asignatura y solicitados por la Dirección General de Personal de la UNAM. ▪ Consulta y descarga de oficios de contratación generados en soporte de documento portable por la secretaria auxiliar del H. Consejo Técnico. ▪ Consulta y descarga de contrataciones en soporte electrónico Excel solicitado por este usuario para realizar el proceso de gestión de contrataciones del semestre a iniciar.
Obligaciones*:	Cumplir con la obligación legal de resguardar los datos personales de los candidatos(as) registrados y aprobadas sus contrataciones en el sistema utilizando la información solo con fines administrativos.
(Nombre del Usuario 5*)	Dra. María del Río Francos
Cargo*:	Coordinadora de Área 1: Físico-Matemáticas y de las ingenierías.
Funciones*:	▪ Realiza las gestiones de contrataciones de las licenciaturas: Geociencias, Tecnologías para la Información en Ciencias, Ciencia de Materiales Sustentables. ▪ Oferta las asignaturas de la convocatoria de solicitud de candidatos a impartir una asignatura en el siguiente semestre inmediato. ▪ Edición de las asignaturas ofertadas en dicha convocatoria de acuerdo con las necesidades de la licenciatura, posgrado o programa extracurricular complementario. ▪ Consulta y descarga en hoja de cálculo de los candidatos(as) registrados en la convocatoria abierta para este cometido. ▪ Selección de los candidatos registrados para la posterior generación del acta de comité académico. ▪ Solicitud de una baja de contratación de una convocatoria inmediata anterior por razones inherentes al profesor.

	▪ Generar el acta de comité académico en soporte electrónico de documento portable, una vez sesionado para recabar las firmas autógrafas de los miembros incluidos en el oficio y entregar físicamente el documento al asistente de la secretaría académica. ▪ Consulta y descarga en soporte electrónico de formato de documento portable de las actas de comité académico de las diversas convocatorias lanzadas de contratación. ▪ Consulta y descarga en soporte electrónico de hoja de cálculo de las asignaturas ofertadas de convocatorias de contratación anteriores. ▪ Consulta y descarga en soporte electrónico de hoja de cálculo de los candidatos(as) registrados en convocatorias anteriores.
Obligaciones*:	Cumplir con la obligación legal de resguardar los datos personales de los candidatos(as) registrados en el sistema y de los documentos generados en soporte electrónico y físico utilizando la información solo con fines administrativos.
(Nombre del Usuario 6*)	Dra. Lucero Sevillano García-Mayeya
Cargo*:	Coordinadora de Área 2: Ciencias Biológicas y de la Salud
Funciones*:	▪ Realiza las gestiones de contrataciones de las licenciaturas: Ciencias Ambientales, Ecología y Ciencias Agroforestales ▪ Oferta las asignaturas de la convocatoria de solicitud de candidatos a impartir una asignatura en el siguiente semestre inmediato. ▪ Edición de las asignaturas ofertadas en dicha convocatoria de acuerdo con las necesidades de la licenciatura, posgrado o programa extracurricular complementario. ▪ Consulta y descarga en soporte electrónico de hoja de cálculo de los candidatos(as) registrados en la convocatoria abierta para este cometido. ▪ Selección de los candidatos registrados para la posterior generación del acta de comité académico. ▪ Solicitud de una baja de contratación de una convocatoria inmediata anterior por razones

	inherentes al profesor. ▪ Generar el acta de comité académico en soporte electrónico de formato de documento portable, una vez sesionado para recabar las firmas autógrafas de los miembros incluidos en el oficio y entregar físicamente el documento al asistente de la secretaría académica. ▪ Consulta y descarga en soporte electrónico de formato de documento portable de las actas de comité académico de las diversas convocatorias lanzadas de contratación. ▪ Consulta y descarga en soporte electrónico de hoja de cálculo de las asignaturas ofertadas de convocatorias de contratación anteriores. ▪ Consulta y descarga en soporte electrónico de hoja de cálculo de los candidatos(as) registrados en convocatorias anteriores.
Obligaciones*:	Cumplir con la obligación legal de resguardar los datos personales de los candidatos(as) registrados en el sistema y de los documentos generados en soporte electrónico y físico utilizando la información solo con fines administrativos.
(Nombre del Usuario 7*)	Dra. Nuri Celene Fuerte Álvarez
Cargo*:	Coordinadora de Área 3: Ciencias Sociales y Posgrado
Funciones*:	▪ Realiza las gestiones de contrataciones de las licenciaturas: Estudios Sociales y Gestión Local, Geohistoria y los programas de posgrado de la ENES Unidad Morelia. ▪ Oferta las asignaturas de la convocatoria de solicitud de candidatos a impartir una asignatura en el siguiente semestre inmediato. ▪ Edición de las asignaturas ofertadas en dicha convocatoria de acuerdo con las necesidades de la licenciatura, posgrado o programa extracurricular complementario. ▪ Consulta y descarga en soporte electrónico de hoja de cálculol de los candidatos(as) registrados en la convocatoria abierta para este cometido. ▪ Selección de los candidatos registrados para la posterior generación del acta de comité académico.

	▪ Solicitud de una baja de contratación de una convocatoria inmediata anterior por razones inherentes al profesor. ▪ Generar el acta de comité académico en soporte electrónico de formato de documento portable, una vez sesionado para recabar las firmas autógrafas de los miembros incluidos en el oficio y entregar físicamente el documento al asistente de la secretaría académica. ▪ Consulta y descarga en soporte electrónico de formato de documento portable de las actas de comité académico de las diversas convocatorias lanzadas de contratación. ▪ Consulta y descarga en soporte electrónico de hoja de cálculo de las asignaturas ofertadas de convocatorias de contratación anteriores. ▪ Consulta y descarga en soporte electrónico hoja de cálculo de los candidatos(as) registrados en convocatorias anteriores.
Obligaciones*:	Cumplir con la obligación legal de resguardar los datos personales de los candidatos(as) registrados en el sistema y de los documentos generados en soporte electrónico y físico utilizando la información solo con fines administrativos.
(Nombre del Usuario 8*)	Mtra. Beatriz Alejandra Pimentel Ávila
Cargo*:	Coordinadora de Área 4: Humanidades y Artes
Funciones*:	▪ Realiza las gestiones de contrataciones de las licenciaturas: Literatura Intercultural, Historia del Arte, Arte y Diseño, Administración de Archivos y Gestión Documental y Música y Tecnología Artística. ▪ Oferta las asignaturas de la convocatoria de solicitud de candidatos a impartir una asignatura en el siguiente semestre inmediato. ▪ Edición de las asignaturas ofertadas en dicha convocatoria de acuerdo con las necesidades de la licenciatura, posgrado o programa extracurricular complementario. ▪ Consulta y descarga en soporte electrónico de hoja de cálculo de los candidatos(as) registrados en la convocatoria abierta para este cometido.

	▪ Selección de los candidatos registrados para la posterior generación del acta de comité académico. ▪ Solicitud de una baja de contratación de una convocatoria inmediata anterior por razones inherentes al profesor. ▪ Generar el acta de comité académico en soporte electrónico de formato de documento portable, una vez sesionado para recabar las firmas autógrafas de los miembros incluidos en el oficio y entregar físicamente el documento al asistente de la secretaría académica. ▪ Consulta y descarga en soporte electrónico formato de documento portable de las actas de comité académico de las diversas convocatorias lanzadas de contratación. ▪ Consulta y descarga en soporte electrónico de hoja de cálculo de las asignaturas ofertadas de convocatorias de contratación anteriores. ▪ Consulta y descarga en soporte electrónico de hoja de cálculo de los candidatos(as) registrados en convocatorias anteriores.
Obligaciones*:	▪ Cumplir con la obligación legal de resguardar los datos personales de los candidatos(as) registrados en el sistema y de los documentos generados en soporte electrónico y físico utilizando la información solo con fines administrativos.
(Nombre del Usuario 9*)	▪ Usuario genérico de comité académico
Cargo*:	Comité Académico por Licenciatura, posgrado y/o programa complementario
Funciones*:	▪ Consulta de asignaturas ofertadas por la Coordinación de Área correspondiente. ▪ Consulta de candidatos registrados por convocatoria para revisión de perfiles y sesionar para aprobar a los candidatos(as) a solicitar contratación. Visualiza los datos personales del candidato(a), su currículum vitae y las asignaturas para las cuales se postuló. Este usuario se declara como “genérico” ya que es un mismo acceso para todos los miembros del comité académico y debido a su rotación fue definido así.

Obligaciones*:	▪ Cumplir con la obligación legal de resguardar los datos personales de los candidatos(as) registrados en el sistema.

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

Secretaría Técnica	
Identificador único*	EM005
Nombre del sistema*	Sistema de contratación temporal de profesores de asignatura, interinos y ayudantes de profesor
Tipo de soporte[2]:*	Electrónico y físico.
Descripción[3]:*	Para almacenamiento de datos se utiliza un Sistema Gestor de Bases de Datos Relacional y para informes ejecutivos y reportes se generan archivos separados por comas, hojas de cálculo y formato de documentos portables. Para el soporte físico se debe preguntar a cada uno de los usuarios especificados en este documento que generan archivo en papel para su resguardo.
[redacted]	

[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.

[redacted]

Eliminado: Información específica sobre el lugar donde se resguardan los soportes de la información.

Fundamentación: De conformidad con 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 los artículos 32 y 36 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

Motivación: En virtud de que estos datos hace identificable las formas en que es posible atacar o vulnerar nuestros sistemas de información que resguardan datos personales y 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.

3. ANÁLISIS DE RIESGOS

[redacted]

[redacted]

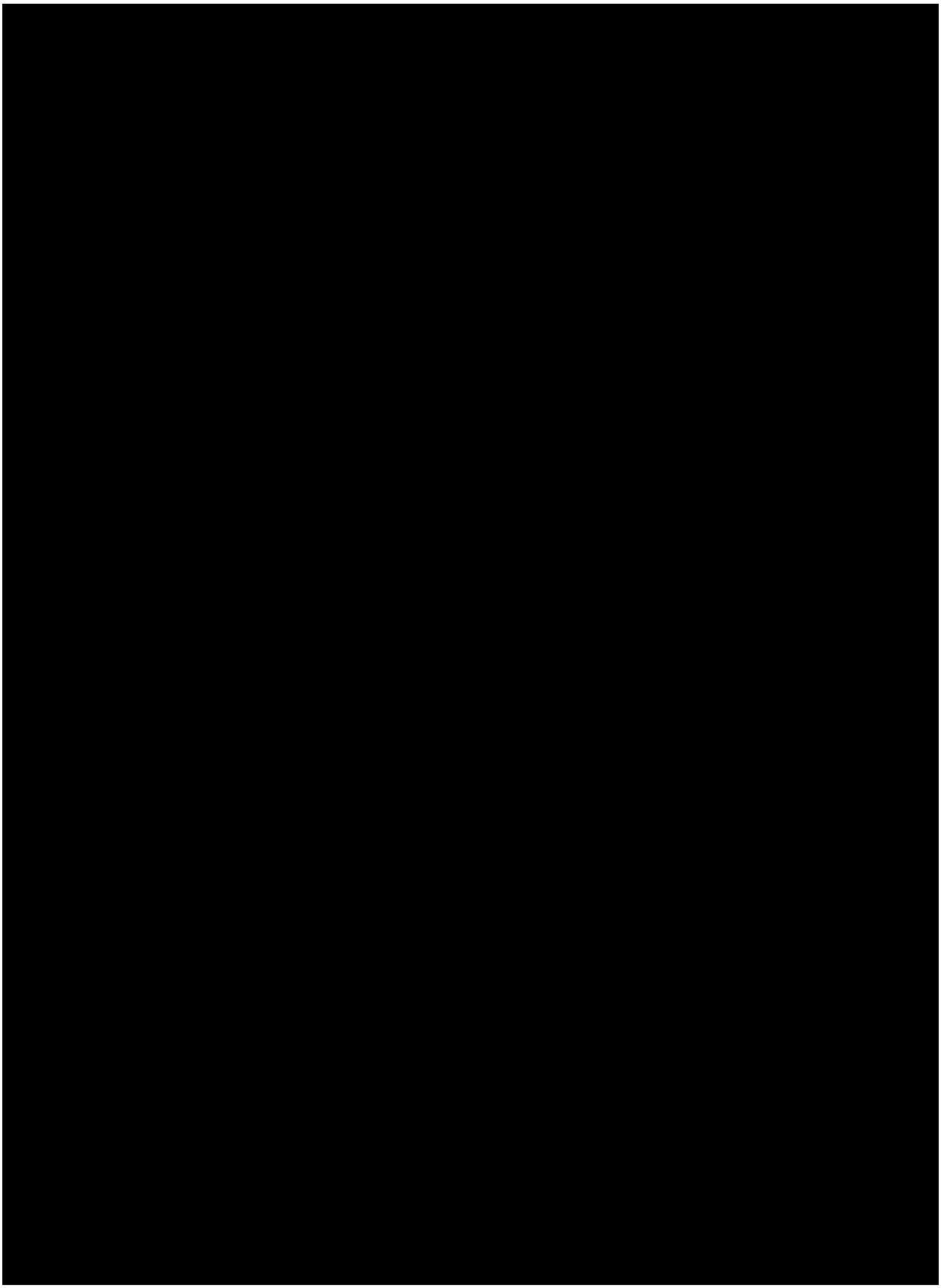
Eliminado: Análisis de riesgos.

Fundamentación: De conformidad con 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 los artículos 32 y 36 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

Motivación: En virtud de que estos datos hace identificable las formas en que es posible atacar o vulnerar nuestros sistemas de información que resguardan datos personales y 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.

4. ANÁLISIS DE BRECHA

[redacted]



[redacted]

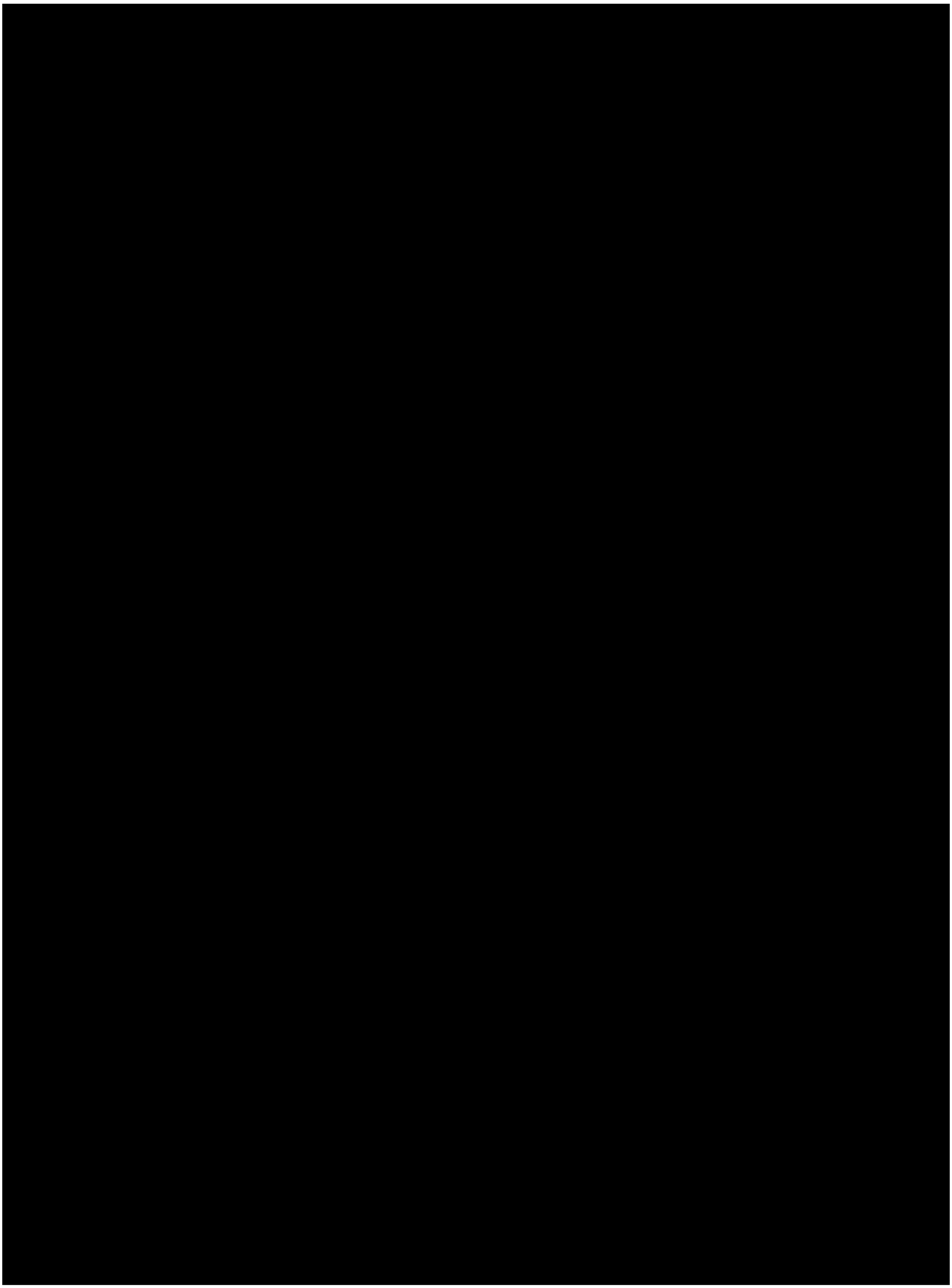
Eliminado: Análisis de brecha.

Fundamentación: De conformidad con 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 los artículos 32 y 36 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

Motivación: En virtud de que estos datos hace identificable las formas en que es posible atacar o vulnerar nuestros sistemas de información que resguardan datos personales y 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.

5. PLAN DE TRABAJO

[redacted]



[redacted]

Eliminado: Plan de trabajo.

Fundamentación: De conformidad con 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 los artículos 32 y 36 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

Motivación: En virtud de que estos datos hace identificable las formas en que es posible atacar o vulnerar nuestros sistemas de información que resguardan datos personales y 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.

6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

I. TRANSFERENCIAS DE DATOS PERSONALES

Secretaría Técnica*	
Identificador único*	EM005
(Nombre del sistema A1)*	Sistema de contratación temporal de profesores de asignatura, interinos y ayudantes de profesor
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:[5]	No se realizan transferencias de datos personales mediante el traslado de soportes físicos. Toda la visualización es de manera electrónica a menos que los usuarios administradores, coordinadores de área, asistente de secretaría académica, etc., impriman el documento generado en hojas de cálculo y formato de documentos portables.
Transferencias mediante el traslado de soportes electrónicos:	La transferencia de datos personales se hace a través del usuario Administrador, Asistente de Secretaría académica, auxiliar del consejo técnico, Coordinadores de Área y Comité Académico, con el privilegio de descarga de informes

[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.

	ejecutivos y/o reportes en hojas de cálculo y formato de documentos portables (según el permiso).
Transferencias mediante el traslado sobre redes electrónicas:	Actualmente no se cuenta con una infraestructura privada de almacenamiento (nube) en la ENES Unidad Morelia.

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]
2. Señalar en un listado las personas (nombre, cargo, funciones y obligaciones) que tienen acceso a los soportes físicos del sistema.[7]

El Sistema de contratación temporal de profesores de asignatura, interinos y ayudantes de profesor no realiza transferencia de datos personales en soportes físicos ya que todo el resguardo de los datos se hace mediante soporte electrónico mediante el uso de bases de datos relacionales y su descarga a través de hojas de cálculo formato de documentos portables.

Como se mencionó: el Secretario Académico, el asistente, la auxiliar de consejo técnico, los coordinadores de área o comité académico pueden realizar impresiones de estos documentos electrónicos generados por sistema para su resguardo físico o consulta.

II. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

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

[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:

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

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

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.

---

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.

El Sistema de contratación temporal de profesores de asignatura, interinos y ayudantes de profesor, actualmente no cuenta con una bitácora donde se almacena cierta actividad de los usuarios que ingresan al sistema, ni la actividad que realizan.

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 cuenta con un procedimiento de atención de incidentes.

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 electrónicos7: 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):

[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.

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

Para las personas que acceden a sus instalaciones:

a) ¿Cómo las identifica?
No se cuenta con mecanismos de identificación.

b) ¿Cómo las autentifica?
No se cuenta con mecanismos de autenticación.

c) ¿Cómo les autoriza el acceso?
No se cuenta con mecanismos de control de acceso.

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

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

Para las personas que acceden a dichos espacios interiores:

1. ¿Cómo las identifica?
   Se tiene definida una lista de acceso para el personal autorizado.
2. ¿Cómo las autentifica?
   Mediante credencial y número de trabajador.
3. ¿Cómo les autoriza el acceso?
   Si se encuentran en la lista de acceso autorizada, o si son proveedores acompañados por un empleado autorizado. Se les solicita se registren en la bitácora correspondiente.

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

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

En caso de detectar error y/o realizar alguna actualización de datos personales del académico se tienen dos procedimientos:

1) Si es profesor de asignatura/ayudante, mediante el sistema de contrataciones temporales de profesores de asignatura, interinos y ayudantes se realiza dicha actualización en la opción “Mi perfil” y posteriormente mediante proceso automatizado estos datos actualizados se “realimentan” en el presente sistema.
2) Para académicos de tiempo completo, técnicos académicos e invitados, la actualización de datos personales se hace a través de medio escrito (correo electrónico) ya sea del interesado o a través de su Coordinador de Área y/o Licenciatura al responsable de Sistemas Informáticos de la ENES Unidad Morelia, señalando el sistema donde se encuentra el ajuste a realizar y éste procede a realizarlo.

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

VII. PERFILES DE USUARIO Y CONTRASEÑAS

1. Modelo de control de acceso:

Basado en perfiles o privilegios de acceso (permisos).

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?
Únicamente las contraseñas.

4. Administración de perfiles de usuario y contraseñas:

a) ¿Quién da de alta nuevos perfiles?
El Responsable del sistema a su cargo. Lic. Gustavo Cano Salazar.

b) ¿Quién autoriza la creación de nuevos perfiles?
El Secretario Técnico autoriza la creación de nuevos perfiles con privilegios administrativos.

c) ¿Se lleva registro de la creación de nuevos perfiles?
Mediante control interno del Departamento de Sistemas Informáticos y a través del sistema.

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

a) ¿Requieren los usuarios acceso remoto al equipo de cómputo que por lo general utilizan para trabajar con el sistema?

No, cada usuario puede acceder al sistema desde cualquier equipo con conexión a internet y el navegador web de su preferencia.

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

Si, con acceso mediante VPN y SSH.

c) ¿Cómo se evita el acceso remoto no autorizado?

- Se cuenta con controles de acceso basados en roles y privilegios.
- El acceso remoto a los servidores se realiza mediante conexiones VPN habilitadas únicamente a los responsables de los sistemas.
- Implementación de captcha en el inicio de sesión del sistema.

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

1. Señalar si realiza respaldos

a) Completos_X_, diferenciales ___ o incrementales__X_;

b) De forma automática ____ o Manual _X_,

c) Periodicidad con que los realiza: _Semestral_

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 externo.

3. Cómo y dónde archiva esos medios, y Consultar los documentos: Plan de respaldos ENES Morelia y Bitácora de control de los respaldos.

4. Quién es el responsable de realizar estas operaciones (el área universitaria o un tercero). El responsable (encargado) del sistema a su cargo.

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.

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

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

No se cuenta con plan de contingencia.

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

[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.

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.

Actualmente la ENES Unidad Morelia, no cuenta con sitio redundante para cubrir los incisos anteriores.

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*		
Identificador único*	EM005	
Nombre del sistema*	Sistema de contratación temporal de profesores de asignatura, interinos y ayudantes de profesor	
Recurso*	**Descripción***	**Control***
Reportes especiales de datos almacenados en el sistema.	Al solicitar reportes que no se encuentran en el sistema y su descarga en soporte electrónico, estos se generan y se descargan	Evitar adjuntar archivos por correo electrónico porque es un servicio de terceros (Google).

[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.

	mediante un vínculo que vence en determinado tiempo para su descarga.	Una vez vencido el plazo de descarga (max. 24 horas) es imposible volver a descargar el soporte electrónico solicitado.
Reportes especiales de datos almacenados en el sistema en soportes electrónicos adjuntos por correo electrónico.	Solicitud de reportes especiales entregados en un soporte electrónico específico y que se piden se adjunten por correo electrónico.	Se utiliza un programa de software libre para cifrar el archivo y personalmente se indica la contraseña para descifrar en el equipo de cómputo del usuario para utilizar el archivo que fue adjuntado por correo electrónico.

7.2 Procedimiento para la revisión de las medidas de seguridad

Secretaría Técnica*		
Identificador único*	EM005	
Nombre del sistema*	Sistema de contratación temporal de profesores de asignatura, interinos y ayudantes de profesor.	
Medida de seguridad*	**Procedimiento***	**Responsable***
Principio del menor privilegio	Otorgar el acceso al usuario autorizado por la Secretaría técnica de acuerdo con el permiso requerido.	Encargado del sistema. Lic. Gustavo Cano Salazar. (01 día hábil).
Respaldos del sistema y base de datos.	Generación de archivos de respaldo tanto del sistema web como de la base de datos y control de bitácoras de respaldo.	Encargado del sistema. Lic. Gustavo Cano Salazar. (01 día hábil).
Sincronizar la fecha y hora con el servidor NTP	Revisiones periódicas de la hora y fecha del servidor	Mtro. Froylan Hernández Rendón (01 día hábil).

(Network Time Protocol) oficial de la UNAM	donde se encuentra el sistema.	
Instalar y mantener actualizado el software antimalware.	Revisión y actualización de la versión del software antivirus y de la base de datos.	Mtro. Froylan Hernández Rendón (01 día hábil).
Instalar las actualizaciones de seguridad más recientes disponibles.	Revisión y actualizaciones del sistema operativo.	Mtro. Froylan Hernández Rendón (02 días hábiles).

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

Secretaría Técnica*		
Identificador único*	EM005	
Nombre del sistema*	Sistema de contratación temporal de profesores de asignatura, interinos y ayudantes de profesor	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***
Principio del menor privilegio	Se encontró que todas las cuentas de usuarios del sistema cuentan con los permisos correspondientes.	Encargado del sistema. Lic. Gustavo Cano Salazar.
Respaldo del sistema y base de datos.	Se cuenta con respaldos actualizados de la información del sistema.	Encargado del sistema. Lic. Gustavo Cano Salazar.
Sincronizar la fecha y hora con el servidor NTP (Network Time Protocol) oficial de la UNAM	La fecha y hora están sincronizadas con el servidor NTP de la UNAM.	Mtro. Froylán Hernández Rendón.
Instalar y mantener actualizado el software antimalware.	El Software antivirus está actualizado.	Mtro. Froylán Hernández Rendón.
Instalar las actualizaciones de seguridad más recientes disponibles.	El sistema operativo cuenta con las actualizaciones correspondientes.	Mtro. Froylán Hernández Rendón.

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

Secretaría Técnica*		
Identificador único*	EM005	
Nombre del sistema*	Sistema de contratación temporal de profesores de asignatura, interinos y ayudantes de profesor	
Medida de seguridad*	**Acciones***	**Responsable***
Uso de certificados SSL	Implementar el protocolo “HTTPS” en el sistema. Realizar la renovación anual del certificado SSL para el subdominio donde se encuentra el sistema.	Mtro. Froylán Hernández Rendón

8 PROGRAMA ESPECÍFICO DE CAPACITACIÓN

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

Secretaría Técnica*			
Identificador único*	EM005		
Nombre del sistema*	Sistema de contratación temporal de profesores de asignatura, interinos y ayudantes de profesor		
Actividad*	**Descripción***	**Duración***	**Cobertura***

Capacitación para la Protección de Datos Personales	Curso en línea	25 horas. Fecha de inicio: 20 de noviembre de 2020. Fecha de término: 17 de enero de 2021	Público objetivo: Enlaces de Transparencia, Responsables de Seguridad de Datos Personales, Responsables de Tecnologías de la Información, así como funcionarios y empleados universitarios. Sin vigencia. Sin frecuencia de actualización.
Medidas de Seguridad Técnicas para la Protección de Datos Personales	Curso en línea	25 horas. Fecha de inicio: 8 de febrero de 2021. Fecha de término: 14 de marzo de 2021.	Público objetivo: Enlaces de Transparencia, Responsables de Seguridad de Datos Personales, Responsables de Tecnologías de la Información, así como funcionarios y empleados universitarios. Sin vigencia. Sin frecuencia de actualización.
Elaboración de Documento de Seguridad y Sistema de Gestión de Seguridad de Datos Personales de las áreas universitarias	Curso en línea	25 horas. Fecha de inicio: 25 de marzo de 2022 Fecha de término: 25 de marzo de 2022.	Público objetivo: Enlaces de Transparencia, Responsables de Seguridad de Datos Personales, Responsables de Tecnologías de la Información, así como funcionarios y

			empleados universitarios. Sin vigencia. Sin frecuencia de actualización.
La importancia de la protección de datos personales	Seminario en línea	1 hora. Fecha: 16 de junio de 2022.	Público en general. Sin vigencia. Sin frecuencia de actualización.

8.2 Programa de difusión de la protección a los datos personales

Secretaría Técnica*			
Identificador único*	EM005		
Nombre del sistema*	Sistema de contratación temporal de profesores de asignatura, interinos y ayudantes de profesor		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Indique actividad, tema, recursos para la difusión. Agregar un renglón por cada elemento	*Describa el tipo de elemento, sus objetivos y forma de impartición, publicación o distribución*	*Indique duración del elemento en horas, días, meses, su fecha de inicio y de término*	*Mencione público objetivo, vigencia del elemento y frecuencia de actualización*

Actualmente, no se cuenta con un programa de difusión de la protección de datos personales.

9 MEJORA CONTINUA

9.1 Actualización y mantenimiento de sistemas de información

Secretaría Técnica*			
Identificador único*	EM005		
Nombre del sistema*	Sistema de contratación temporal de profesores de asignatura, interinos y ayudantes de profesor		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Actualización de tecnologías de desarrollo	1.Solicitud de actualización de la arquitectura de desarrollo del sistema de datos personales. 2. Corregir y/o actualizar módulos del sistema. 3. Pruebas unitarias e integrales de las actualizaciones realizadas al sistema. 4. Actualización de archivos de sistema y/o sentencias de bases de datos en servidor de producción.	12 meses	“Back-end” del sistema.

9.2 Actualización y mantenimiento de equipo de cómputo

Secretaría Técnica*			
Identificador único*	EM005		
Nombre del sistema*	Sistema de contratación temporal de profesores de asignatura, interinos y ayudantes de profesor		
Actividad*	**Descripción***	**Duración***	**Cobertura***

Indique actividad. Agregar un renglón por cada elemento	*Describa el tipo de actividad, sus objetivos e impacto la actualización o mantenimiento del equipo de cómputo*	*Indique duración en la ejecución de la actividad en horas, días, meses, su fecha de inicio y de término*	*Mencione los aspectos de equipo de cómputo que son resueltos, total o parcialmente, por la actividad.*

Actualmente, no se han asignado recursos para la actualización del equipo de cómputo.

9.3 Procesos para la conservación, preservación y respaldos de información

Secretaría Técnica*		
Identificador único*	EM005	
Nombre del sistema*	Sistema de contratación temporal de profesores de asignatura, interinos y ayudantes de profesor	
Proceso*	**Descripción***	**Responsable***
Poner en fase de “mantenimiento” del sistema.	Se coloca un mensaje en la parte de acceso al sistema con un aviso de “mantenimiento” y de ser posible la fecha de “regreso” a la operación del sistema.	Encargado del sistema: Lic. Gustavo Cano Salazar. (01 día hábil).
Ingresar remotamente al servidor.	Acceso al servidor de manera remota para realizar el respaldo de ambos componentes (script del sistema y de la base de datos)	Encargado del sistema: Lic. Gustavo Cano Salazar. (01 día hábil).

Descarga de respaldos del sistema a soporte físico electrónico.	Descarga directa al Disco Duro externo proporcionado por secretaría técnica con los respaldos realizados del sistema.	Encargado del sistema: Lic. Gustavo Cano Salazar. (01 día hábil).
Salida del servidor y de fase de “mantenimiento” en el sistema.	Quitar el mensaje del modo mantenimiento del sistema y salida completa del servidor.	Encargado del sistema: Lic. Gustavo Cano Salazar. (01 día hábil).
El proceso de respaldo de información se encuentra contenido en el documento: Plan de respaldos ENES Morelia	El proceso se describe en el documento: Plan de respaldos ENES Morelia	Encargado del sistema: Lic. Gustavo Cano Salazar. (01 día hábil).

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

Secretaría Técnica*		
Identificador único*	EM005	
(Nombre del sistema A1)*	Sistema de contratación temporal de profesores de asignatura, interinos y ayudantes de profesor	
Proceso*	**Descripción***	**Responsable***
Borrado de datos mediante sistema (jnterfaz).	En la interfaz se tienen habilitadas opciones de “Actualizar y/o borrar datos” para los usuarios del sistema.	Encargado del sistema: Lic. Gustavo Cano Salazar.
Borrado de datos dentro del Sistema Gestor de Base de Datos.	Aplicación de transacciones y ejecución de instrucciones SQL para actualización y/o borrado de datos. Una vez completada la transacción	Encargado del sistema: Lic. Gustavo Cano Salazar.

	aplicar la instrucción correspondiente para conservar o borrar definitivamente los datos.	
El proceso se encuentra contenido en el documento: Borrado Seguro ENES Morelia	El proceso se describe en el documento: Borrado Seguro ENES Morelia	Borrado seguro: Encargado del sistema: Lic. Gustavo Cano Salazar. Responsable de la disposición final de equipos o componentes de cómputo: Mtro. Froylán Hernández Rendón Tiempo máximo de ejecución: 05 días hábiles.

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

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

(Informar y describir el procedimiento para la cancelación de un sistema de tratamiento de datos personales.)[13]

[13] 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

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

a) Denominación
b) Motivo de la cancelación

B) PLAZOS Y CONDICIONES PARA EL BLOQUEO DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES:[14]

(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)

---

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.

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

SISTEMA DE PRÁCTICAS DE CAMPO

Sistema web que administra el proceso de realización de prácticas y trabajos de campo que se realizan en algunas de las licenciaturas de la ENES Unidad Morelia, en algunos posgrados y por los proyectos especiales que generan los académicos y que requieren hacer investigaciones específicas de acuerdo con el trabajo que están realizando. Asimismo, aquellas actividades deportivas de formación complementaria que se llevan a cabo como torneos fuera de la entidad académica.

Con este sistema se agiliza la parte administrativa de contar con los oficios y documentos correspondientes para firma autógrafa de las partes correspondientes y asegurar a las personas que saldrán de campo para contar con un registro de las prácticas que se están llevando a cabo y monitorear el desarrollo de estas, desde su punto de salida origen hasta el punto de llegada de retorno en las fechas indicadas en el sistema.

Cabe reportar que este sistema se conecta con el ESCOLARES (EM002) para tener automatizado el proceso de los datos personales del alumno(a), de académicos y de las licenciaturas y programas de estudio que realizan estas prácticas de campo.

ANEXO I: Documento de Seguridad de datos personales

ÍNDICE

INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Secretaría Técnica	
Identificador único*	EM007
Nombre del sistema*	Sistema de Prácticas y Trabajos de Campo
Datos personales (sensibles o no) contenidos en el sistema*:	● Datos personales del alumno(a): ○ Nombre completo (apellido paterno, apellido materno, nombre) ○ Número de cuenta ○ Nacionalidad ○ Sexo ○ Fecha de nacimiento ○ CURP ○ Domicilio (Calle, número exterior e interior, colonia, entidad, delegación o municipio, código postal) ○ Teléfono 1 (fijo o móvil) ○ Teléfono 2 (fijo o móvil) ○ Correo electrónico. ○ Número de seguridad social (IMSS) ○ Número de carnet. ○ Nombre completo del beneficiario ○ Teléfono del beneficiario ○ Nombre del Padre o Tutor responsable ○ Teléfono móvil del padre o tutor responsable ○ Nombre de la madre ○ Teléfono móvil de la madre. ○ Tipo de sangre. ○ Alergias ○ Si tiene trabajo ● Datos académicos del alumno(a): ○ Licenciatura ○ Plan de estudios ○ Generación ○ Aplicación de art 22 ○ Comprobante de inscripción del alumno(a) ○ Status del alumno. ● Datos personales del académico(a) ○ Nombre completo (apellido paterno, apellido materno, nombre).
Responsable*:	Escuela Nacional de Estudios Superiores Unidad Morelia
Nombre*:	Dr. Santiago Cortés Hernández

Cargo*:	Secretario Técnico
Funciones*:	Decidir sobre el tratamiento automatizado de los datos personales, así como el contenido, finalidad y uso del sistema.
Obligaciones*:	- Decidir a qué usuarios se le da acceso al sistema con privilegios administrativos. - Decidir sobre la incorporación de nuevas funcionalidades en el sistema. - Vigilar que el sistema cumpla con todas las medidas de seguridad técnicas, físicas y administrativas.
	Encargados[1]:
(Nombre del Encargado 1*)	Lic. Gustavo Cano Salazar
Cargo*:	Técnico Académico, responsable del Depto. de Sistemas Informáticos de la ENES Unidad Morelia.
Funciones*:	Análisis, diseño, implementación, mantenimiento, documentación, soporte y capacitación de usuarios, sobre los diversos sistemas informáticos a su cargo en operación de la ENES Unidad Morelia.
Obligaciones*:	● Vigilar la operación correcta del sistema durante el periodo de mayor uso de este (inicio de semestre). ● Registrar, actualizar, eliminar datos según requerimiento por escrito de la Secretaría Técnica y/o los usuarios que utilizan el sistema (acceso mediante usuario y contraseña). ● Monitorear la protección de los datos personales contenidos en el sistema mediante la implementación de estrategias y mecanismos de seguridad en su desarrollo y mantenimiento, a nivel interno y externo.
	Usuarios:
(Nombre del Usuario 1*)	Dra. Yunuen Tapia Torres
Cargo*:	Secretaria General / Profesora de carrera asociada “C”.
Funciones*:	Vigilar, dirigir y controlar los procesos de trámites que se realizan con respecto a las prácticas y trabajos de campo registrados en el sistema.
Obligaciones*:	Cumplir con la obligación legal de resguardar los datos personales de los alumnos(as) registrados en el sistema utilizando la información con fines administrativos.
(Nombre del Usuario 2*)	L.A. Gherolinet Marillat Arreola García
Cargo*:	Asistente de Secretaría General

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

Funciones*:	▪ Consulta de prácticas y/o trabajos de campo registrados en el semestre lectivo. ▪ Bloqueo / desbloqueo de alumnos que se les impide asistir a una práctica de campo por comportamiento indebido. ▪ Consulta y descarga en hoja de cálculo y formato de documento portable de la documentación requerida para realizar los trámites ante las dependencias correspondientes para garantizar las condiciones adecuadas de una práctica de campo.
Obligaciones*:	Cumplir con la obligación legal de resguardar los datos personales de los alumnos(as) registrados en el sistema utilizando la información con fines administrativos.
(Nombre del Usuario 3*)	Médico Francisco Ambriz Vázquez
Cargo*:	Médico general de la ENES Unidad Morelia.
Funciones*:	▪ Consulta de las prácticas registradas en sistema por parte de los académicos registrados en la ENES Unidad Morelia. ▪ Consulta de los asistentes a la práctica para hacer la valoración correspondiente e ingresar datos propios del área para el almacenamiento y entregarlos en el informe médico correspondiente.
Obligaciones*:	Cumplir con la obligación legal de resguardar los datos personales médicos de los alumnos(as) registrados en el sistema utilizando la información con fines administrativos.
(Nombre del Usuario 4*)	Lic. Ana Gabriela Vargas Gómez
Cargo*:	Secretaría Académica
Funciones*:	▪ Consulta de las prácticas registradas en el periodo o semestre lectivo. (únicamente detalles de la práctica: origen, destino, fechas de regreso y salida, profesor(a) responsable, etc.). ▪ Asignación de presupuesto solicitado por el profesor(a) responsable. ▪ Consulta y descarga en soporte electrónico de hoja de cálculo de las prácticas registradas en un semestre (no se descargan datos personales de alumnos(as) y/o académicos(as)).
Obligaciones*:	Cumplir con la obligación legal de resguardar los datos

	personales de los alumnos(as) registrados en el sistema utilizando la información con fines administrativos.
(Nombre del Usuario 5*)	Académico de la ENES Unidad Morelia
Cargo*:	Docente en la ENES Unidad Morelia.
Funciones*:	▪ Registro y edición de prácticas de campo. ▪ Consulta de grupos, materias y alumnos(as) inscritos. ▪ Selección de alumnos(as) que asisten a la práctica de campo y edición de datos personales en caso de estar incompletos. ▪ Descarga de hoja de cálculo y formato de documento portable de la documentación requerida para poder realizar una práctica y/o trabajo de campo.
Obligaciones*:	Cumplir con la obligación legal de resguardar los datos personales de los alumnos(as) registrados en el sistema utilizando la información con fines administrativos.

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

Secretaría Técnica	
Identificador único*	EM007
Nombre del sistema*	Sistema de Prácticas y Trabajos de campo.
Tipo de soporte[2]:*	Electrónico
Descripción[3]:*	Para almacenamiento de datos se utiliza un Sistema Gestor de Bases de Datos Relacional y para informes ejecutivos y reportes se generan archivos separados por comas, archivos hojas de cálculo y formato de documento portable.

[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.

[redacted]

Eliminado: Información específica sobre el lugar donde se resguardan los soportes de la información.

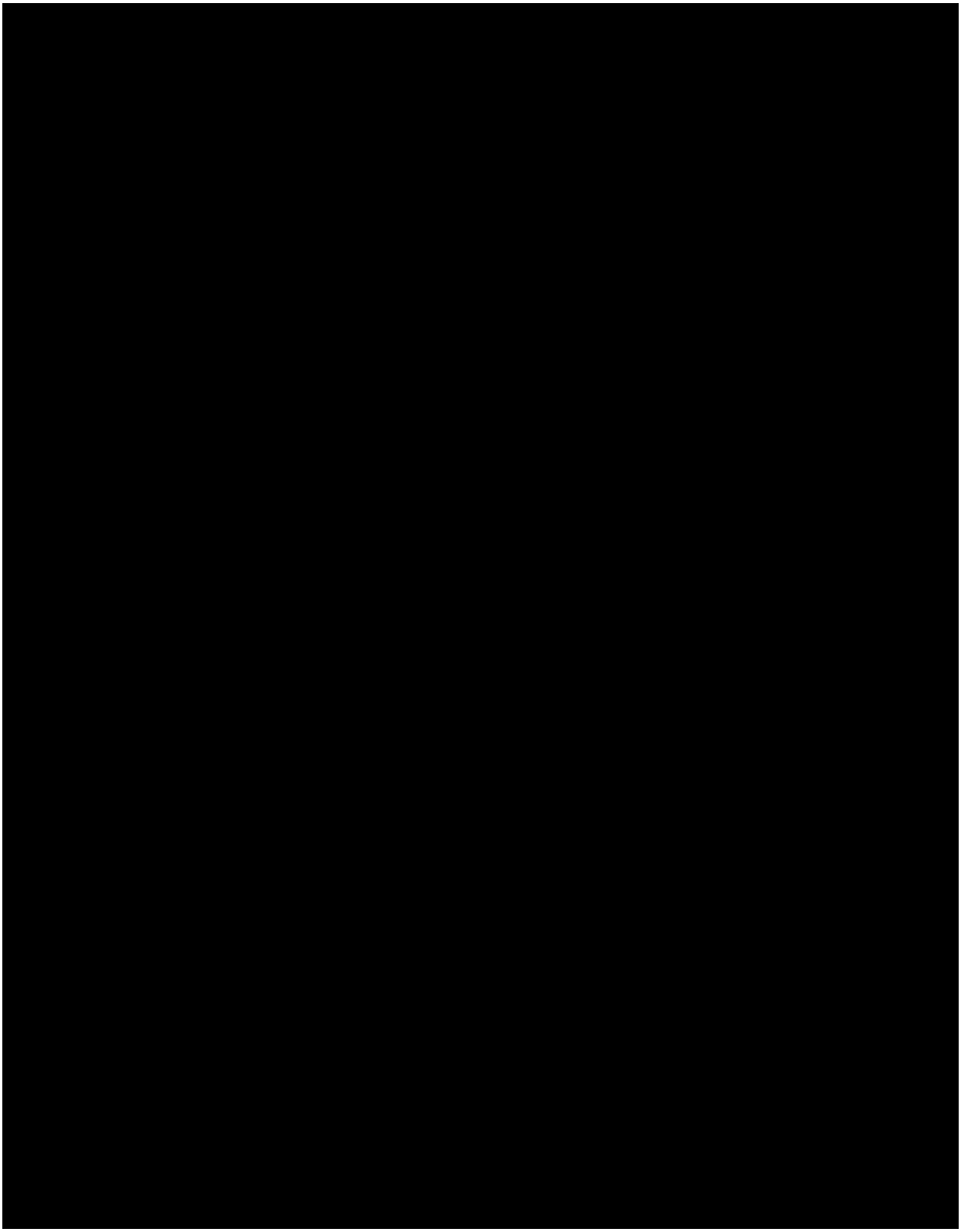
Fundamentación: De conformidad con los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública, así como los artículos 32 y 36 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

Motivación: En virtud de que estos datos hace identificable las formas en que es posible atacar o vulnerar nuestros sistemas de información que resguardan datos personales y 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.

[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



[redacted]

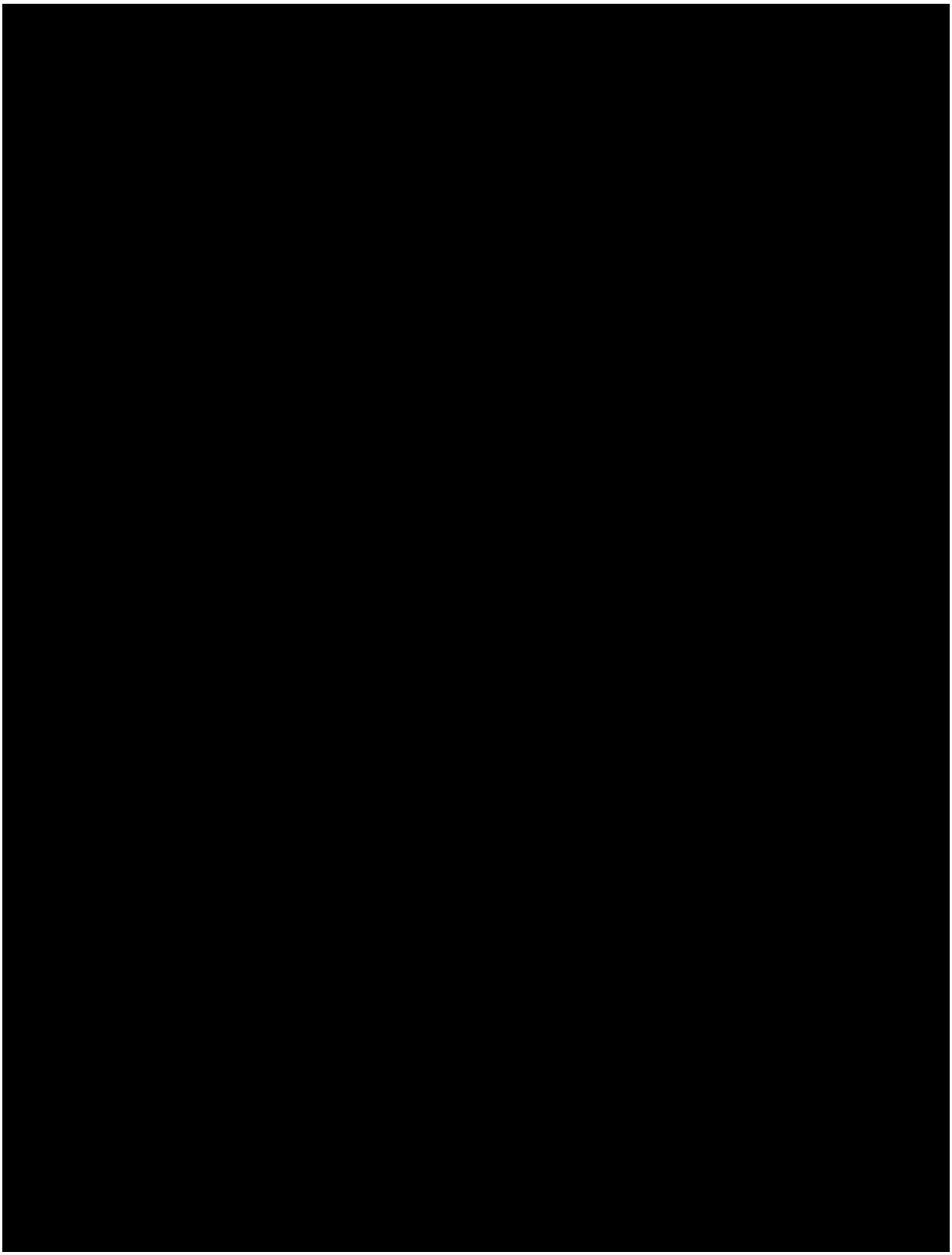
Eliminado: Análisis de riesgos.

Fundamentación: De conformidad con 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 los artículos 32 y 36 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

Motivación: En virtud de que estos datos hace identificable las formas en que es posible atacar o vulnerar nuestros sistemas de información que resguardan datos personales y 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.

4. ANÁLISIS DE BRECHA

[redacted]



[redacted]

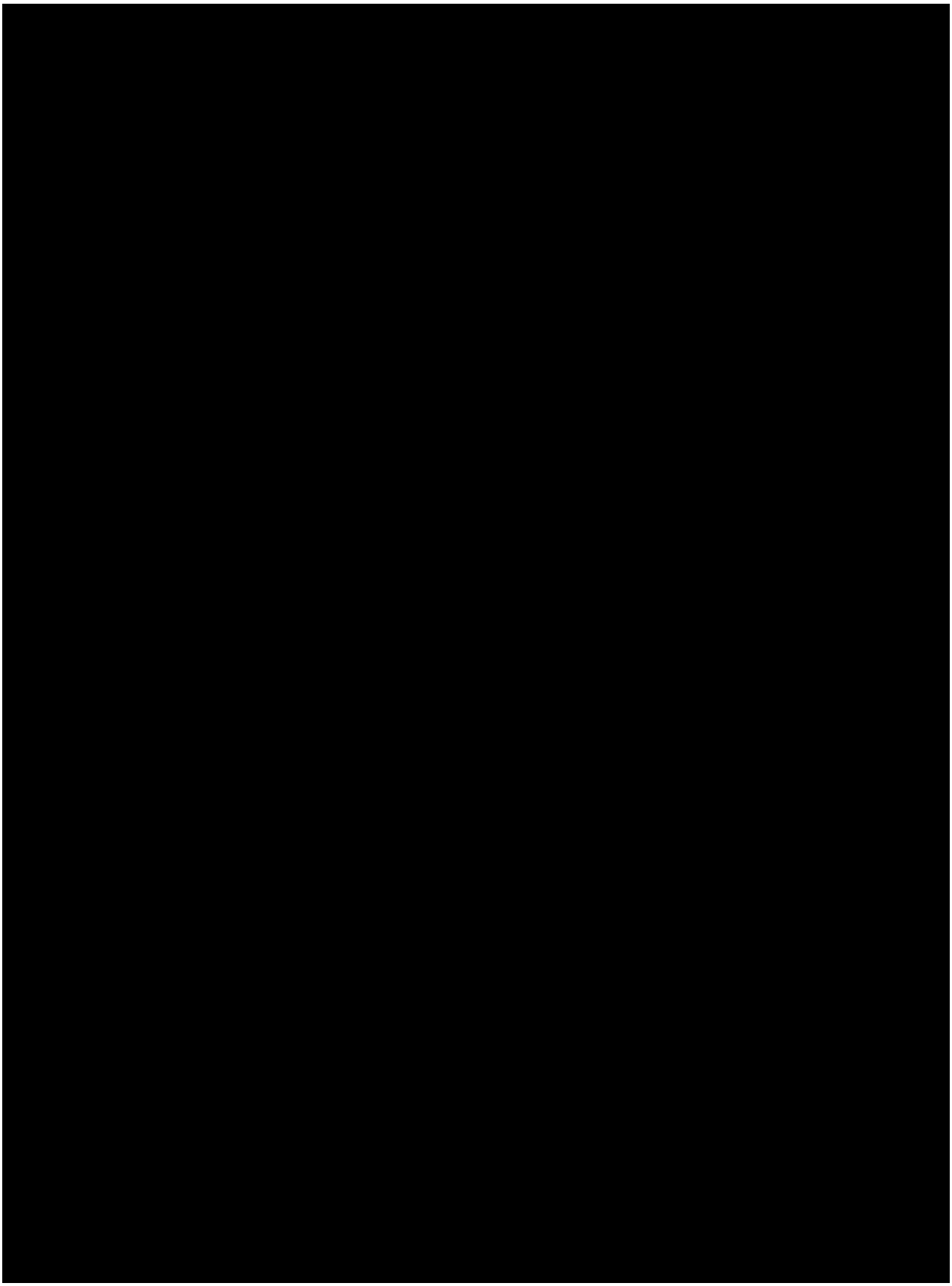
Eliminado: Análisis de brecha.

Fundamentación: De conformidad con 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 los artículos 32 y 36 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

Motivación: En virtud de que estos datos hace identificable las formas en que es posible atacar o vulnerar nuestros sistemas de información que resguardan datos personales y 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.

5. PLAN DE TRABAJO

[redacted]



Eliminado: Plan de trabajo.

Fundamentación: De conformidad con 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 los artículos 32 y 36 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

Motivación: En virtud de que estos datos hace identificable las formas en que es posible atacar o vulnerar nuestros sistemas de información que resguardan datos personales y 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.

6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

I. TRANSFERENCIAS DE DATOS PERSONALES

Secretaría Técnica*	
Identificador único*	EM007
(Nombre del sistema A1)*	Sistema de Prácticas y Trabajos de Campo
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:[5]	No se realizan transferencias de datos personales mediante el traslado de soportes físicos.
Transferencias mediante el traslado de soportes electrónicos:	La transferencia de datos personales en soportes electrónicos la pueden realizar los usuarios especificados en este documento previa identificación con credenciales de acceso (usuario y contraseña). Los soportes electrónicos solicitados se procesan en hojas de cálculo y formato de documentos portable.
Transferencias mediante el traslado sobre redes electrónicas:	Actualmente no se cuenta con una infraestructura privada de almacenamiento (nube) en la ENES Unidad Morelia.

[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.

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]

2. Señalar en un listado las personas (nombre, cargo, funciones y obligaciones) que tienen acceso a los soportes físicos del sistema.[7]

El Sistema de Prácticas y Trabajos de Campo, no realiza transferencia de datos personales en soportes físicos ya que todo el resguardo de los datos se hace mediante soporte electrónico mediante el uso de bases de datos relacionales y su descarga a través de hojas de cálculo y formatos de documento portables.

II. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

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

[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:

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

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

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.

El Sistema de Prácticas y Trabajos de Campo, actualmente no cuenta con bitácoras de acceso digitales para conocer la actividad de los usuarios autorizados dentro del sistema.

III. REGISTRO DE INCIDENTES:

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

---

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.

No se cuenta con un procedimiento de atención de incidentes.

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 electrónicos7: Los campos, registros, tablas, bases de datos o archivos electrónicos, tanto dañados como recuperados, el nombre de los sistemas y la infraestructura afectada, indicar si el incidente afectó el servidor principal y los servidores de respaldo, etc.
2. Si el registro está en soporte físico o en soporte electrónico;
3. Cómo asegura la integridad de dicho registro, y
4. Para el caso de soportes electrónicos, quién autoriza la recuperación de datos.

V. ACCESO A LAS INSTALACIONES

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

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

Para las personas que acceden a sus instalaciones:

a) ¿Cómo las identifica?

No se cuenta con mecanismos de identificación.

b) ¿Cómo las autentifica?

No se cuenta con mecanismos de autenticación.

---

[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.

c) ¿Cómo les autoriza el acceso?
No se cuenta con mecanismos de control de acceso.

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

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

Para las personas que acceden a dichos espacios interiores:

1. ¿Cómo las identifica?
   Se tiene definida una lista de acceso para el personal autorizado.
2. ¿Cómo las autentifica?
   Mediante credencial y número de trabajador.
3. ¿Cómo les autoriza el acceso?
   Si se encuentran en la lista de acceso autorizada, o si son proveedores acompañados por un empleado autorizado. Se les solicita se registren en la bitácora correspondiente.

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

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

1) Los administradores y profesores que registran las prácticas de campo pueden realizar la actualización de datos personales del alumno que sale a actividades escolares (solo puede editar: Domicilio del alumno, teléfono de localización, número de carnet del alumno).

2) Los alumnos pueden hacer este proceso desde el sistema ESCOLARES (EM002) desde la sección “Mis datos” (estos son los mismos campos que se editan en el sistema de prácticas escolares.

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

VII. PERFILES DE USUARIO Y CONTRASEÑAS

1. Modelo de control de acceso:

Basado en perfiles o privilegios de acceso (permisos).

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?
Únicamente las contraseñas.

4. Administración de perfiles de usuario y contraseñas:

a) ¿Quién da de alta nuevos perfiles?
El Responsable del sistema a su cargo. Lic. Gustavo Cano Salazar.

b) ¿Quién autoriza la creación de nuevos perfiles?
El Secretario Técnico autoriza la creación de nuevos perfiles con privilegios administrativos.

c) ¿Se lleva registro de la creación de nuevos perfiles?
Mediante control interno del Departamento de Sistemas Informáticos y a través del sistema.

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

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

b) ¿Requiere el administrador acceso remoto al equipo donde reside el sistema para realizar tareas de mantenimiento?
Si, con acceso mediante VPN y SSH.

c) ¿Cómo se evita el acceso remoto no autorizado?

- Se cuenta con controles de acceso basados en roles y privilegios.
- El acceso remoto a los servidores se realiza mediante conexiones VPN habilitadas únicamente a los responsables de los sistemas.
- Implementación de captcha en el inicio de sesión del sistema.

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

1. Señalar si realiza respaldos

a) Completos_X_, diferenciales ___ o incrementales__X_;

b) De forma automática ____ o Manual _X_,

c) Periodicidad con que los realiza: _Semestral_

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 externo.

3. Cómo y dónde archiva esos medios, y Consultar los documentos: Plan de respaldos ENES Morelia y Bitácora de control de los respaldos.

4. Quién es el responsable de realizar estas operaciones (el área universitaria o un tercero). El responsable (encargado) del sistema a su cargo.

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.

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

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

No se cuenta con plan de contingencia.

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

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

Actualmente la ENES Unidad Morelia, no cuenta con sitio redundante para cubrir los incisos anteriores.

---

[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.

[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.

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*		
Identificador único*	EM007	
Nombre del sistema*	Sistema de Prácticas y Trabajos de Campo	
Recurso*	**Descripción***	**Control***
Reportes especiales de datos almacenados en el sistema.	Al solicitar reportes que no se encuentran en el sistema y su descarga en soporte electrónico, estos se generan y se descargan mediante un vínculo que vence en determinado tiempo para su descarga.	Evitar adjuntar archivos por correo electrónico porque es un servicio de terceros (Google). Una vez vencido el plazo de descarga (max. 24 horas) es imposible volver a descargar el soporte electrónico solicitado.
Reportes especiales de datos almacenados en el sistema en soportes electrónicos adjuntos por correo electrónico.	Solicitud de reportes especiales entregados en un soporte electrónico específico (hoja de cálculo, texto plano, etc.) y que se piden se adjunten por correo electrónico.	Se utiliza un programa de software libre para cifrar el archivo y personalmente se indica la contraseña para descifrar en el equipo de cómputo del usuario para utilizar el archivo que fue adjuntado por correo electrónico.

7.2 Procedimiento para la revisión de las medidas de seguridad

Secretaría Técnica*		
Identificador único*	EM007	
Nombre del sistema*	Sistema de Prácticas y Trabajos de Campo	
Medida de seguridad*	**Procedimiento***	**Responsable***
Principio del menor privilegio	Otorgar el acceso al usuario autorizado por la Secretaría técnica de acuerdo con el permiso requerido.	Encargado del sistema. Lic. Gustavo Cano Salazar. (01 día hábil).
Respaldos del sistema y base de datos.	Generación de archivos de respaldo tanto del sistema web como de la base de datos y control de bitácoras de respaldo.	Encargado del sistema. Lic. Gustavo Cano Salazar. (01 día hábil).
Sincronizar la fecha y hora con el servidor NTP (Network Time Protocol) oficial de la UNAM	Revisiones periódicas de la hora y fecha del servidor donde se encuentra el sistema.	Mtro. Froylan Hernández Rendón (01 día hábil).
Instalar y mantener actualizado el software antimalware.	Revisión y actualización de la versión del software antivirus y de la base de datos.	Mtro. Froylan Hernández Rendón (01 día hábil).
Instalar las actualizaciones de seguridad más recientes disponibles.	Revisión y actualizaciones del sistema operativo.	Mtro. Froylan Hernández Rendón (02 días hábiles).

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

Secretaría Técnica*		
Identificador único*	EM007	
Nombre del sistema*	Sistema de Prácticas y Trabajos de Campo	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***

Principio del menor privilegio	Se encontró que todas las cuentas de usuarios del sistema cuentan con los permisos correspondientes.	Encargado del sistema. Lic. Gustavo Cano Salazar.
Respaldo del sistema y base de datos.	Se cuenta con respaldos actualizados de la información del sistema.	Encargado del sistema. Lic. Gustavo Cano Salazar.
Sincronizar la fecha y hora con el servidor NTP (Network Time Protocol) oficial de la UNAM	La fecha y hora están sincronizadas con el servidor NTP de la UNAM.	Mtro. Froylán Hernández Rendón.
Instalar y mantener actualizado el software antimalware.	El Software antivirus está actualizado.	Mtro. Froylán Hernández Rendón.
Instalar las actualizaciones de seguridad más recientes disponibles.	El sistema operativo cuenta con las actualizaciones correspondientes.	Mtro. Froylán Hernández Rendón.

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

Secretaría Técnica*		
Identificador único*	EM007	
Nombre del sistema*	Sistema e Prácticas y Trabajos de Campo	
Medida de seguridad*	**Acciones***	**Responsable***
Uso de certificados SSL	Implementar el protocolo “HTTPS” en el sistema. Realizar la renovación anual del certificado SSL para el subdominio donde se encuentra el sistema.	Mtro. Froylán Hernández Rendón

8 PROGRAMA ESPECÍFICO DE CAPACITACIÓN

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

Secretaría Técnica*			
Identificador único*	EM007		
Nombre del sistema*	Sistema de Prácticas y Trabajos de Campo		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Capacitación para la Protección de Datos Personales	Curso en línea	25 horas. Fecha de inicio: 20 de noviembre de 2020. Fecha de término: 17 de enero de 2021	Público objetivo: Enlaces de Transparencia, Responsables de Seguridad de Datos Personales, Responsables de Tecnologías de la Información, así como funcionarios y empleados universitarios. Sin vigencia. Sin frecuencia de actualización.
Medidas de Seguridad Técnicas para la Protección de Datos Personales	Curso en línea	25 horas. Fecha de inicio: 8 de febrero de 2021. Fecha de término: 14 de marzo de 2021.	Público objetivo: Enlaces de Transparencia, Responsables de Seguridad de Datos Personales, Responsables de Tecnologías de la Información, así como funcionarios y empleados universitarios.

			Sin vigencia. Sin frecuencia de actualización.
Elaboración de Documento de Seguridad y Sistema de Gestión de Seguridad de Datos Personales de las áreas universitarias	Curso en línea	25 horas. Fecha de inicio: 25 de marzo de 2022 Fecha de término: 25 de marzo de 2022.	Público objetivo: Enlaces de Transparencia, Responsables de Seguridad de Datos Personales, Responsables de Tecnologías de la Información, así como funcionarios y empleados universitarios. Sin vigencia. Sin frecuencia de actualización.
La importancia de la protección de datos personales	Seminario en línea	1 hora. Fecha: 16 de junio de 2022.	Público en general. Sin vigencia. Sin frecuencia de actualización.

8.2 Programa de difusión de la protección a los datos personales

Secretaría Técnica*			
Identificador único*	EM007		
Nombre del sistema*	Sistema de Prácticas y Trabajos de Campo		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Indique actividad, tema, recursos para la difusión. Agregar	*Describa el tipo de elemento, sus objetivos y forma*	*Indique duración del elemento en horas, días,*	*Mencione público objetivo, vigencia del*

un renglón por cada elemento	*de impartición, publicación o distribución*	*meses, su fecha de inicio y de término*	*elemento y frecuencia de actualización*

Actualmente, no se cuenta con un programa de difusión de la protección de datos personales.

9 MEJORA CONTINUA

9.1 Actualización y mantenimiento de sistemas de información

Secretaría Técnica*			
Identificador único*	EM007		
Nombre del sistema*	Sistema de Prácticas y Trabajos de Camp7		
Actividad*	**Descripción***	**Duración ***	**Cobertura***
Actualización de tecnologías de desarrollo	1.Solicitud de actualización de la arquitectura de desarrollo del sistema de datos personales. 2. Corregir y/o actualizar módulos del sistema. 3. Pruebas unitarias e integrales de las actualizaciones realizadas al sistema. 4. Actualización de archivos de sistema y/o sentencias de bases de datos en servidor de producción.	12 meses	“Back-end” del sistema.

9.2 Actualización y mantenimiento de equipo de cómputo

Secretaría Técnica*			
Identificador único*	EM007		
Nombre del sistema*	Sistema de Prácticas y Trabajos de Campo		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Indique actividad. Agregar un renglón por cada elemento	*Describa el tipo de actividad, sus objetivos e impacto la actualización o mantenimiento del equipo de cómputo*	*Indique duración en la ejecución de la actividad en horas, días, meses, su fecha de inicio y de término*	*Mencione los aspectos de equipo de cómputo que son resueltos, total o parcialmente, por la actividad.*

Actualmente, no se han asignado recursos para la actualización del equipo de cómputo.

9.3 Procesos para la conservación, preservación y respaldos de información

Secretaría Técnica*		
Identificador único*	EM007	
Nombre del sistema*	Sistema de Prácticas y Trabaos de Campo	
Proceso*	**Descripción***	**Responsable***
Poner en fase de “mantenimiento” del sistema.	Se coloca un mensaje en la parte de acceso al sistema con un aviso de “mantenimiento” y de ser posible la fecha de “regreso” a la operación del sistema.	Encargado del sistema: Lic. Gustavo Cano Salazar. (01 día hábil).

Ingresar remotamente al servidor.	Acceso al servidor de manera remota para realizar el respaldo de ambos componentes (script del sistema y de la base de datos)	Encargado del sistema: Lic. Gustavo Cano Salazar. (01 día hábil).
Descarga de respaldos del sistema a soporte físico electrónico.	Descarga directa al Disco Duro externo proporcionado por secretaría técnica con los respaldos realizados del sistema.	Encargado del sistema: Lic. Gustavo Cano Salazar. (01 día hábil).
Salida del servidor y de fase de “mantenimiento” en el sistema.	Quitar el mensaje del modo mantenimiento del sistema y salida completa del servidor.	Encargado del sistema: Lic. Gustavo Cano Salazar. (01 día hábil).
El proceso de respaldo de información se encuentra contenido en el documento: Plan de respaldos ENES Morelia	El proceso se describe en el documento: Plan de respaldos ENES Morelia	Encargado del sistema: Lic. Gustavo Cano Salazar. (01 día hábil).

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

Secretaría Técnica*		
Identificador único*	EM007	
(Nombre del sistema A1)*	Sistema de Prácticas y Trabajos de Campo	
Proceso*	**Descripción***	**Responsable***
Borrado de datos mediante sistema (jnterfaz).	En la interfaz se tienen habilitadas opciones de	Encargado del sistema: Lic. Gustavo Cano Salazar.

	“Actualizar y/o borrar datos” para los usuarios del sistema.	
Borrado de datos dentro del Sistema Gestor de Base de Datos.	Aplicación de transacciones y ejecución de instrucciones SQL para actualización y/o borrado de datos. Una vez completada la transacción aplicar la instrucción correspondiente para conservar o borrar definitivamente los datos.	Encargado del sistema: Lic. Gustavo Cano Salazar.
El proceso se encuentra contenido en el documento: Borrado Seguro ENES Morelia	El proceso se describe en el documento: Borrado Seguro ENES Morelia	Borrado seguro: Encargado del sistema: Lic. Gustavo Cano Salazar. Responsable de la disposición final de equipos o componentes de cómputo: Mtro. Froylán Hernández Rendón Tiempo máximo de ejecución: 05 días hábiles.

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

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

(Informar y describir el procedimiento para la cancelación de un sistema de tratamiento de datos personales.)[13]

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

a) Denominación
b) Motivo de la cancelación

A) PLAZOS Y CONDICIONES PARA EL BLOQUEO DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES:[14]

(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)

B) 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)

C) 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)

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

(Describir las técnicas para la eliminación física del sistema)

---

[13] 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.

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

SISTEMA DE EVALUACIÓN DOCENTE

Sistema web que automatiza el proceso de evaluación docente por parte de los alumnos que inscribieron asignaturas en el semestre cursado.

El presente sistema se conecta con ESCOLARES (EM002) para identificar al alumno inscrito y las asignaturas registradas en el semestre. Asimismo, se aprovecha esta intercomunicación para saber las licenciaturas, planes y programas de estudio, así como los datos básicos del profesor evaluado(a).

Es importante señalar que, al ser una evaluación anónima por parte del alumno, es decir, ni los administradores, coordinadores de licenciatura o profesores puede saber de manera precisa la evaluación realizada, los datos personales del alumno se mantienen aislados, identificando únicamente al alumno(a) cuando ingresa en el periodo de evaluación.

ANEXO I: Documento de Seguridad de datos personales

ÍNDICE

INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Secretaría Técnica	
Identificador único*	EM008
Nombre del sistema*	Sistema de Evaluación Docente (SIEDO)
Datos personales (sensibles o no) contenidos en el sistema*:	● Datos personales del alumno(a): o Nombre completo (apellido paterno, apellido materno, nombre) o Número de cuenta o Correo electrónico. ● Datos académicos del alumno(a): o Licenciatura o Plan de estudios o Generación o Asignaturas inscritas ● Datos personales del académico(a) o Nombre completo (apellido paterno, apellido materno, nombre).
Responsable*:	Escuela Nacional de Estudios Superiores Unidad Morelia
Nombre*:	Dr. Santiago Cortés Hernández
Cargo*:	Secretario Técnico
Funciones*:	Decidir sobre el tratamiento automatizado de los datos personales, así como el contenido, finalidad y uso del sistema.
Obligaciones*:	- Decidir a qué usuarios se le da acceso al sistema con privilegios administrativos. - Decidir sobre la incorporación de nuevas funcionalidades en el sistema. - Vigilar que el sistema cumpla con todas las medidas de seguridad técnicas, físicas y administrativas.
	Encargados[1]:
(Nombre del Encargado 1*)	Lic. Gustavo Cano Salazar
Cargo*:	Técnico Académico, responsable del Depto. de Sistemas Informáticos de la ENES Unidad Morelia.
Funciones*:	Análisis, diseño, implementación, mantenimiento, documentación, soporte y capacitación de usuarios, sobre los diversos sistemas informáticos a su cargo en operación de la ENES Unidad Morelia.
Obligaciones*:	● Vigilar la operación correcta del sistema durante el

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

	periodo de mayor uso de este (casi al final de semestre). ● Registrar, actualizar, eliminar datos según requerimiento por escrito de la Secretaría Técnica y/o los usuarios que utilizan el sistema (acceso mediante usuario y contraseña). ● Monitorear la protección de los datos personales contenidos en el sistema mediante la implementación de estrategias y mecanismos de seguridad en su desarrollo y mantenimiento, a nivel interno y externo.
	Usuarios:
(Nombre del Usuario 1*)	Mtra. Diana Moncada Vargas
Cargo*:	Jefa de la Unidad de Estrategia Educativa
Funciones*:	Vigilar, dirigir y controlar los procesos de evaluación docente que se programan cada semestre con el fin de captar la mayor evaluación por parte del alumnado y retroalimentar a los coordinadores de licenciatura para casos específicos de profesores(as) que requieran mejorar la impartición de cátedra que hacen.
Obligaciones*:	Cumplir con la obligación legal de resguardar los datos personales de los alumnos(as) y académicos(a) registrados en el sistema utilizando la información con fines únicamente académico-administrativos.
(Nombre del Usuario 2*)	Mtra. Alejandra Ceja Fernández
Cargo*:	Responsable de la Evaluación Docente / Unidad de Estrategia Educativa
Funciones*:	Vigilar, dirigir y controlar los procesos de evaluación docente que se programan cada semestre con el fin de captar la mayor evaluación por parte del alumnado y retroalimentar a los coordinadores de licenciatura para casos específicos de profesores(as) que requieran mejorar la impartición de cátedra que hacen.
Obligaciones*:	Cumplir con la obligación legal de resguardar los datos personales de los alumnos(as) y académicos(a) registrados en el sistema utilizando la información con fines únicamente académico-administrativos.
(Nombre del Usuario 3*)	Académicos(a) de Tiempo Completo.
Cargo*:	Coordinadores de Licenciatura
Funciones*:	▪ Consulta de las asignaturas registradas en su licenciatura para el semestre seleccionado. ▪ Visualización de asignatura-grupo-profesor y el promedio general obtenido en cada una de las evaluaciones ▪ Consulta a detalle del cuestionario aplicado y los comentarios generales del alumno al profesor con respecto al desarrollo de la asignatura (anónimos).

Obligaciones*:	Cumplir con la obligación legal de resguardar los datos personales los alumnos(as) y académicos(as) registrados en el sistema utilizando la información con fines académico-administrativos.
(Nombre del Usuario 4*)	Académicos de la ENES Unidad Morelia.
Cargo*:	Profesores(as)
Funciones*:	▪ Consulta de las asignaturas registradas en su licenciatura y asignadas al usuario académico que impartió clase para el semestre seleccionado. ▪ Visualización de asignatura-grupo-profesor y el promedio general obtenido en cada una de las evaluaciones. ▪ Consulta a detalle del cuestionario aplicado y los comentarios generales del alumno al profesor con respecto al desarrollo de la asignatura (anónimos).
Obligaciones*:	Cumplir con la obligación legal de resguardar los datos personales de los alumnos(as) registrados en el sistema utilizando la información con fines académicos.
(Nombre del Usuario 5*)	Alumnos(as)
Cargo*:	Alumno(a) inscrito en la ENES Unidad Morelia.
Funciones*:	▪ Consulta de asignaturas inscritas en el semestre actual. ▪ Evaluación de cada profesor registrado por las asignaturas que inscribió el alumno(a) en el semestre.
Obligaciones*:	Únicamente el dato que visualizan personal de profesor es su nombre completo, el resto de sus datos no son visibles.

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

Secretaría Técnica	
Identificador único*	EM008
Nombre del sistema*	Sistema de Evaluación Docente (SIEDO)
Tipo de soporte[2]:*	Electrónico

[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.

Descripción[3]**:***	Para almacenamiento de datos se utiliza un Sistema Gestor de Bases de Datos Relacional y para informes ejecutivos y reportes se generan formatos de documentos portables.

[redacted]

Eliminado: Información específica sobre el lugar donde se resguardan los soportes de la información.

Fundamentación: De conformidad con 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 los artículos 32 y 36 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

Motivación: En virtud de que estos datos hace identificable las formas en que es posible atacar o vulnerar nuestros sistemas de información que resguardan datos personales y 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.

3. ANÁLISIS DE RIESGOS

[redacted]

[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.

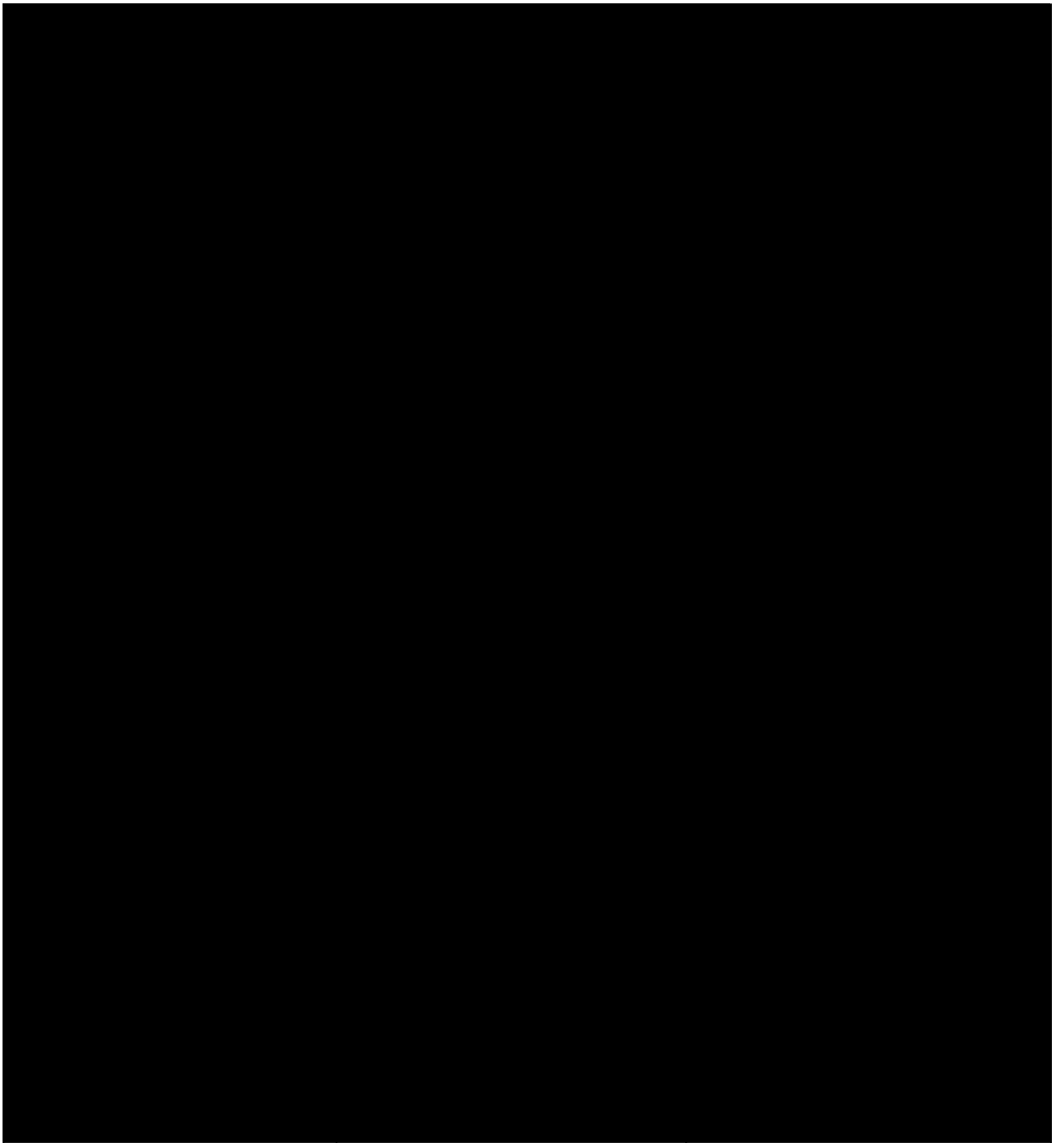
[redacted]

Eliminado: Análisis de riesgos.

Fundamentación: De conformidad con 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 los artículos 32 y 36 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

Motivación: En virtud de que estos datos hace identificable las formas en que es posible atacar o vulnerar nuestros sistemas de información que resguardan datos personales y 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.

4. ANÁLISIS DE BRECHA



[redacted]

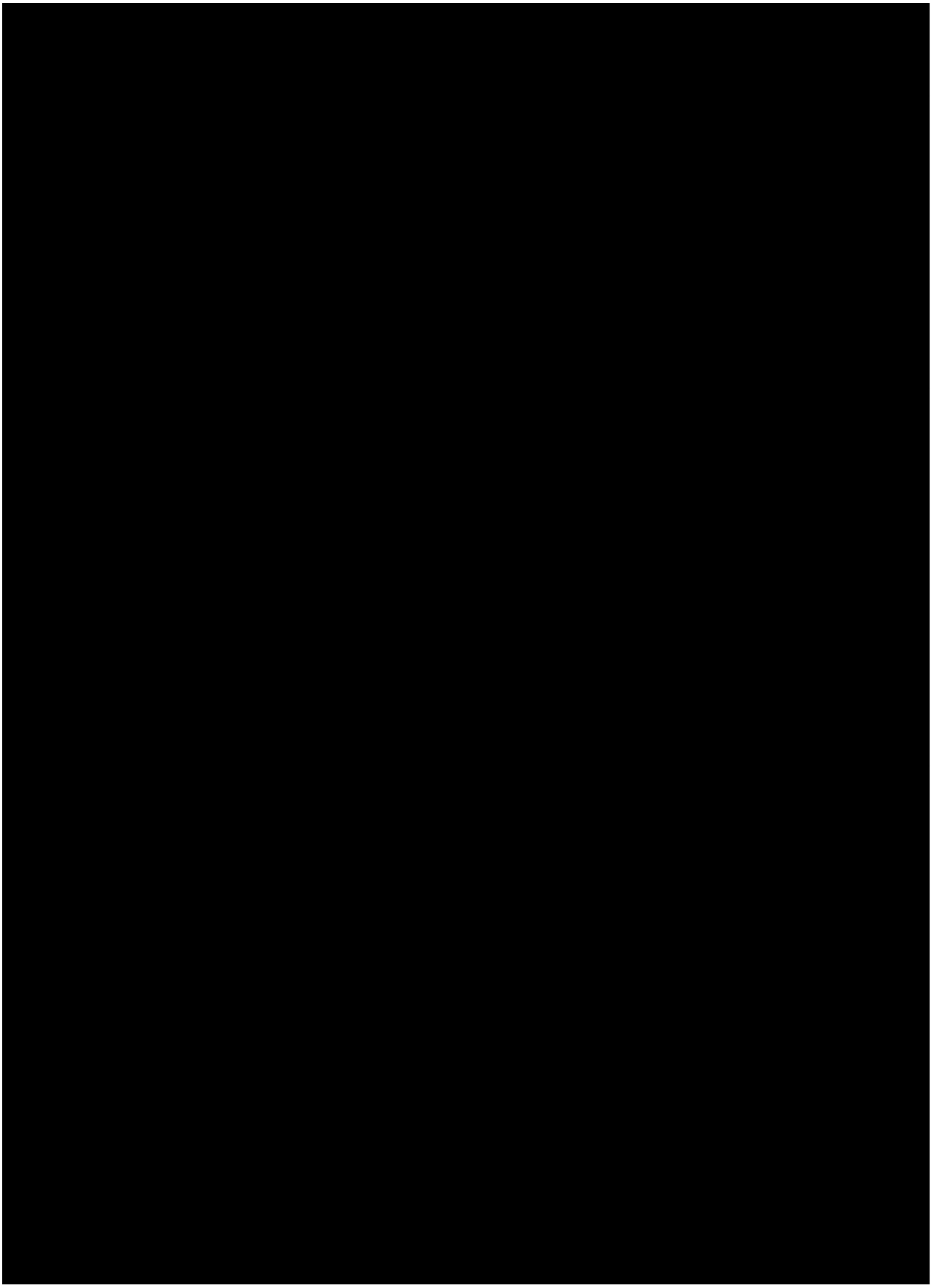
Eliminado: Análisis de brecha.

Fundamentación: De conformidad con 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 los artículos 32 y 36 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

Motivación: En virtud de que estos datos hace identificable las formas en que es posible atacar o vulnerar nuestros sistemas de información que resguardan datos personales y 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.

5. PLAN DE TRABAJO

[redacted]



[redacted]

Eliminado: Plan de trabajo.

Fundamentación: De conformidad con 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 los artículos 32 y 36 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

Motivación: En virtud de que estos datos hace identificable las formas en que es posible atacar o vulnerar nuestros sistemas de información que resguardan datos personales y 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.

6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

I. TRANSFERENCIAS DE DATOS PERSONALES

Secretaría Técnica*	
Identificador único*	EM008
(Nombre del sistema A1)*	Sistema de Evaluación Docente (SIEDO)
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:[5]	No se realizan transferencias de datos personales mediante el traslado de soportes físicos.

[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.

Transferencias mediante el traslado de soportes electrónicos:	La transferencia de datos personales en soportes electrónicos la pueden realizar los usuarios especificados en este documento previa identificación con credenciales de acceso (usuario y contraseña). Los soportes electrónicos solicitados se hacen en formato de documentos portables.
Transferencias mediante el traslado sobre redes electrónicas:	Actualmente no se cuenta con una infraestructura privada de almacenamiento (nube) en la ENES Unidad Morelia.

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]
2. Señalar en un listado las personas (nombre, cargo, funciones y obligaciones) que tienen acceso a los soportes físicos del sistema.[7]

El Sistema de Evaluación Docente, no realiza transferencia de datos personales en soportes físicos ya que todo el resguardo de los datos se hace mediante soporte electrónico mediante el uso de bases de datos relacionales y su descarga a través de formato de documentos portables.

II. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

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

[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:

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.

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

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.

El Sistema de Evaluación Docente, actualmente no cuenta con bitácoras de acceso digitales para conocer la actividad de los usuarios autorizados dentro del sistema.

III. REGISTRO DE INCIDENTES:

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

---

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.

No se cuenta con un procedimiento de atención de incidentes.

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:

a) ¿Cómo las identifica?

No se cuenta con mecanismos de identificación.

b) ¿Cómo las autentifica?

No se cuenta con mecanismos de autenticación.

c) ¿Cómo les autoriza el acceso?

No se cuenta con mecanismos de control de acceso.

---

[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.

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

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

Para las personas que acceden a dichos espacios interiores:

1. ¿Cómo las identifica?
   Se tiene definida una lista de acceso para el personal autorizado.
2. ¿Cómo las autentifica?
   Mediante credencial y número de trabajador.
3. ¿Cómo les autoriza el acceso?
   Si se encuentran en la lista de acceso autorizada, o si son proveedores acompañados por un empleado autorizado. Se les solicita se registren en la bitácora correspondiente.

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

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

El sistema de tratamiento de datos personales no realiza ninguna modificación de datos personales para el propósito del mismo.

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

VII. PERFILES DE USUARIO Y CONTRASEÑAS

1. Modelo de control de acceso:

Basado en perfiles o privilegios de acceso (permisos).

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?
Únicamente las contraseñas.

4. Administración de perfiles de usuario y contraseñas:

a) ¿Quién da de alta nuevos perfiles?
El Responsable del sistema a su cargo. Lic. Gustavo Cano Salazar.

b) ¿Quién autoriza la creación de nuevos perfiles?
El Secretario Técnico autoriza la creación de nuevos perfiles con privilegios administrativos.

c) ¿Se lleva registro de la creación de nuevos perfiles?
Mediante control interno del Departamento de Sistemas Informáticos y a través del sistema.

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

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

b) ¿Requiere el administrador acceso remoto al equipo donde reside el sistema para realizar tareas de mantenimiento?
Si, con acceso mediante VPN y SSH.

c) ¿Cómo se evita el acceso remoto no autorizado?

- Se cuenta con controles de acceso basados en roles y privilegios.
- El acceso remoto a los servidores se realiza mediante conexiones VPN habilitadas únicamente a los responsables de los sistemas.
- Implementación de captcha en el inicio de sesión del sistema.

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

1. Señalar si realiza respaldos
   a) Completos_X_, diferenciales ___ o incrementales__X_;
   b) De forma automática ____ o Manual _X_,
   c) Periodicidad con que los realiza: _Semestral_

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 externo.

3. Cómo y dónde archiva esos medios, y Consultar los documentos: Plan de respaldos ENES Morelia y Bitácora de control de los respaldos.

4. Quién es el responsable de realizar estas operaciones (el área universitaria o un tercero). El responsable (encargado) del sistema a su cargo.

[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.

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.

   Se cuenta con algunas medidas como las especificadas en el documento: Medidas de seguridad en los periodos de inactividad o mantenimiento, pero no se tiene desarrollado el plan de contingencia.
2. Si cuenta con plan de contingencia y lo ha implementado, deberá indicar si realiza pruebas de eficiencia de este.

   No se cuenta con plan de contingencia.
3. Informar si cuenta con un sitio redundante (alterno) y señalar lo siguiente:
   - **a)** El tipo de sitio (caliente, tibio o frío);[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.

Actualmente la ENES Unidad Morelia, no cuenta con sitio redundante para cubrir los incisos anteriores.

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*		
Identificador único*	EM008	
Nombre del sistema*	Sistema de Evaluación Docente (SIEDO)	
Recurso*	**Descripción***	**Control***

[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.

Reportes especiales de datos almacenados en el sistema.	Al solicitar reportes que no se encuentran en el sistema y su descarga en soporte electrónico, estos se generan y se descargan mediante un vínculo que vence en determinado tiempo para su descarga.	Evitar adjuntar archivos por correo electrónico porque es un servicio de terceros (Google). Una vez vencido el plazo de descarga (max. 24 horas) es imposible volver a descargar el soporte electrónico solicitado.
Reportes especiales de datos almacenados en el sistema en soportes electrónicos adjuntos por correo electrónico.	Solicitud de reportes especiales entregados en un soporte electrónico específico (hoja de cálculo, texto plano, etc.) y que se piden se adjunten por correo electrónico.	Se utiliza un programa de software libre para cifrar el archivo y personalmente se indica la contraseña para descifrar en el equipo de cómputo del usuario para utilizar el archivo que fue adjuntado por correo electrónico.

7.2 Procedimiento para la revisión de las medidas de seguridad

Secretaría Técnica*		
Identificador único*	EM008	
Nombre del sistema*	Sistema de Evaluación Docente (SIEDO)	
Medida de seguridad*	**Procedimiento***	**Responsable***
Principio del menor privilegio	Otorgar el acceso al usuario autorizado por la Secretaría técnica de acuerdo con el permiso requerido.	Encargado del sistema. Lic. Gustavo Cano Salazar. (01 día hábil).
Respaldos del sistema y base de datos.	Generación de archivos de respaldo tanto del sistema de datos personales como de la base de datos y control de bitácoras de respaldo.	Encargado del sistema. Lic. Gustavo Cano Salazar. (01 día hábil).
Sincronizar la fecha y hora con el servidor NTP	Revisiones periódicas de la hora y fecha del servidor	Mtro. Froylan Hernández Rendón (01 día hábil).

(Network Time Protocol) oficial de la UNAM	donde se encuentra el sistema.	
Instalar y mantener actualizado el software antimalware.	Revisión y actualización de la versión del software antivirus y de la base de datos.	Mtro. Froylan Hernández Rendón (01 día hábil).
Instalar las actualizaciones de seguridad más recientes disponibles.	Revisión y actualizaciones del sistema operativo.	Mtro. Froylan Hernández Rendón (02 días hábiles).

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

Secretaría Técnica*		
Identificador único*	EM008	
Nombre del sistema*	Sistema de Evaluación Docente (SIEDO)	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***
Principio del menor privilegio	Se encontró que todas las cuentas de usuarios del sistema cuentan con los permisos correspondientes.	Encargado del sistema. Lic. Gustavo Cano Salazar.
Respaldo del sistema y base de datos.	Se cuenta con respaldos actualizados de la información del sistema.	Encargado del sistema. Lic. Gustavo Cano Salazar.
Sincronizar la fecha y hora con el servidor NTP (Network Time Protocol) oficial de la UNAM	La fecha y hora están sincronizadas con el servidor NTP de la UNAM.	Mtro. Froylán Hernández Rendón.
Instalar y mantener actualizado el software antimalware.	El Software antivirus está actualizado.	Mtro. Froylán Hernández Rendón.
Instalar las actualizaciones de seguridad más recientes disponibles.	El sistema operativo cuenta con las actualizaciones correspondientes.	Mtro. Froylán Hernández Rendón.

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

Secretaría Técnica*		
Identificador único*	EM008	
Nombre del sistema*	Sistema de Evaluación Docente (SIEDO)	
Medida de seguridad*	**Acciones***	**Responsable***
Uso de certificados SSL	Implementar el protocolo “HTTPS” en el sistema. Realizar la renovación anual del certificado SSL para el subdominio donde se encuentra el sistema.	Mtro. Froylán Hernández Rendón

8 PROGRAMA ESPECÍFICO DE CAPACITACIÓN

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

Secretaría Técnica*			
Identificador único*	EM008		
Nombre del sistema*	Sistema de Evaluación Docente (SIEDO)		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Capacitación para la Protección de Datos Personales	Curso en línea	25 horas. Fecha de inicio: 20 de noviembre de 2020.	Público objetivo: Enlaces de Transparencia, Responsables de Seguridad de Datos Personales, Responsables de Tecnologías de la Información, así como

		Fecha de término: 17 de enero de 2021	funcionarios y empleados universitarios. Sin vigencia. Sin frecuencia de actualización.
Medidas de Seguridad Técnicas para la Protección de Datos Personales	Curso en línea	25 horas. Fecha de inicio: 8 de febrero de 2021. Fecha de término: 14 de marzo de 2021.	Público objetivo: Enlaces de Transparencia, Responsables de Seguridad de Datos Personales, Responsables de Tecnologías de la Información, así como funcionarios y empleados universitarios. Sin vigencia. Sin frecuencia de actualización.
Elaboración de Documento de Seguridad y Sistema de Gestión de Seguridad de Datos Personales de las áreas universitarias	Curso en línea	25 horas. Fecha de inicio: 25 de marzo de 2022 Fecha de término: 25 de marzo de 2022.	Público objetivo: Enlaces de Transparencia, Responsables de Seguridad de Datos Personales, Responsables de Tecnologías de la Información, así como funcionarios y empleados universitarios. Sin vigencia. Sin frecuencia de actualización.
La importancia de la protección de datos personales	Seminario en línea	1 hora. Fecha: 16 de junio de 2022.	Público en general.

			Sin vigencia. Sin frecuencia de actualización.

8.2 Programa de difusión de la protección a los datos personales

Secretaría Técnica*			
Identificador único*	EM008		
Nombre del sistema*	Sistema de Evaluación Docente (SIEDO)		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Indique actividad, tema, recursos para la difusión. Agregar un renglón por cada elemento	*Describa el tipo de elemento, sus objetivos y forma de impartición, publicación o distribución*	*Indique duración del elemento en horas, días, meses, su fecha de inicio y de término*	*Mencione público objetivo, vigencia del elemento y frecuencia de actualización*

Actualmente, no se cuenta con un programa de difusión de la protección de datos personales.

9 MEJORA CONTINUA

9.1 Actualización y mantenimiento de sistemas de información

Secretaría Técnica*			
Identificador único*	EM008		
Nombre del sistema*	Sistema de Evaluación Docente (SIEDO)		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Actualización de tecnologías de desarrollo	1.Solicitud de actualización de la arquitectura de desarrollo del sistema de datos personales.	12 meses	“Back-end” del sistema.

	2. Corregir y/o actualizar módulos del sistema. 3. Pruebas unitarias e integrales de las actualizaciones realizadas al sistema. 4. Actualización de archivos de sistema y/o sentencias de bases de datos en servidor de producción.		

9.2 Actualización y mantenimiento de equipo de cómputo

Secretaría Técnica*			
Identificador único*	EM008		
Nombre del sistema*	Sistema de Evaluación Docente (SIEDO)		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Indique actividad. Agregar un renglón por cada elemento	*Describa el tipo de actividad, sus objetivos e impacto la actualización o mantenimiento del equipo de cómputo*	*Indique duración en la ejecución de la actividad en horas, días, meses, su fecha de inicio y de término*	*Mencione los aspectos de equipo de cómputo que son resueltos, total o parcialmente, por la actividad.*

Actualmente, no se han asignado recursos para la actualización del equipo de cómputo.

9.3 Procesos para la conservación, preservación y respaldos de información

Secretaría Técnica*

Identificador único*	EM008	
Nombre del sistema*	Sistema de Evaluación Docente (SIEDO)	
Proceso*	**Descripción***	**Responsable***
Poner en fase de “mantenimiento” del sistema.	Se coloca un mensaje en la parte de acceso al sistema con un aviso de “mantenimiento” y de ser posible la fecha de “regreso” a la operación del sistema.	Encargado del sistema: Lic. Gustavo Cano Salazar. (01 día hábil).
Ingresar remotamente al servidor.	Acceso al servidor de manera remota para realizar el respaldo de ambos componentes (script del sistema y de la base de datos)	Encargado del sistema: Lic. Gustavo Cano Salazar. (01 día hábil).
Descarga de respaldos del sistema a soporte físico electrónico.	Descarga directa al Disco Duro externo proporcionado por secretaría técnica con los respaldos realizados del sistema.	Encargado del sistema: Lic. Gustavo Cano Salazar. (01 día hábil).
Salida del servidor y de fase de “mantenimiento” en el sistema.	Quitar el mensaje del modo mantenimiento del sistema y salida completa del servidor.	Encargado del sistema: Lic. Gustavo Cano Salazar. (01 día hábil).
El proceso de respaldo de información se encuentra contenido en el documento: Plan de respaldos ENES Morelia	El proceso se describe en el documento: Plan de respaldos ENES Morelia	Encargado del sistema: Lic. Gustavo Cano Salazar. (01 día hábil).

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

Secretaría Técnica*

Identificador único*	EM008	
(Nombre del sistema A1)*	Sistema de Evaluación Docente (SIEDO)	
Proceso*	**Descripción***	**Responsable***
Borrado de datos dentro del Sistema Gestor de Base de Datos.	Aplicación de transacciones y ejecución de instrucciones SQL para actualización y/o borrado de datos. Una vez completada la transacción aplicar la instrucción correspondiente para conservar o borrar definitivamente los datos.	Encargado del sistema: Lic. Gustavo Cano Salazar.
El proceso se encuentra contenido en el documento: Borrado Seguro ENES Morelia	El proceso se describe en el documento: Borrado Seguro ENES Morelia	Borrado seguro: Encargado del sistema: Lic. Gustavo Cano Salazar. Responsable de la disposición final de equipos o componentes de cómputo: Mtro. Froylán Hernández Rendón Tiempo máximo de ejecución: 05 días hábiles.

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

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

(Informar y describir el procedimiento para la cancelación de un sistema de tratamiento de datos personales.)[13]

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

a) Denominación
b) Motivo de la cancelación

B) PLAZOS Y CONDICIONES PARA EL BLOQUEO DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES:[14]

(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)

---

[13] 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.

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

ENCUESTAS INSTITUCIONALES (LIMESURVEY)

Sistema web desarrollado por un externo que se puede instalar en un servidor privado y utilizarlo como un encuestador para la comunidad de la ENES Unidad Morelia.

Aunque se pueden hacer encuestas y formularios en servidores públicos y de manera gratuita sin tener que invertir en infraestructura, no se tiene la garantía completa de que precisamente los datos personales que puedan ser solicitados por las encuestas queden debidamente protegidos como lo marca la ley; es por eso que se decide instalar esta herramienta para que se encuentren los datos solicitados en las encuestas debidamente protegidos y dándole el mantenimiento que requiere esta plataforma de forma adecuada.

ANEXO I: Documento de Seguridad de datos personales

ÍNDICE

INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Secretaría Técnica	
Identificador único*	EM014
Nombre del sistema*	Encuestas Institucionales (Limesurvey)
Datos personales (sensibles o no) contenidos en el sistema*:	Este sistema solicita diversos datos personales, según la encuesta o formulario que se aplique y así lo requiera, ya que funciona como un encuestador y a la vez como un formato de registro. De forma general en las encuestas se puede solicitar: ● Datos personales del alumno(a) y/o trabajador UNAM: o Nombre completo (apellido paterno, apellido materno, nombre) o Número de cuenta / Número de trabajador o Correo electrónico. o Fecha de nacimiento o Número telefónico móvil o Dirección o Licenciatura que estudia, imparte clase o dependencia/departamento que labora. o Datos médicos y de salud o Archivo en formato de documento portables variados que puedan contener otro tipo de datos sensibles.
Responsable*:	Escuela Nacional de Estudios Superiores Unidad Morelia
Nombre*:	Dr. Santiago Cortés Hernández
Cargo*:	Secretario Técnico
Funciones*:	Decidir sobre el tratamiento automatizado de los datos personales, así como el contenido, finalidad y uso del sistema.
Obligaciones*:	- Decidir a qué usuarios se le da acceso al sistema con privilegios administrativos. - Decidir sobre la incorporación de nuevas funcionalidades en el sistema. - Vigilar que el sistema cumpla con todas las medidas de seguridad técnicas, físicas y administrativas.
	Encargados[1]:
(Nombre del Encargado 1*)	Lic. Gustavo Cano Salazar
Cargo*:	Técnico Académico, responsable del Depto. de Sistemas

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

	Informáticos de la ENES Unidad Morelia.
Funciones*:	Análisis, diseño, implementación, mantenimiento, documentación, soporte y capacitación de usuarios, sobre los diversos sistemas informáticos a su cargo en operación de la ENES Unidad Morelia.
Obligaciones*:	● Vigilar la operación correcta del sistema durante el periodo de mayor uso de este. ● Registrar, actualizar, eliminar datos según requerimiento por escrito de la Secretaría Técnica y/o los usuarios que utilizan el sistema (acceso mediante usuario y contraseña). ● Monitorear la protección de los datos personales contenidos en el sistema mediante la implementación de estrategias y mecanismos de seguridad en su desarrollo y mantenimiento, a nivel interno y externo.
	Usuarios:
(Nombre del Usuario 1*)	Mtro. Jose Alfredo Noriega Carmona.
Cargo*:	Técnico Académico Asociado “C” de Tiempo Completo.
Funciones*:	Administrador secundario de la plataforma de encuestas institucionales, apoyando en la capacitación y uso de esta plataforma. Configuración de encuestas según las necesidades de la ENES Unidad Morelia.
Obligaciones*:	Cumplir con la obligación legal de resguardar los datos personales de los alumnos(as) y académicos(a) registrados en el sistema utilizando la información con fines únicamente académico-administrativos.
(Nombre del Usuario 2*)	Lic. Daniel Barajas Gutiérrez
Cargo*:	Asistente de la Secretaría Académica
Funciones*:	Configurador de formatos de registro relacionados a la plantilla docente de la ENES Unidad Morelia UNAM.
Obligaciones*:	Cumplir con la obligación legal de resguardar los datos personales de los alumnos(as) y académicos(a) registrados en el sistema utilizando la información con fines únicamente académico-administrativos.
(Nombre del Usuario 3*)	Médico Francisco Ambriz Vázquez.
Cargo*:	Médico de la ENES Unidad Morelia UNAM.
Funciones*:	Visualizador de datos solicitados a través de las encuestas realizadas con fines médicos y de estadísticas que son previamente configuradas por el Mtro. José Alfredo Noriega Carmona.
Obligaciones*:	Cumplir con la obligación legal de resguardar los datos personales los alumnos(as) y académicos(as) registrados en el sistema utilizando la información con fines académico-administrativos.
(Nombre del Usuario 4*)	Lic. María Dolores Rodríguez Guzman
Cargo*:	Coordinadora de Atención a la Comunidad.

Funciones*:	Configuradora de encuestas con fines de recopilación de datos para talles, actividades deportivas, préstamo de bicicletas, etc. Por otro lado, elaborar encuestas a las generaciones de egresados y bolsa de trabajo de la ENES Unidad Morelia UNAM.
Obligaciones*:	Cumplir con la obligación legal de resguardar los datos personales de los alumnos(as) registrados en el sistema utilizando la información con fines académicos.
(Nombre del Usuario 5*)	Dra. Yunuen Tapia Torres
Cargo*:	Secretaria General / Profa. de Tiempo Completo.
Funciones*:	Visualización y monitoreo de encuestas elaboradas previamente por la Coordinadora de Atención a la comunidad para tomar decisiones sobre los datos y opiniones vertidos en estas encuestas.
Obligaciones*:	Cumplir con la obligación legal de resguardar los datos personales de los alumnos(as) registrados en el sistema utilizando la información con fines académicos.

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

Secretaría Técnica	
Identificador único*	EM014
Nombre del sistema*	Encuestas Institucionales (Limesurvey)
Tipo de soporte[2]:*	Electrónico
Descripción[3]:*	Para almacenamiento de datos se utiliza un Sistema Gestor de Bases de Datos Relacional y para informes ejecutivos y reportes se generan formatos de documentos portables y hojas de cálculo.

[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.

[redacted]

Eliminado: Información específica sobre el lugar donde se resguardan los soportes de la información.

Fundamentación: De conformidad con 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 los artículos 32 y 36 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

Motivación: En virtud de que estos datos hace identificable las formas en que es posible atacar o vulnerar nuestros sistemas de información que resguardan datos personales y 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.

3. ANÁLISIS DE RIESGOS

[redacted]

[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.

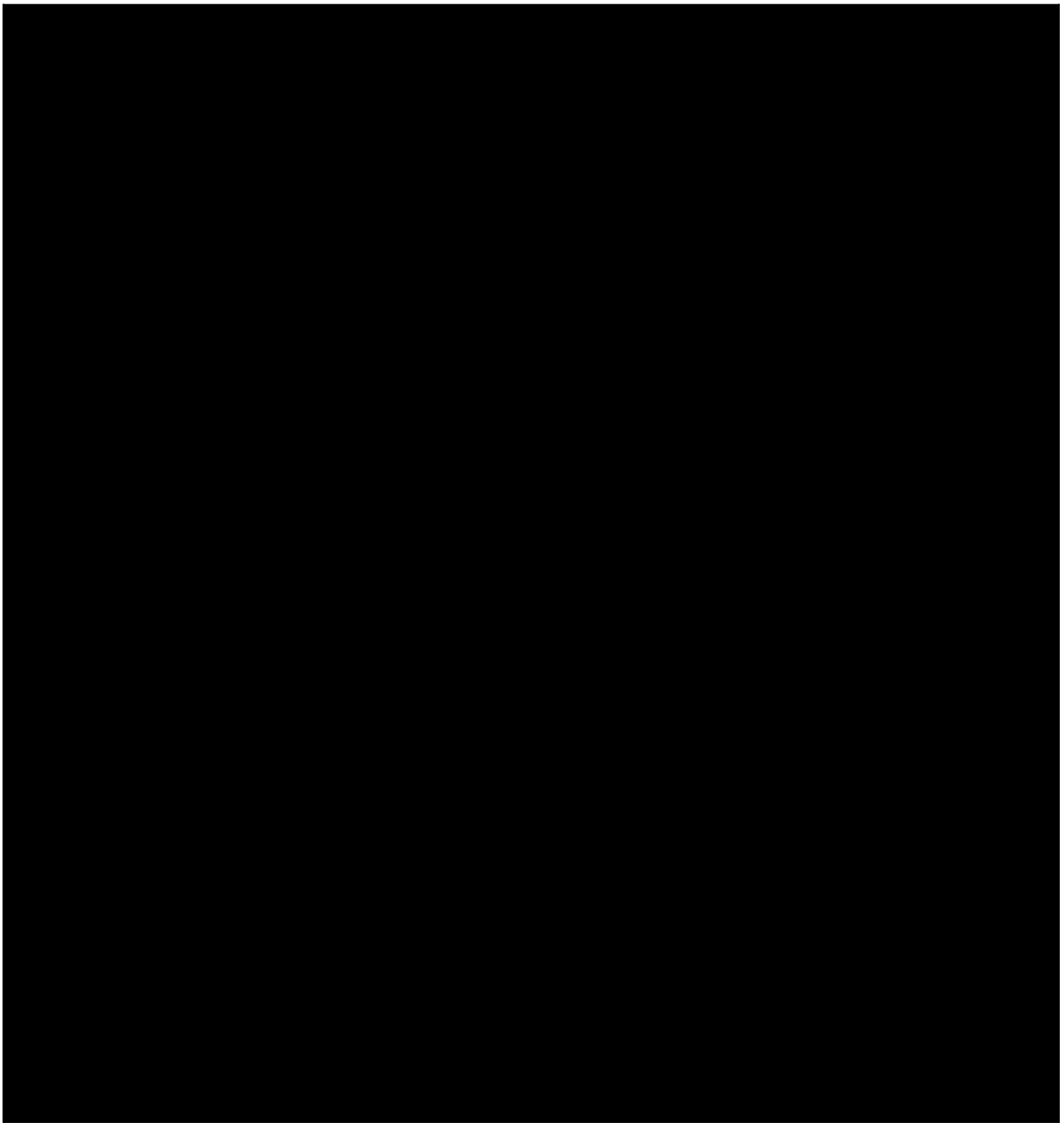
[redacted]

Eliminado: Análisis de riesgos.

Fundamentación: De conformidad con 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 los artículos 32 y 36 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

Motivación: En virtud de que estos datos hace identificable las formas en que es posible atacar o vulnerar nuestros sistemas de información que resguardan datos personales y 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.

4. ANÁLISIS DE BRECHA



[redacted]

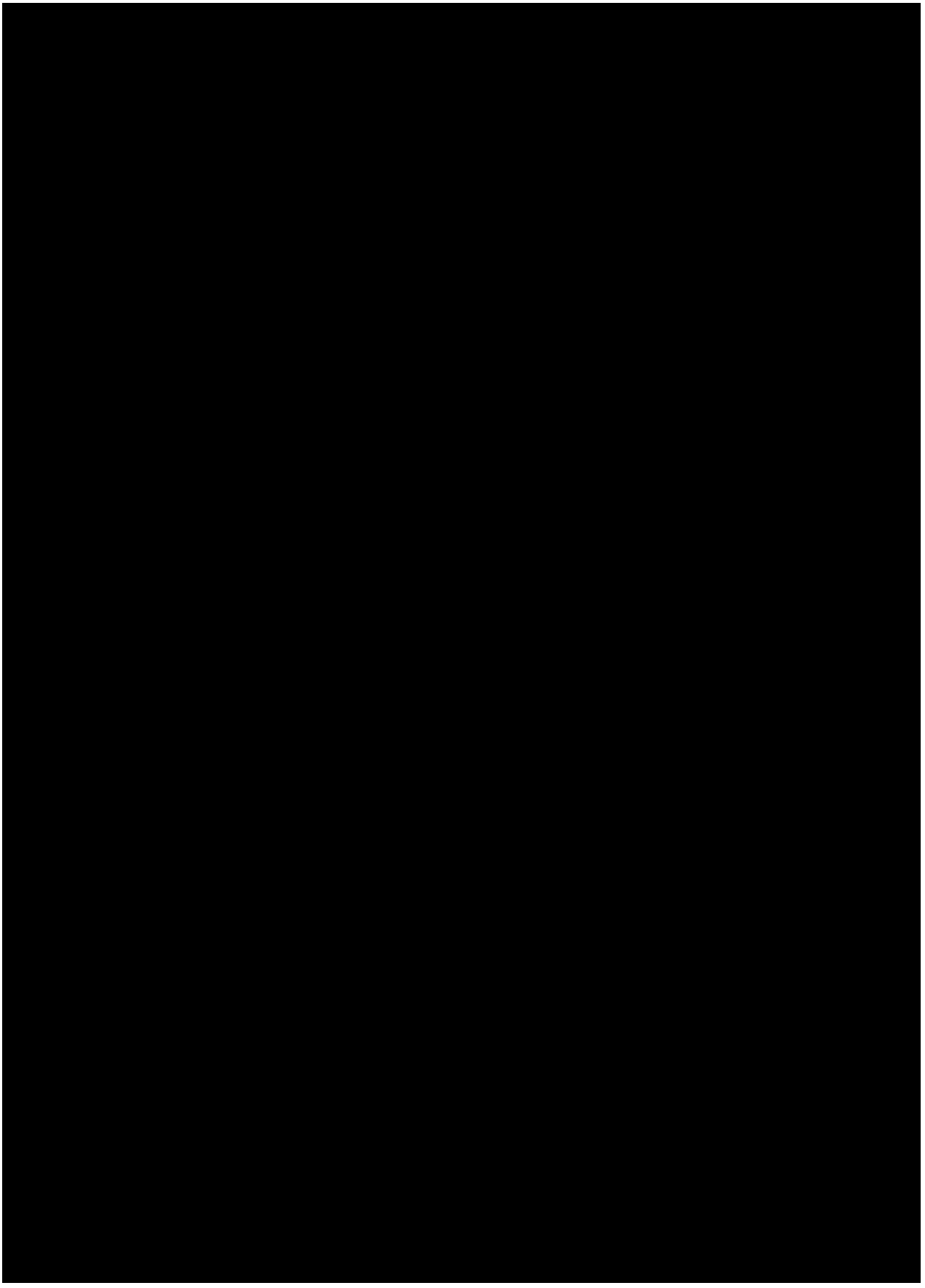
Eliminado: Análisis de brecha.

Fundamentación: De conformidad con 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 los artículos 32 y 36 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

Motivación: En virtud de que estos datos hace identificable las formas en que es posible atacar o vulnerar nuestros sistemas de información que resguardan datos personales y 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.

5. PLAN DE TRABAJO

[redacted]



[redacted]

Eliminado: Plan de trabajo.

Fundamentación: De conformidad con 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 los artículos 32 y 36 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

Motivación: En virtud de que estos datos hace identificable las formas en que es posible atacar o vulnerar nuestros sistemas de información que resguardan datos personales y 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.

6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

I. TRANSFERENCIAS DE DATOS PERSONALES

Secretaría Técnica*	
Identificador único*	EM014
(Nombre del sistema A1)*	Encuestas Institucionales (Limesurvey)
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:[5]	No se realizan transferencias de datos personales mediante el traslado de soportes físicos.

[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.

Transferencias mediante el traslado de soportes electrónicos:	La transferencia de datos personales en soportes electrónicos la pueden realizar los usuarios especificados en este documento previa identificación con credenciales de acceso (usuario y contraseña). Los soportes electrónicos solicitados se hacen en formato de documentos portables y hojas de cálculo.
Transferencias mediante el traslado sobre redes electrónicas:	Actualmente no se cuenta con una infraestructura privada de almacenamiento (nube) en la ENES Unidad Morelia.

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]
2. Señalar en un listado las personas (nombre, cargo, funciones y obligaciones) que tienen acceso a los soportes físicos del sistema.[7]

La plataforma de encuestas no realiza transferencia de datos personales en soportes físicos ya que todo el resguardo de los datos se hace mediante soporte electrónico mediante el uso de bases de datos relacionales y su descarga a través de formato de documentos portables y hojas de cálculo.

II. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

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

[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:

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

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

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.

La plataforma de encuestas sus bitácoras son con respecto a los usuarios que ingresan datos a las mismas, o bien al momento de dar por respondida una encuesta, pero al parecer, no almacena más allá de esos datos sobre el uso de la plataforma.

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

---

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.

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 cuenta con un procedimiento de atención de incidentes. No se han presentado incidentes al respecto.

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 electrónicos7: Los campos, registros, tablas, bases de datos o archivos electrónicos, tanto dañados como recuperados, el nombre de los sistemas y la infraestructura afectada, indicar si el incidente afectó el servidor principal y los servidores de respaldo, etc.
2. Si el registro está en soporte físico o en soporte electrónico;
3. Cómo asegura la integridad de dicho registro, y
4. Para el caso de soportes electrónicos, quién autoriza la recuperación de datos.

V. ACCESO A LAS INSTALACIONES

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

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

Para las personas que acceden a sus instalaciones:

a) ¿Cómo las identifica?
No se cuenta con mecanismos de identificación.

b) ¿Cómo las autentifica?
No se cuenta con mecanismos de autenticación.

---

[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.

c) ¿Cómo les autoriza el acceso?
No se cuenta con mecanismos de control de acceso.

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

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

Para las personas que acceden a dichos espacios interiores:

1. ¿Cómo las identifica?
   Se tiene definida una lista de acceso para el personal autorizado.
2. ¿Cómo las autentifica?
   Mediante credencial y número de trabajador.
3. ¿Cómo les autoriza el acceso?
   Si se encuentran en la lista de acceso autorizada, o si son proveedores acompañados por un empleado autorizado. Se les solicita se registren en la bitácora correspondiente.

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

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

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

VII. PERFILES DE USUARIO Y CONTRASEÑAS

1. Modelo de control de acceso:

Basado en perfiles o privilegios de acceso (permisos).

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?
Únicamente las contraseñas.

4. Administración de perfiles de usuario y contraseñas:

a) ¿Quién da de alta nuevos perfiles?
El Responsable del sistema a su cargo. Lic. Gustavo Cano Salazar.

b) ¿Quién autoriza la creación de nuevos perfiles?
El Secretario Técnico autoriza la creación de nuevos perfiles con privilegios administrativos.

c) ¿Se lleva registro de la creación de nuevos perfiles?
Mediante control interno del Departamento de Sistemas Informáticos y a través del sistema.

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

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

b) ¿Requiere el administrador acceso remoto al equipo donde reside el sistema para realizar tareas de mantenimiento?
Si, con acceso mediante VPN y SSH.

c) ¿Cómo se evita el acceso remoto no autorizado?
- Se cuenta con controles de acceso basados en roles y privilegios.
- El acceso remoto a los servidores se realiza mediante conexiones VPN habilitadas únicamente a los responsables de los sistemas.

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

1. Señalar si realiza respaldos
- **a)** Completos_X_, diferenciales ___ o incrementales__X_;
- **b)** De forma automática ____ o Manual _X_,
- **c)** Periodicidad con que los realiza: _Semestral_

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 externo.

3. Cómo y dónde archiva esos medios, y Consultar los documentos: Plan de respaldos ENES Morelia y Bitácora de control de los respaldos.

4. Quién es el responsable de realizar estas operaciones (el área universitaria o un tercero). El responsable (encargado) del sistema a su cargo.

[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.

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.

   Se cuenta con algunas medidas como las especificadas en el documento: Medidas de seguridad en los periodos de inactividad o mantenimiento, pero no se tiene desarrollado el plan de contingencia.
2. Si cuenta con plan de contingencia y lo ha implementado, deberá indicar si realiza pruebas de eficiencia de este.

   No se cuenta con plan de contingencia.
3. Informar si cuenta con un sitio redundante (alterno) y señalar lo siguiente:
   - **a)** El tipo de sitio (caliente, tibio o frío);[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.

Actualmente la ENES Unidad Morelia, no cuenta con sitio redundante para cubrir los incisos anteriores.

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*		
Identificador único*	EM014	
Nombre del sistema*	Encuestas institucionales (Limesurvey)	
Recurso*	**Descripción***	**Control***

[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.

Reportes especiales de datos almacenados en el sistema.	Al solicitar reportes que no se encuentran en el sistema y su descarga en soporte electrónico, estos se generan y se descargan mediante un vínculo que vence en determinado tiempo para su descarga.	Evitar adjuntar archivos por correo electrónico porque es un servicio de terceros (Google). Una vez vencido el plazo de descarga (max. 24 horas) es imposible volver a descargar el soporte electrónico solicitado.
Reportes especiales de datos almacenados en el sistema en soportes electrónicos adjuntos por correo electrónico.	Solicitud de reportes especiales entregados en un soporte electrónico específico (hoja de cálculo, texto plano, etc.) y que se piden se adjunten por correo electrónico.	Se utiliza un programa de software libre para cifrar el archivo y personalmente se indica la contraseña para descifrar en el equipo de cómputo del usuario para utilizar el archivo que fue adjuntado por correo electrónico.

7.2 Procedimiento para la revisión de las medidas de seguridad

Secretaría Técnica*		
Identificador único*	EM008	
Nombre del sistema*	Sistema de Evaluación Docente (SIEDO)	
Medida de seguridad*	**Procedimiento***	**Responsable***
Principio del menor privilegio	Otorgar el acceso al usuario autorizado por la Secretaría técnica de acuerdo con el permiso requerido.	Encargado del sistema. Lic. Gustavo Cano Salazar. (01 día hábil).
Respaldos del sistema y base de datos.	Generación de archivos de respaldo tanto del sistema de datos personales como de la base de datos y control de bitácoras de respaldo.	Encargado del sistema. Lic. Gustavo Cano Salazar. (01 día hábil).
Sincronizar la fecha y hora con el servidor NTP	Revisiones periódicas de la hora y fecha del servidor	Mtro. Froylan Hernández Rendón (01 día hábil).

(Network Time Protocol) oficial de la UNAM	donde se encuentra el sistema.	
Instalar y mantener actualizado el software antimalware.	Revisión y actualización de la versión del software antivirus y de la base de datos.	Mtro. Froylan Hernández Rendón (01 día hábil).
Instalar las actualizaciones de seguridad más recientes disponibles.	Revisión y actualizaciones del sistema operativo.	Mtro. Froylan Hernández Rendón (02 días hábiles).

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

Secretaría Técnica*		
Identificador único*	EM014	
Nombre del sistema*	Encuestas institucionales (Limesurvey)	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***
Principio del menor privilegio	Se encontró que todas las cuentas de usuarios del sistema cuentan con los permisos correspondientes.	Encargado del sistema. Lic. Gustavo Cano Salazar.
Respaldo del sistema y base de datos.	Se cuenta con respaldos actualizados de la información del sistema.	Encargado del sistema. Lic. Gustavo Cano Salazar.
Sincronizar la fecha y hora con el servidor NTP (Network Time Protocol) oficial de la UNAM	La fecha y hora están sincronizadas con el servidor NTP de la UNAM.	Mtro. Froylán Hernández Rendón.
Instalar y mantener actualizado el software antimalware.	El Software antivirus está actualizado.	Mtro. Froylán Hernández Rendón.

Instalar las actualizaciones de seguridad más recientes disponibles.	El sistema operativo cuenta con las actualizaciones correspondientes.	Mtro. Froylán Hernández Rendón.

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

Secretaría Técnica*		
Identificador único*	EM014	
Nombre del sistema*	Encuestas institucionales (Limesurvey)	
Medida de seguridad*	**Acciones***	**Responsable***
Uso de certificados SSL	Implementar el protocolo “HTTPS” en el sistema. Realizar la renovación anual del certificado SSL para el subdominio donde se encuentra el sistema.	Mtro. Froylán Hernández Rendón

8 PROGRAMA ESPECÍFICO DE CAPACITACIÓN

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

Secretaría Técnica*			
Identificador único*	EM008		
Nombre del sistema*	Sistema de Evaluación Docente (SIEDO)		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Capacitación para la Protección de Datos Personales	Curso en línea	25 horas. Fecha de inicio: 20 de noviembre de 2020. Fecha de término: 17 de enero de 2021	Público objetivo: Enlaces de Transparencia, Responsables de Seguridad de Datos Personales, Responsables de Tecnologías de la Información, así como funcionarios y empleados universitarios. Sin vigencia. Sin frecuencia de actualización.
Medidas de Seguridad Técnicas para la Protección de Datos Personales	Curso en línea	25 horas. Fecha de inicio: 8 de febrero de 2021. Fecha de término: 14 de marzo de 2021.	Público objetivo: Enlaces de Transparencia, Responsables de Seguridad de Datos Personales, Responsables de Tecnologías de la Información, así como funcionarios y empleados universitarios. Sin vigencia. Sin frecuencia de actualización.
Elaboración de Documento de Seguridad y Sistema de Gestión de	Curso en línea	25 horas.	Público objetivo: Enlaces de Transparencia, Responsables de Seguridad de Datos

Seguridad de Datos Personales de las áreas universitarias		Fecha de inicio: 25 de marzo de 2022 Fecha de término: 25 de marzo de 2022.	Personales, Responsables de Tecnologías de la Información, así como funcionarios y empleados universitarios. Sin vigencia. Sin frecuencia de actualización.
La importancia de la protección de datos personales	Seminario en línea	1 hora. Fecha: 16 de junio de 2022.	Público en general. Sin vigencia. Sin frecuencia de actualización.

8.2 Programa de difusión de la protección a los datos personales

Secretaría Técnica*			
Identificador único*	EM014		
Nombre del sistema*	Encuestas institucionales (Limesurvey)		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Indique actividad, tema, recursos para la difusión. Agregar un renglón por cada elemento	*Describa el tipo de elemento, sus objetivos y forma de impartición, publicación o distribución*	*Indique duración del elemento en horas, días, meses, su fecha de inicio y de término*	*Mencione público objetivo, vigencia del elemento y frecuencia de actualización*

Actualmente, no se cuenta con un programa de difusión de la protección de datos personales.

9 MEJORA CONTINUA

9.1 Actualización y mantenimiento de sistemas de información

Secretaría Técnica*			
Identificador único*	EM014		
Nombre del sistema*	Encuestas institucionales (Limesurvey)		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Actualización de tecnologías de desarrollo	1.Solicitud de actualización de la arquitectura de desarrollo del sistema de datos personales. 2. Corregir y/o actualizar módulos del sistema. 3. Pruebas unitarias e integrales de las actualizaciones realizadas al sistema. 4. Actualización de archivos de sistema y/o sentencias de bases de datos en servidor de producción.	12 meses	"Back-end" del sistema.

9.2 Actualización y mantenimiento de equipo de cómputo

Secretaría Técnica*			
Identificador único*	EM014		
Nombre del sistema*	Encuestas institucionales (Limesurvey)		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Indique actividad. Agregar un renglón por cada elemento	*Describa el tipo de actividad, sus objetivos e impacto la actualización o*	*Indique duración en la ejecución de la actividad en horas, días, meses, su fecha*	*Mencione los aspectos de equipo de cómputo que son resueltos, total*

	mantenimiento del equipo de cómputo	*de inicio y de término*	*o parcialmente, por la actividad.*

Actualmente, no se han asignado recursos para la actualización del equipo de cómputo.

9.3 Procesos para la conservación, preservación y respaldos de información

Secretaría Técnica*		
Identificador único*	EM014	
Nombre del sistema*	Encuestas institucionales (Limesurvey)	
Proceso*	**Descripción***	**Responsable***
Poner en fase de “mantenimiento” del sistema.	Se coloca un mensaje en la parte de acceso al sistema con un aviso de “mantenimiento” y de ser posible la fecha de “regreso” a la operación del sistema.	Encargado del sistema: Lic. Gustavo Cano Salazar. (01 día hábil).
Ingresar remotamente al servidor.	Acceso al servidor de manera remota para realizar el respaldo de ambos componentes (script del sistema y de la base de datos)	Encargado del sistema: Lic. Gustavo Cano Salazar. (01 día hábil).
Descarga de respaldos del sistema a soporte físico electrónico.	Descarga directa al Disco Duro externo proporcionado por secretaría técnica con los respaldos realizados del sistema.	Encargado del sistema: Lic. Gustavo Cano Salazar. (01 día hábil).
Salida del servidor y de fase de “mantenimiento” en el sistema.	Quitar el mensaje del modo mantenimiento del sistema y salida completa del servidor.	Encargado del sistema: Lic. Gustavo Cano Salazar. (01 día hábil).

El proceso de respaldo de información se encuentra contenido en el documento: Plan de respaldos ENES Morelia	El proceso se describe en el documento: Plan de respaldos ENES Morelia	Encargado del sistema: Lic. Gustavo Cano Salazar. (01 día hábil).

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

Secretaría Técnica*		
Identificador único*	EM014	
(Nombre del sistema A1)*	Encuestas institucionales (Limesurvey)	
Proceso*	**Descripción***	**Responsable***
Borrado de datos dentro del Sistema Gestor de Base de Datos.	Aplicación de transacciones y ejecución de instrucciones SQL para actualización y/o borrado de datos. Una vez completada la transacción aplicar la instrucción correspondiente para conservar o borrar definitivamente los datos.	Encargado del sistema: Lic. Gustavo Cano Salazar.
El proceso se encuentra contenido en el documento: Borrado Seguro ENES Morelia	El proceso se describe en el documento: Borrado Seguro ENES Morelia	Borrado seguro: Encargado del sistema: Lic. Gustavo Cano Salazar. Responsable de la disposición final de equipos o componentes de cómputo: Mtro. Froylán Hernández Rendón Tiempo máximo de ejecución: 05 días hábiles.

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

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

(Informar y describir el procedimiento para la cancelación de un sistema de tratamiento de datos personales.)[13]

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

a) Denominación
b) Motivo de la cancelación

B) PLAZOS Y CONDICIONES PARA EL BLOQUEO DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES:[14]

(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:

---

[13] 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.

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

(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)

PLATAFORMA MOODLE

Plataforma instalada para ofrecer un apoyo adicional a la docencia de los profesores/as que imparten docencia en la ENES Unidad Morelia. El objetivo de tener esta herramienta es tener material adicional a la modalidad presencial que se tiene, es un apoyo que se brinda para que se puedan tener un repositorio de recursos y de actividades que coadyuven en el trabajo colaborativo y fortalecer el entorno de aprendizaje del alumno.

ANEXO I: Documento de Seguridad de datos personales

ÍNDICE

INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Secretaría Técnica	
Identificador único*	EM017
Nombre del sistema*	Moodle
Datos personales (sensibles o no) contenidos en el sistema*:	● Datos personales del alumno(a): o Nombre completo (apellido paterno, apellido materno, nombre) o Número de cuenta o Fecha de nacimiento o Correo electrónico. o Licenciatura / Materia / Programa / Curso ● Datos personales del académico(a) o Nombre completo (apellido paterno, apellido materno, nombre). o Número de trabajador o RFC con homoclave o Correo electrónico o Licenciatura / Curso que imparte.
Responsable*:	Escuela Nacional de Estudios Superiores Unidad Morelia
Nombre*:	Dr. Santiago Cortés Hernández
Cargo*:	Secretario Técnico
Funciones*:	Decidir sobre el tratamiento automatizado de los datos personales, así como el contenido, finalidad y uso del sistema.
Obligaciones*:	- Decidir a qué usuarios se le da acceso al sistema con privilegios administrativos. - Decidir sobre la incorporación de nuevas funcionalidades en el sistema. - Vigilar que el sistema cumpla con todas las medidas de seguridad técnicas, físicas y administrativas.
	Encargados[1]:
(Nombre del Encargado 1*)	Lic. Gustavo Cano Salazar
Cargo*:	Técnico Académico, responsable del Depto. de Sistemas Informáticos de la ENES Unidad Morelia.
Funciones*:	Análisis, diseño, implementación, mantenimiento, documentación, soporte y capacitación de usuarios, sobre los diversos sistemas informáticos a su cargo en operación de la ENES Unidad Morelia.
Obligaciones*:	● Vigilar la operación correcta del sistema durante el

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

	periodo de mayor uso de este, ● Registrar, actualizar, eliminar datos según requerimiento por escrito de la Secretaría Técnica y/o los usuarios que utilizan el sistema (acceso mediante usuario y contraseña). ● Monitorear la protección de los datos personales contenidos en el sistema mediante la implementación de estrategias y mecanismos de seguridad en su desarrollo y mantenimiento, a nivel interno y externo.
	Usuarios:
(Nombre del Usuario 1*)	Mtra. Melba Selene Cardoso Gómez
Cargo*:	Jefa del Departamento de Idiomas
Funciones*:	Matriculación de alumnos/as a los diferentes niveles de inglés para aplicación de examenes parciales y finales en la escuela.
Obligaciones*:	Cumplir con la obligación legal de resguardar los datos personales de los alumnos(as) y académicos(a) registrados en el sistema utilizando la información con fines únicamente académico-administrativos.
(Nombre del Usuario 2*)	Mtra. Karla Quintero Gómez
Cargo*:	Asistente de la Jefa del Departamento de Idiomas
Funciones*:	Matriculación de alumnos/as a los diferentes niveles de inglés para aplicación de examenes parciales y finales en la escuela.
Obligaciones*:	Cumplir con la obligación legal de resguardar los datos personales de los alumnos(as) y académicos(a) registrados en el sistema utilizando la información con fines únicamente académico-administrativos.
(Nombre del Usuario 3*)	Docentes de la ENES Unidad Morelia.
Cargo*:	Profesores / Ayudantes
Funciones*:	▪ Solicitud de “virtualizar” el curso como apoyo para la materia que imparten de forma presencial ▪ Matriculación de los alumnos/as inscritos/as en su materia.
Obligaciones*:	Cumplir con la obligación legal de resguardar los datos personales los alumnos(as) y académicos(as) registrados en el sistema utilizando la información con fines académico-administrativos.

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

Secretaría Técnica	
Identificador único*	EM017
Nombre del sistema*	Moodle
Tipo de soporte[2]:*	Electrónico
Descripción[3]:*	Para almacenamiento de datos se utiliza un Sistema Gestor de Bases de Datos Relacional y para informes ejecutivos y reportes se generan formatos de documentos portables y hojas de cálculo.
Características del lugar donde se resguardan los soportes[4]:*	El espacio cuenta con sistema de aire acondicionado de alta precisión de baterí El "Datac Edificio H

Eliminado: Información específica sobre el lugar donde se resguardan los soportes de la información.

Fundamentación: De conformidad con 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 los artículos 32 y 36 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

Motivación: En virtud de que estos datos hace identificable las formas en que es posible atacar o vulnerar nuestros sistemas de información que resguardan datos personales y 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.

3. ANÁLISIS DE RIESGOS

Sec		
Identificador único*	EM017	
Nombre del sistema*	Moodle	
Riesgo*	**Impacto***	**Mitigación***

[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.

Uso de contraseñas de acceso débiles (contraseñas cortas que no utilizan combinaciones de letras, números, símbolos y mayúsculas/minúsculas)	Las contraseñas de acceso débiles son fácilmente descifrables por procesos automáticos permitiendo que usuarios malintencionados ingresen al sistema y accedan a información personal de los usuarios.	Realizar una difusión y cultura de buenas prácticas para generar contraseñas seguras. Agregar una capa adicional de seguridad de acceso dependiendo del sistema y su impacto en el uso de nivel de datos personales y/o sensibles (Captcha, frase de seguridad, imágenes, etc.).
Vulnerabilidades al servidor y/o al sistema web	Las vulnerabilidades pueden surgir en cualquier momento como consecuencia de utilizar versiones obsoletas o abandonadas de la plataforma que utiliza el sistema, el sistema operativo, librerías, dependencias, etc., incrementando la posibilidad de que personas malintencionadas aprovechen estos fallos de seguridad para obtener información personal de los usuarios.	Mantener actualizada la arquitectura sobre la cual está desarrollado la plataforma Moodle. Tener vigentes las librerías y/o dependencias que utilice el sistema para que se adapten a las actualizaciones de los nuevos navegadores y/o dispositivos electrónicos (“frameworks”, animaciones, íconos, exportación de datos, etc.). Actualizar siempre a la última versión la plataforma Moodle.
No contar con un servidor de respaldo en caso de fallo físico o de pérdida de información o un ambiente de pruebas.	En ocasiones por mantenimiento al servidor contingencia física o digital, en el ambiente productivo, sería óptimo contar con un respaldo del servidor para trabajar las actualizaciones del sistema o bien, utilizarlo como servidor respaldo para tener en operación 24/7 el sistema.	Instalar un servidor con las mismas características que se tiene en ambiente de producción para que, en caso de contingencia, se pueda trabajar temporalmente en este esquema.
Instalar el sistema en servidores con más de 5 años de uso	Fallas en el hardware del equipo y posible pérdida de información	Gestión de recursos para mantener actualizado el Hardware

No ha
inform

Eliminado: Análisis de riesgos.

Fundamentación: De conformidad con 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 los artículos 32 y 36 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

Motivación: En virtud de que estos datos hace identificable las formas en que es posible atacar o vulnerar nuestros sistemas de información que resguardan datos personales y 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.

4. ANÁLISIS DE BRECHA

Secretaría Técnica		
Identificador único*	EM017	
Nombre del sistema*	Moodle	
Medida de seguridad actual*	**Medida de seguridad necesaria***	**Acciones para remediación***
Acceso al sistema mediante una credencial de acceso que consta de un nombre de usuario y contraseña.	Evitar el acceso automatizado a personas no autorizadas o robots.	Implementar el uso de contraseñas de al menos 10 caracteres con las siguientes características: no palabras de diccionario, al menos: una letra mayúscula, una minúscula, un número, un caractér alfanumérico y simbolos especiales y “frases” fáciles de recordar para el usuario. Almacenamiento de contraseña en la base de datos de manera encriptada (algoritmo de reducción criptográfico de 128 bits). Agregar una capa extra de seguridad que identifique que efectivamente el usuario es un ser humano (captcha, imágenes, texto, etc.).

Solicitar a los administradores y usuarios del sistema que realicen la actualización de sus contraseñas de acceso al sistema al menos una vez al año.	Actualizar regularmente las contraseñas de acceso al sistema	Baja de usuarios y contraseñas una vez terminada la gestión del usuario, registro y actualización de contraseñas de usuarios nuevos.
Monitoreo del sistema con la arquitectura actual del sistema de tratamiento de datos personales.	Actualizar la arquitectura sobre la cual trabaja Moodle y en su caso, revisar el ajuste del sistema a las nuevas tecnologías.	Solicitar al responsable de la administración de servidores la actualización de la arquitectura sobre la que opera el sistema de tratamiento de datos personales. Verificar y asegurar la compatibilidad del sistema con la nueva versión del lenguaje de programación. Revisar el funcionamiento del sistema con la arquitectura actualizada. Actualizar la plataforma

Eliminado: Análisis de brecha.

Fundamentación: De conformidad con 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 los artículos 32 y 36 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

Motivación: En virtud de que estos datos hace identificable las formas en que es posible atacar o vulnerar nuestros sistemas de información que resguardan datos personales y 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.

5. PLAN DE TRABAJO

Secretaría Técnica			
Identificador único*	EM017		
Nombre del sistema *	Moodle		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Capa de seguridad extra para evitar accesos automatizados.	Investigar como habilitar una tecnología que impida el acceso automatizado o de “robots”	01 de agosto de 2022 al 31 de julio de 2023 (conforme se vaya requiriendo).	Evitar que los datos personales sean accedidos por personas no autorizadas o “robots” debido a accesos automatizados.
Implementar el uso de contraseñas de al menos 10 caracteres, que utilicen combinaciones de letras, números, símbolos y mayúsculas/minúsculas.	Creación de contraseñas seguras para los usuarios que utilicen el sistema.	01 de agosto de 2022 al 31 de julio de 2023 (conforme se vayan requiriendo).	Evitar que los datos personales sean accedidos por personas no autorizadas o robots debido por uso de contraseñas débiles en credenciales de acceso con privilegios administrativos.
Actualizar la arquitectura sobre la cual trabaja el sistema de tratamiento de datos personales.	Revisión, actualización y/o instalación de los componentes necesarios para que opere correctamente el sistema de datos personales.	01 de agosto de 2022 al 31 de julio de 2023.	Mantener actualizada la arquitectura sobre la que trabaja el sistema para evitar que los datos personales sean accedidos ante alguna vulnerabilidad de seguridad en versiones obsoletas o abandonadas de dicha arquitectura.
Funcionamiento integral del sistema con la arquitectura de trabajo actualizada y de	Revisar completament e el sistema para verificar	01 de agosto de 2022 al 31 de julio de 2023.	El sistema funciona adecuadamente bajo el esquema actualizado de trabajo para proteger los

la plataforma en su última versión.	su correcto funcionamiento con las versiones actualizadas de la plataforma de trabajo instaladas.		datos personales de los académicos y usuarios que hacen uso del sistema.

Eliminado: Plan de trabajo.

Fundamentación: De conformidad con 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 los artículos 32 y 36 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

Motivación: En virtud de que estos datos hace identificable las formas en que es posible atacar o vulnerar nuestros sistemas de información que resguardan datos personales y 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.

6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

I. TRANSFERENCIAS DE DATOS PERSONALES

Secretaría Técnica*	
Identificador único*	EM017
(Nombre del sistema A1)*	Moodle
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:[5]	No se realizan transferencias de datos personales mediante el traslado de soportes físicos.
Transferencias mediante el traslado de soportes electrónicos:	La transferencia de datos personales en soportes electrónicos la pueden realizar los usuarios especificados en este documento previa identificación con credenciales de acceso

[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.

	(usuario y contraseña). Los soportes electrónicos solicitados se hacen en formato de documentos portables y hojas de cálculo.
Transferencias mediante el traslado sobre redes electrónicas:	Actualmente no se cuenta con una infraestructura privada de almacenamiento (nube) en la ENES Unidad Morelia.

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]
2. Señalar en un listado las personas (nombre, cargo, funciones y obligaciones) que tienen acceso a los soportes físicos del sistema.[7]

La plataforma Moodle no realiza transferencia de datos personales en soportes físicos ya que todo el resguardo de los datos se hace mediante soporte electrónico mediante el uso de bases de datos relacionales y la transferencia a través de formato de documentos portables y hojas de cálculo. Cabe señalar que en estas bitácoras no se hace transferenca de datos personales.

II. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

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

[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:

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

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

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.

La plataforma Moodle cuenta con bitácoras de acceso y consulta de datos y acciones que los usuarios realizan dentro de la misma.

1) El acceso lo realiza el administrador de la plataforma o de la persona que tenga el permiso para su consulta.
2) Las bitácoras se almacenan en la base de datos relacional y pueden ser extraídas mediante soporte electrónico en hojas de cálculo.
3) Las bitácoras se almacenan permanentemente. Actualmente no hay una política de borrado de bitácoras ni herramientas para su análisis. Únicamente cuando se presenta un incidente se rastrea mediante la bitácora indicando el periodo y analizando manualmente la actividad del usuario dentro de la plataforma.

---

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.

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 cuenta con un procedimiento de atención de incidentes.

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 electrónicos7: Los campos, registros, tablas, bases de datos o archivos electrónicos, tanto dañados como recuperados, el nombre de los sistemas y la infraestructura afectada, indicar si el incidente afectó el servidor principal y los servidores de respaldo, etc.
2. Si el registro está en soporte físico o en soporte electrónico;
3. Cómo asegura la integridad de dicho registro, y
4. Para el caso de soportes electrónicos, quién autoriza la recuperación de datos.

V. ACCESO A LAS INSTALACIONES

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

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

Para las personas que acceden a sus instalaciones:

a) ¿Cómo las identifica?

No se cuenta con mecanismos de identificación.

---

[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.

b) ¿Cómo las autentifica?
No se cuenta con mecanismos de autenticación.

c) ¿Cómo les autoriza el acceso?
No se cuenta con mecanismos de control de acceso.

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

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

Para las personas que acceden a dichos espacios interiores:

1. ¿Cómo las identifica?
   Se tiene definida una lista de acceso para el personal autorizado.
2. ¿Cómo las autentifica?
   Mediante credencial y número de trabajador.
3. ¿Cómo les autoriza el acceso?
   Si se encuentran en la lista de acceso autorizada, o si son proveedores acompañados por un empleado autorizado. Se les solicita se registren en la bitácora correspondiente.

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

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

1) Cada usuario que se da de alta en esta plataforma tiene la opción de actualizar o corregir sus datos en la sección “Editar mi perfil”.

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

VII. PERFILES DE USUARIO Y CONTRASEÑAS

1. Modelo de control de acceso:

Basado en perfiles o privilegios de acceso (permisos).

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?
Únicamente las contraseñas.

4. Administración de perfiles de usuario y contraseñas:

a) ¿Quién da de alta nuevos perfiles?
El Responsable del sistema a su cargo. Lic. Gustavo Cano Salazar.

b) ¿Quién autoriza la creación de nuevos perfiles?
El Secretario Técnico autoriza la creación de nuevos perfiles con privilegios administrativos.

c) ¿Se lleva registro de la creación de nuevos perfiles?
Mediante control interno del Departamento de Sistemas Informáticos y a través del sistema.

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

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

b) ¿Requiere el administrador acceso remoto al equipo donde reside el sistema para realizar tareas de mantenimiento?
Si, con acceso mediante VPN y SSH.

c) ¿Cómo se evita el acceso remoto no autorizado?

- Se cuenta con controles de acceso basados en roles y privilegios.
- El acceso remoto a los servidores se realiza mediante conexiones VPN habilitadas únicamente a los responsables de los sistemas.
- Implementación de captcha en el inicio de sesión del sistema.

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

1. Señalar si realiza respaldos
- **a)** Completos_X_, diferenciales ___ o incrementales__X_;
- **b)** De forma automática ____ o Manual _X_,
- **c)** Periodicidad con que los realiza: _Semestral_

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 externo.

[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.

3. Cómo y dónde archiva esos medios, y Consultar los documentos: Plan de respaldos ENES Morelia y Bitácora de control de los respaldos.
4. Quién es el responsable de realizar estas operaciones (el área universitaria o un tercero). El responsable (encargado) del sistema a su cargo.

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.
   Se cuenta con algunas medidas como las especificadas en el documento: Medidas de seguridad en los periodos de inactividad o mantenimiento, pero no se tiene desarrollado el plan de contingencia.
2. Si cuenta con plan de contingencia y lo ha implementado, deberá indicar si realiza pruebas de eficiencia de este.
   No se cuenta con plan de contingencia.
3. Informar si cuenta con un sitio redundante (alterno) y señalar lo siguiente:
   a) El tipo de sitio (caliente, tibio o frío);[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.

Actualmente la ENES Unidad Morelia, no cuenta con sitio redundante para cubrir los incisos anteriores.

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*

[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.

Identificador único*	EM017	
Nombre del sistema*	Moodle	
Recurso*	**Descripción***	**Control***
Reportes especiales de datos almacenados en el sistema.	Al solicitar reportes que no se encuentran en el sistema y su descarga en soporte electrónico, estos se generan y se descargan mediante un vínculo que vence en determinado tiempo para su descarga.	Evitar adjuntar archivos por correo electrónico porque es un servicio de terceros (Google). Una vez vencido el plazo de descarga (max. 24 horas) es imposible volver a descargar el soporte electrónico solicitado.
Reportes especiales de datos almacenados en el sistema en soportes electrónicos adjuntos por correo electrónico.	Solicitud de reportes especiales entregados en un soporte electrónico específico (hoja de cálculo, texto plano, etc.) y que se piden se adjunten por correo electrónico.	Se utiliza un programa de software libre para cifrar el archivo y personalmente se indica la contraseña para descifrar en el equipo de cómputo del usuario para utilizar el archivo que fue adjuntado por correo electrónico.

7.2 Procedimiento para la revisión de las medidas de seguridad

Secretaría Técnica*		
Identificador único*	EM017	
Nombre del sistema*	Moodle	
Medida de seguridad*	**Procedimiento***	**Responsable***
Principio del menor privilegio	Otorgar el acceso al usuario autorizado por la Secretaría técnica de acuerdo con el permiso requerido.	Encargado del sistema. Lic. Gustavo Cano Salazar. (01 día hábil).

Respaldos del sistema y base de datos.	Generación de archivos de respaldo tanto del sistema de datos personales como de la base de datos y control de bitácoras de respaldo.	Encargado del sistema. Lic. Gustavo Cano Salazar. (01 día hábil).
Sincronizar la fecha y hora con el servidor NTP (Network Time Protocol) oficial de la UNAM	Revisiones periódicas de la hora y fecha del servidor donde se encuentra el sistema.	Mtro. Froylan Hernández Rendón (01 día hábil).
Instalar y mantener actualizado el software antimalware.	Revisión y actualización de la versión del software antivirus y de la base de datos.	Mtro. Froylan Hernández Rendón (01 día hábil).
Instalar las actualizaciones de seguridad más recientes disponibles.	Revisión y actualizaciones del sistema operativo.	Mtro. Froylan Hernández Rendón (02 días hábiles).

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

Secretaría Técnica*		
Identificador único*	EM017	
Nombre del sistema*	Moodle	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***
Principio del menor privilegio	Se encontró que todas las cuentas de usuarios del sistema cuentan con los permisos correspondientes.	Encargado del sistema. Lic. Gustavo Cano Salazar.
Respaldo del sistema y base de datos.	Se cuenta con respaldos actualizados de la información del sistema.	Encargado del sistema. Lic. Gustavo Cano Salazar.
Sincronizar la fecha y hora con el servidor NTP (Network Time Protocol) oficial de la UNAM	La fecha y hora están sincronizadas con el servidor NTP de la UNAM.	Mtro. Froylán Hernández Rendón.
Instalar y mantener actualizado el software antimalware.	El Software antivirus está actualizado.	Mtro. Froylán Hernández Rendón.

Instalar las actualizaciones de seguridad más recientes disponibles.	El sistema operativo cuenta con las actualizaciones correspondientes.	Mtro. Froylán Hernández Rendón.

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

Secretaría Técnica*		
Identificador único*	EM017	
Nombre del sistema*	Sistema de Evaluación Docente (SIEDO)	
Medida de seguridad*	**Acciones***	**Responsable***
Uso de certificados SSL	Implementar el protocolo “HTTPS” en el sistema. Realizar la renovación anual del certificado SSL para el subdominio donde se encuentra el sistema.	Mtro. Froylán Hernández Rendón

8 PROGRAMA ESPECÍFICO DE CAPACITACIÓN

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

Secretaría Técnica*			
Identificador único*	EM008		
Nombre del sistema*	Sistema de Evaluación Docente (SIEDO)		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Capacitación para la Protección de Datos Personales	Curso en línea	25 horas.	Público objetivo: Enlaces de Transparencia, Responsables de Seguridad de Datos

		Fecha de inicio: 20 de noviembre de 2020. Fecha de término: 17 de enero de 2021	Personales, Responsables de Tecnologías de la Información, así como funcionarios y empleados universitarios. Sin vigencia. Sin frecuencia de actualización.
Medidas de Seguridad Técnicas para la Protección de Datos Personales	Curso en línea	25 horas. Fecha de inicio: 8 de febrero de 2021. Fecha de término: 14 de marzo de 2021.	Público objetivo: Enlaces de Transparencia, Responsables de Seguridad de Datos Personales, Responsables de Tecnologías de la Información, así como funcionarios y empleados universitarios. Sin vigencia. Sin frecuencia de actualización.
Elaboración de Documento de Seguridad y Sistema de Gestión de Seguridad de Datos Personales de las áreas universitarias	Curso en línea	25 horas. Fecha de inicio: 25 de marzo de 2022 Fecha de término: 25 de marzo de 2022.	Público objetivo: Enlaces de Transparencia, Responsables de Seguridad de Datos Personales, Responsables de Tecnologías de la Información, así como funcionarios y empleados universitarios. Sin vigencia. Sin frecuencia de actualización.

La importancia de la protección de datos personales	Seminario en línea	1 hora. Fecha: 16 de junio de 2022.	Público en general. Sin vigencia. Sin frecuencia de actualización.

8.2 Programa de difusión de la protección a los datos personales

Secretaría Técnica*			
Identificador único*	EM017		
Nombre del sistema*	Moodle		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Indique actividad, tema, recursos para la difusión. Agregar un renglón por cada elemento	*Describa el tipo de elemento, sus objetivos y forma de impartición, publicación o distribución*	*Indique duración del elemento en horas, días, meses, su fecha de inicio y de término*	*Mencione público objetivo, vigencia del elemento y frecuencia de actualización*

Actualmente, no se cuenta con un programa de difusión de la protección de datos personales.

9 MEJORA CONTINUA

9.1 Actualización y mantenimiento de sistemas de información

Secretaría Técnica*			
Identificador único*	EM017		
Nombre del sistema*	Moodle		
Actividad*	**Descripción***	**Duración***	**Cobertura***

Actualización de tecnologías de desarrollo	1.Solicitud de actualización de la arquitectura de desarrollo del sistema de datos personales. 2. Corregir y/o actualizar módulos del sistema. 3. Pruebas unitarias e integrales de las actualizaciones realizadas al sistema. 4. Actualización de archivos de sistema y/o sentencias de bases de datos en servidor de producción. 5. Actualización a la última versión de la plataforma Moodle.	12 meses	“Back-end” del sistema.

9.2 Actualización y mantenimiento de equipo de cómputo

Secretaría Técnica*			
Identificador único*	EM017		
Nombre del sistema*	Moodle		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Indique actividad. Agregar un renglón por cada elemento	*Describa el tipo de actividad, sus objetivos e impacto la actualización o mantenimiento del equipo de cómputo*	*Indique duración en la ejecución de la actividad en horas, días, meses, su fecha de inicio y de término*	*Mencione los aspectos de equipo de cómputo que son resueltos, total o parcialmente, por la actividad.*

Actualmente, no se han asignado recursos para la actualización del equipo de cómputo.

9.3 Procesos para la conservación, preservación y respaldos de información

Secretaría Técnica*		
Identificador único*	EM017	
Nombre del sistema*	Moodle	
Proceso*	**Descripción***	**Responsable***
Poner en fase de “mantenimiento” del sistema.	Se coloca un mensaje en la parte de acceso al sistema con un aviso de “mantenimiento” y de ser posible la fecha de “regreso” a la operación del sistema.	Encargado del sistema: Lic. Gustavo Cano Salazar. (01 día hábil).
Ingresar remotamente al servidor.	Acceso al servidor de manera remota para realizar el respaldo de ambos componentes (script del sistema y de la base de datos)	Encargado del sistema: Lic. Gustavo Cano Salazar. (01 día hábil).
Descarga de respaldos del sistema a soporte físico electrónico.	Descarga directa al Disco Duro externo proporcionado por secretaría técnica con los respaldos realizados del sistema.	Encargado del sistema: Lic. Gustavo Cano Salazar. (01 día hábil).
Salida del servidor y de fase de “mantenimiento” en el sistema.	Quitar el mensaje del modo mantenimiento del sistema y salida completa del servidor.	Encargado del sistema: Lic. Gustavo Cano Salazar. (01 día hábil).
El proceso de respaldo de información se encuentra contenido en el documento: Plan de respaldos ENES Morelia	El proceso se describe en el documento: Plan de respaldos ENES Morelia	Encargado del sistema: Lic. Gustavo Cano Salazar. (01 día hábil).

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

Secretaría Técnica*		
Identificador único*	EM017	
(Nombre del sistema A1)*	Moodle	
Proceso*	**Descripción***	**Responsable***
Borrado de datos dentro del Sistema Gestor de Base de Datos.	Aplicación de transacciones y ejecución de instrucciones SQL para actualización y/o borrado de datos. Una vez completada la transacción aplicar la instrucción correspondiente para conservar o borrar definitivamente los datos.	Encargado del sistema: Lic. Gustavo Cano Salazar.
El proceso se encuentra contenido en el documento: Borrado Seguro ENES Morelia	El proceso se describe en el documento: Borrado Seguro ENES Morelia	Borrado seguro: Encargado del sistema: Lic. Gustavo Cano Salazar. Responsable de la disposición final de equipos o componentes de cómputo: Mtro. Froylán Hernández Rendón Tiempo máximo de ejecución: 05 días hábiles.

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

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

(Informar y describir el procedimiento para la cancelación de un sistema de tratamiento de datos personales.)[13]

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

a) Denominación
b) Motivo de la cancelación

B) PLAZOS Y CONDICIONES PARA EL BLOQUEO DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES:[14]

(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)

---

[13] 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.

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

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

Documento de Borrado seguro de la ENES Morelia.

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

Documento de Borrado seguro de la ENES Morelia.

APROBACIÓN DEL DOCUMENTO DE SEGURIDAD

		Nombre y firma de quienes revisaron el presente documento:
Responsable del desarrollo:	Froylan Hernández Rendón Responsable de Cómputo y Tecnologías de Información Tel. 4436893507ext. UNAM 37307 fhernandez@enesmorelia.unam.mx	
Revisó:	Santiago Cortés Hernández Secretario Técnico Tel. 4436893505 ext. UNAM 37305 secretaria_tecnica@enesmorelia.unam.mx	
Autorizó:	Mario Rodríguez Martínez Director Tel. 4436893501 ext. UNAM 37301 direccion@enesmorelia.unam.mx	
Fecha de aprobación:		23/05/2022
Fecha de actualización:		16/08/2022