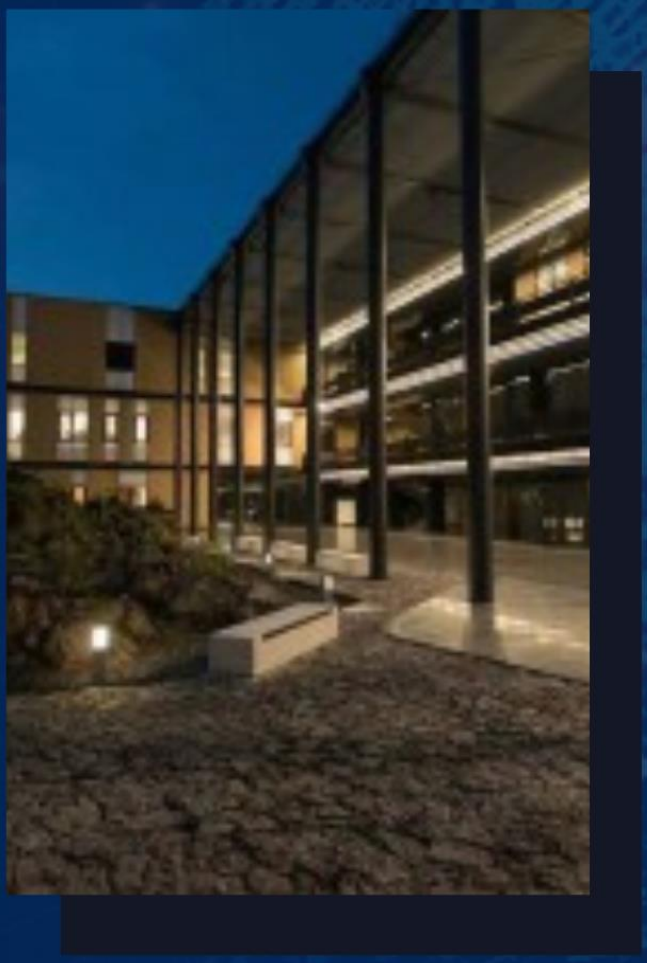
ESCUELA NACIONAL DE CIENCIAS FORENSES
UNAM

Documento de Seguridad de Datos Personales de la Escuela Nacional de Ciencias Forenses



2024

ÍNDICE

Introducción 2

1. Inventario de sistemas de tratamientos de datos personales..... 4

2. Estructura y descripción de los sistemas de tratamientos de datos personales 8

3. Análisis de riesgo en el tratamiento de datos personales 10

4. Análisis de brecha 12

5. Plan de trabajo 15

6. Medidas de seguridad implementadas 17

7. Mecanismos de monitoreo y revisión de las medidas de seguridad 28

8. Programa específico de capacitación..... 30

9. Mejora continua..... 33

10. Procedimiento para la cancelación de un sistema de tratamiento de datos personales 36

11. Aprobación del Documento de Seguridad..... 39

Anexo. Comité de Transparencia de la UNAM. Resolución:..... 40

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 Escuela Nacional de Ciencias Forenses con el fin de asegurar la integridad, confidencialidad y disponibilidad de la información personal que éstos contienen.

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

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”.

Finalmente, el presente documento, menciona las medidas de seguridad administrativas, físicas y técnicas aplicables a los sistemas de tratamiento de datos con el fin de trabajar acorde a los lineamientos institucionales y federales en el tratamiento de datos personales asegurando la integridad, confidencialidad y disponibilidad de la información de cada una de las personas que participan en las actividades académicas de la Escuela Nacional de Ciencias Forenses.

1. INVENTARIO DE SISTEMAS DE TRATAMIENTOS DE DATOS PERSONALES

Escuela Nacional de Ciencias Forenses	
Identificador único*	**ENACIF-Oficina Jurídica**
(Nombre del sistema A1) *	**Orientación Jurídica**
Datos personales (sensibles o no) contenidos en el sistema*:	• Identificación • Nombre(s) • Apellido paterno • Apellido materno • Número de Cuenta • Fecha de nacimiento • Firma o rúbrica de particulares • Fotografías de personas según sus identificaciones oficiales • Edad, • Sexo • Estado civil • Datos Escolares • Huellas dactilares • Correo electrónico • CURP • Domicilio particular • Números de Seguridad Social y registro ante el ISSSTE • Orientación sexual • Origen racial o étnico • Religión • Datos socioeconómicos • Teléfono particular • Cuotas sindicales

	• Información relativa al tránsito de las personas dentro y fuera del país e información migratoria de las personas • Ingresos y egresos • Nombres de familiares, dependientes y beneficiarios. • Parentesco (filiación) • Número de cuenta del alumno o número de matrícula escolar • Número de licencia de conducir • Nacionalidad • Información fiscal • Folio fiscal de facturas expedidas por personas físicas y morales • Número de pasaporte • Número de teléfono fijo o celular • Ocupación y/o estatus laboral de persona física • Participación societaria y nombre de socios, contenidos en documentos notariados, tales como escrituras públicas, estatutos, contratos y convenios privados. • Profesión u ocupación. • Referencias laborales. • Referencias familiares y/o personales • Registro Federal de Contribuyentes (RFC) • Secretos comerciales, industriales, fiscales, bancarios y fiduciarios, así como derecho de la propiedad intelectual (patentes y derechos de autor entre otros) • Seguros • Sello del comprobante fiscal digital por internet (CFDI) • Sello digital y/o código bidimensional.
Responsable*:	
Nombre*:	MÓNICA GUADALUPE RAMIREZ MONARES

Cargo*:	JEFA DE OFICINA JURÍDICA
Funciones*:	● Registrar la correspondencia recibida de manera física y/o electrónica, dirigida a la Oficina Jurídica, la cual pudiera contener datos personales. ● Supervisar el tratamiento de datos personales en poder de la Oficina Jurídica. ● Resguardar física y/o electrónicamente los datos personales recabados hasta en tanto se concluya el tiempo de resguardo legal para su envío al archivo histórico o su disposición final. ● Emitir y coordinar las medidas necesarias para salvaguardar y evitar cualquier vulneración a la seguridad de los datos personales en la Oficina Jurídica. ● Transferir la correspondencia entre la Oficina Jurídica al área que corresponda para su conocimiento, atención, desahogo y/o seguimiento según sea el caso ● Dar seguimiento al estatus que guardan los asuntos turnados. ● Gestionar la generación de los reportes necesarios para el debido funcionamiento de la Oficina Jurídica
Obligaciones*:	● Dar cumplimiento a las obligaciones en materia de tratamiento de datos personales que establece la normativa universitaria. ● Coordinar el acceso, consulta y, en su caso; la transmisión de datos personales con que cuenta la Oficina Jurídica. ● Adoptar las medidas necesarias para garantizar la confidencialidad de la información y los documentos en posesión de la Oficina Jurídica. ● Informar al responsable técnico de datos de la Dirección cuando ocurra o se detecte una posible vulneración a los datos personales. ● Instruir al personal de correspondencia de la Escuela Nacional de Ciencias Forenses, encargado de resguardar los datos personales, a no proporcionar información a personas no

	autorizadas. ● Resguardar el acceso a la información electrónica y documentos que contengan datos personales mediante el usuario y contraseña asignado, para la información electrónica, y a través del uso de llaves y su adecuado resguardo en el caso de información en documentos físicos. ● Mantener la integridad, disponibilidad y confidencialidad de la información. ● Proteger los datos personales contenidos en los documentos que ingresan a la Oficina Jurídica. ● Abstenerse de tratar los datos personales para finalidades distintas a las que tiene encomendadas. ● Abstenerse de realizar transferencias no autorizadas de datos personales relativos a su encargo; salvo por mandato expreso de autoridad competente. ● Cumplir con las medidas de seguridad implementadas por la legislación Universitaria. ● Asegurar el debido resguardo y tratamiento de datos personales en los términos que fije la normatividad vigente aplicable, procurando en todo momento la aplicación de las medidas de seguridad *administrativas, físicas y técnicas* para evitar una posible vulneración a los datos personales en posesión del área universitaria. ● Informar al superior jerárquico inmediato cuando ocurra una vulneración a los datos personales que obren en el sistema. ● Guardar confidencialidad respecto a los datos personales tratados.

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

Escuela Nacional de Ciencias Forenses	
Identificador único*	**ENACIF-Oficina Jurídica**
(Nombre del sistema A1) *	**Orientación Jurídica**
Tipo de soporte:*	El sistema se encuentra en soporte físico y electrónico.
Descripción:	Soporte físico: Archivos donde están los documentos y/o expedientes. Soporte electrónico: Los datos personales del sistema están alojados en un servidor administrado por la Escuela Nacional de Ciencias Forenses y almacenados en el equipo de cómputo destinado a la Oficina Jurídica.
Características del lugar donde se resguardan los soportes	• **SOPORTE FÍSICO: Archiveros en oficina** con ventilación natural, luz natural y artificial, puerta de acceso de madera y chapa, aislada de la humedad que permiten la adecuada conservación de los documentos, los cuales se encuentran bajo llave y con control de acceso al personal facultado para ello. También en **almacén de resguardo** con ventilación natural, luz artificial, puerta de acceso de madera y chapa, aislada de humedad con muebles que permiten la conservación adecuada de los documentos. • **SOPORTE ELECTRÓNICO:** La **base de datos electrónica** en el Servidor propio de la Escuela Nacional de Ciencias Forenses.

	Existe acceso controlado a las instalaciones por medio del responsable del sitio. La información consta en archivos de microsoft office en la computadora que cuenta con claves de acceso biométricos de alta seguridad conforme a los estándares mínimos requeridos cuyo acceso es limitado al personal de esa área.

En la Escuela Nacional de Ciencias Forenses el tratamiento de datos personales que se manejan en cada una de las áreas recae en cada persona que sea responsable de su departamento, área o secretaría.

Se están llevando acciones concretas que permitan visibilizar e implementar las disposiciones y lineamientos establecidos en nuestra Universidad y que sean acordes a la normatividad del INAI.

Es importante reiterar que nuestra entidad sigue los lineamientos planteados en la Unidad de Transparencia de la UNAM y en el manejo de Datos personales (www.datospersonales.unam.mx) Asimismo, los lineamientos de Aviso de Privacidad se encuentran plasmados en nuestro sitio web en la siguiente liga http://www.enacif.unam.mx/transparencia

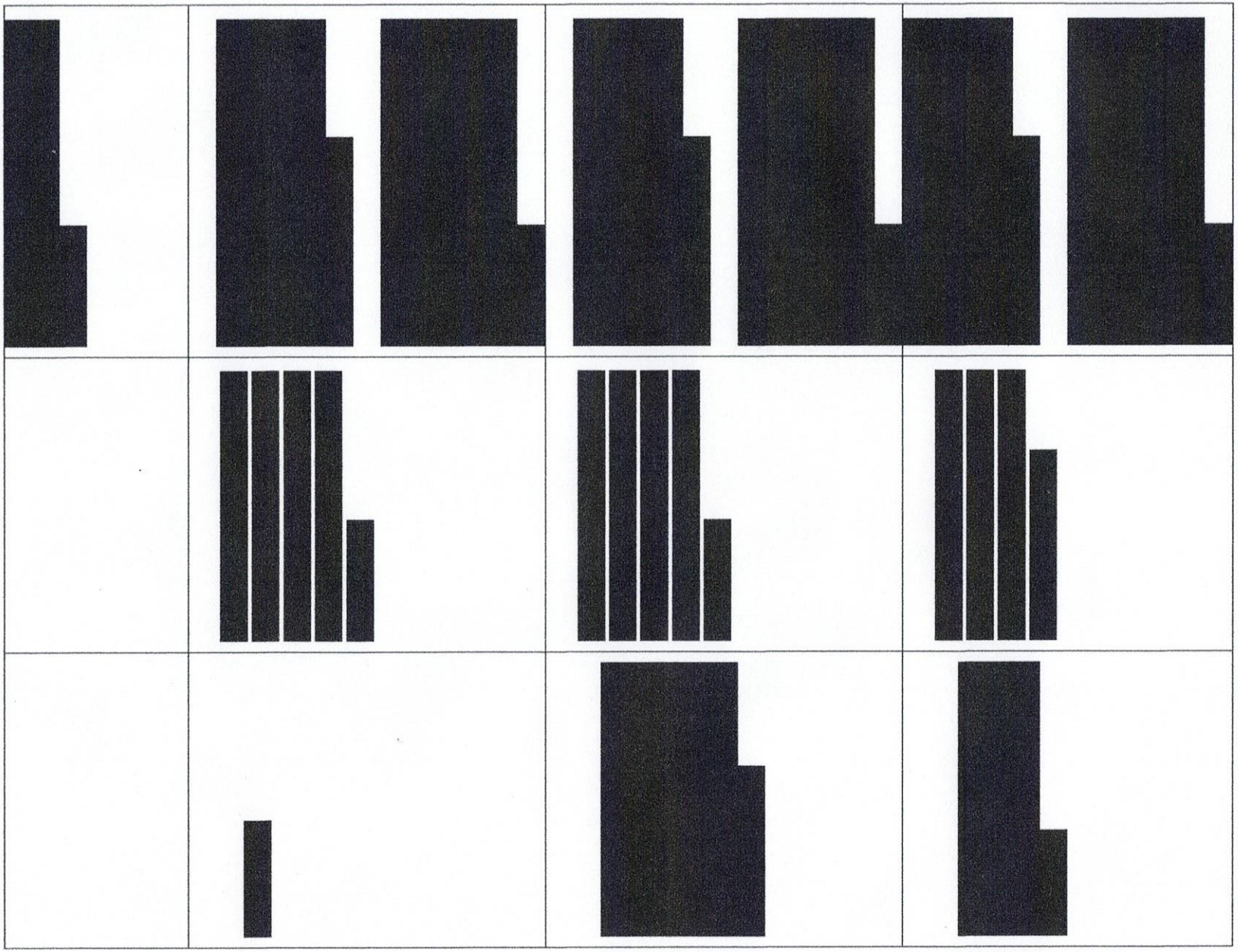
3. ANÁLISIS DE RIESGOS

La seguridad se basa en el entendimiento de la naturaleza del riesgo al que están expuestos los datos personales, el riesgo no se puede erradicar completamente pero sí se puede minimizar a través de la mejora continua.

El objetivo de esta sección es que los responsables determinen las características del riesgo que mayor impacto puede tener sobre los datos personales que tratan, con el fin de que prioricen y tomen la mejor decisión respecto a los controles más relevantes e inmediatos a implementar, en ese sentido, para la Escuela Nacional de Ciencias Forenses, el análisis de riesgo comprende los siguientes resultados:

Escuela Nacional de Ciencias Forenses		
Identificador único*	ENACIF-Oficina Jurídica	
(Nombre del sistema A1	Orientación Jurídica	
Riesgo*	Impacto*	Mitigación*
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

ELIMINADO: ANÁLISIS DE RIESGOS contenidos en el documento de seguridad toda vez que dar a conocer dicha información potencializa el nivel de vulnerabilidad de las medidas de seguridad de los datos personales en posesión de la Escuela Nacional de Ciencias Forenses de la Universidad Nacional Autónoma de México, lo que traería como consecuencia una posible comisión de delitos tipificados en el Código Penal Federal, como lo son, acceso no autorizado a los sistemas , robos de información suplantación de identidades, entre otros. FUNDAMENTO LEGAL: Artículo 113 fracción VII de la Ley General de Transparencia y Acceso a la Información Pública, artículo 110 fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública, en correlación con el artículo 41 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México publicado en la Gaceta UNAM el 25 de agosto de 2016, así como los numerales Quincuagésimo Sexto, Sexagésimo Primero de los Lineamientos Generales en materia de Clasificación y Desclasificación de la Información, así como para la elaboración de Versiones Públicas.



4.ANÁLISIS DE BRECHA

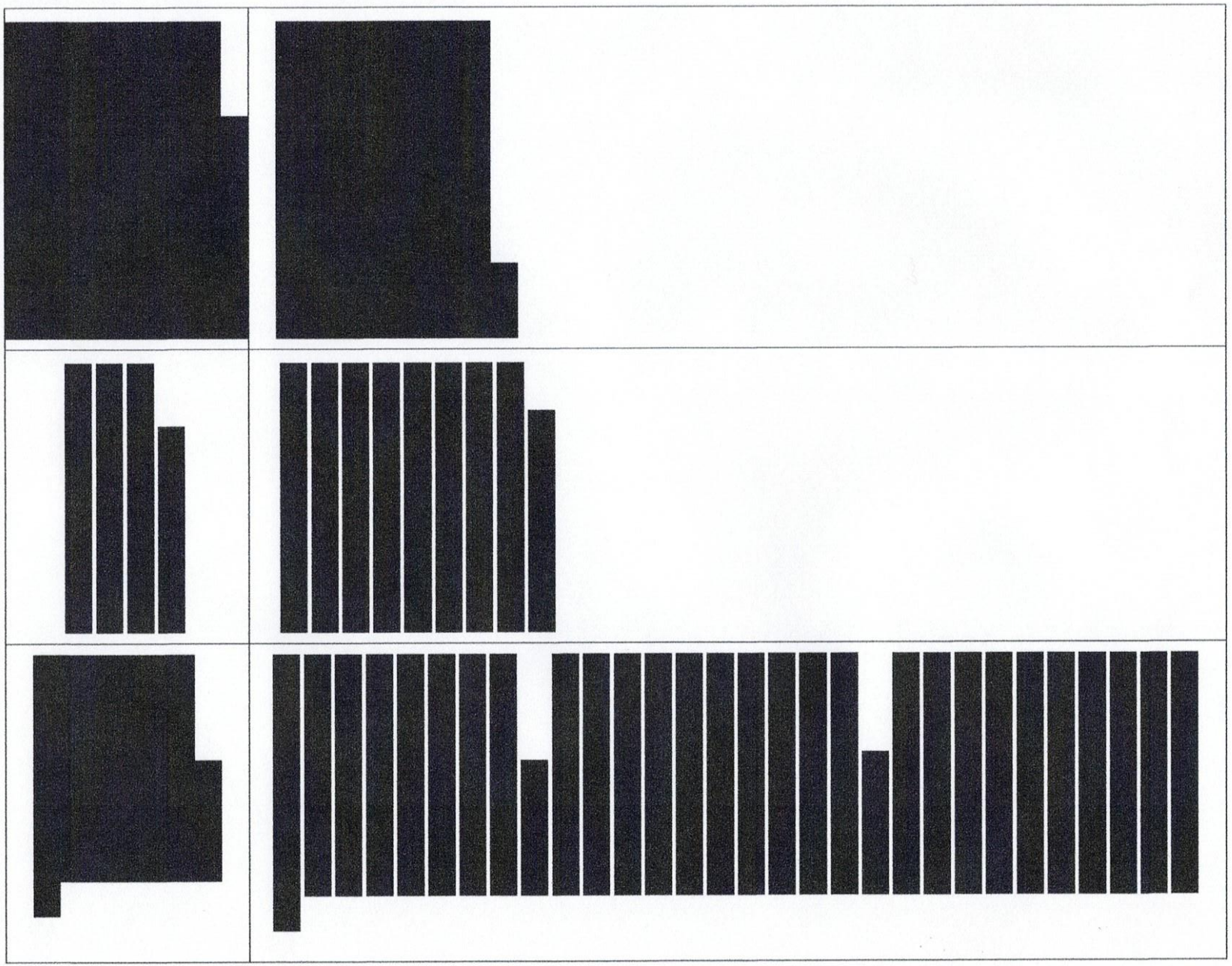
Este análisis consiste en identificar:

[redacted]

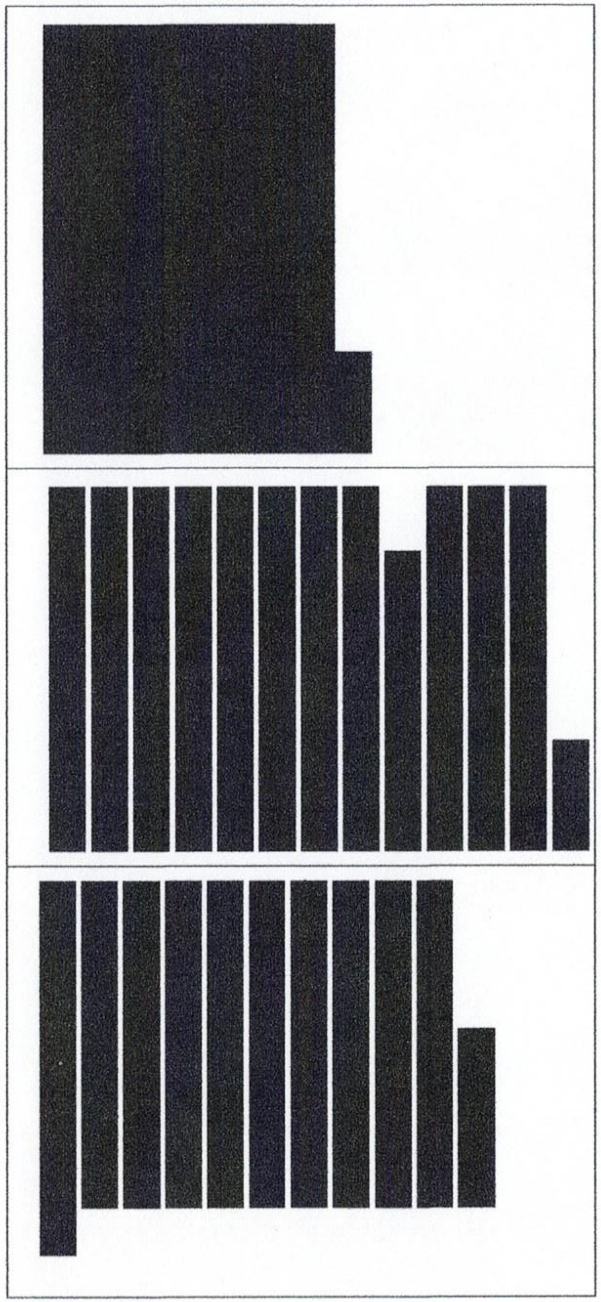
En este caso, para la Escuela Nacional de Ciencias Forenses se presentan los siguientes:

Escuela Nacional de Ciencias Forenses		
Identificador único*	ENACIF-Oficina Jurídica	
(Nombre del sistema A1) *	Orientación Jurídica	
Medida de seguridad actual*	**Medida de seguridad necesaria***	**Acciones para remediación***
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	

ELIMINADO: ANÁLISIS DE BRECHA contenido en el documento de seguridad toda vez que dar a conocer dicha información potencializa el nivel de vulnerabilidad de las medidas de seguridad de los datos personales en posesión de la Escuela Nacional de Ciencias Forenses de la Universidad Nacional Autónoma de México, lo que traería como consecuencia una posible comisión de delitos tipificados en el Código Penal Federal, como lo son, acceso no autorizado a los sistemas , robos de información suplantación de identidades, entre otros. FUNDAMENTO LEGAL : Artículo 113 fracción VII de la Ley General de Transparencia y Acceso a la Información Pública, artículo 110 fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública, en correlación con el artículo 41 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México publicado en la Gaceta UNAM el 25 de agosto de 2016, así como los numerales Quincuagésimo Sexto, Sexagésimo Primero de los Lineamientos Generales en materia de Clasificación y Desclasificación de la Información, así como para la elaboración de Versiones Públicas.



ELIMINADO: ANÁLISIS DE BRECHA contenido en el documento de seguridad toda vez que dar a conocer dicha información potencializa el nivel de vulnerabilidad de las medidas de seguridad de los datos personales en posesión de la Escuela Nacional de Ciencias Forenses de la Universidad Nacional Autónoma de México, lo que traería como consecuencia una posible comisión de delitos tipificados en el Código Penal Federal, como lo son, acceso no autorizado a los sistemas , robos de información suplantación de identidades, entre otros. FUNDAMENTO LEGAL : Artículo 113 fracción VII de la Ley General de Transparencia y Acceso a la Información Pública, artículo 110 fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública, en correlación con el artículo 41 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México publicado en la Gaceta UNAM el 25 de agosto de 2016, así como los numerales Quincuagésimo Sexto, Sexagésimo Primero de los Lineamientos Generales en materia de Clasificación y Desclasificación de la Información, así como para la elaboración de Versiones Públicas.



5. PLAN DE TRABAJO

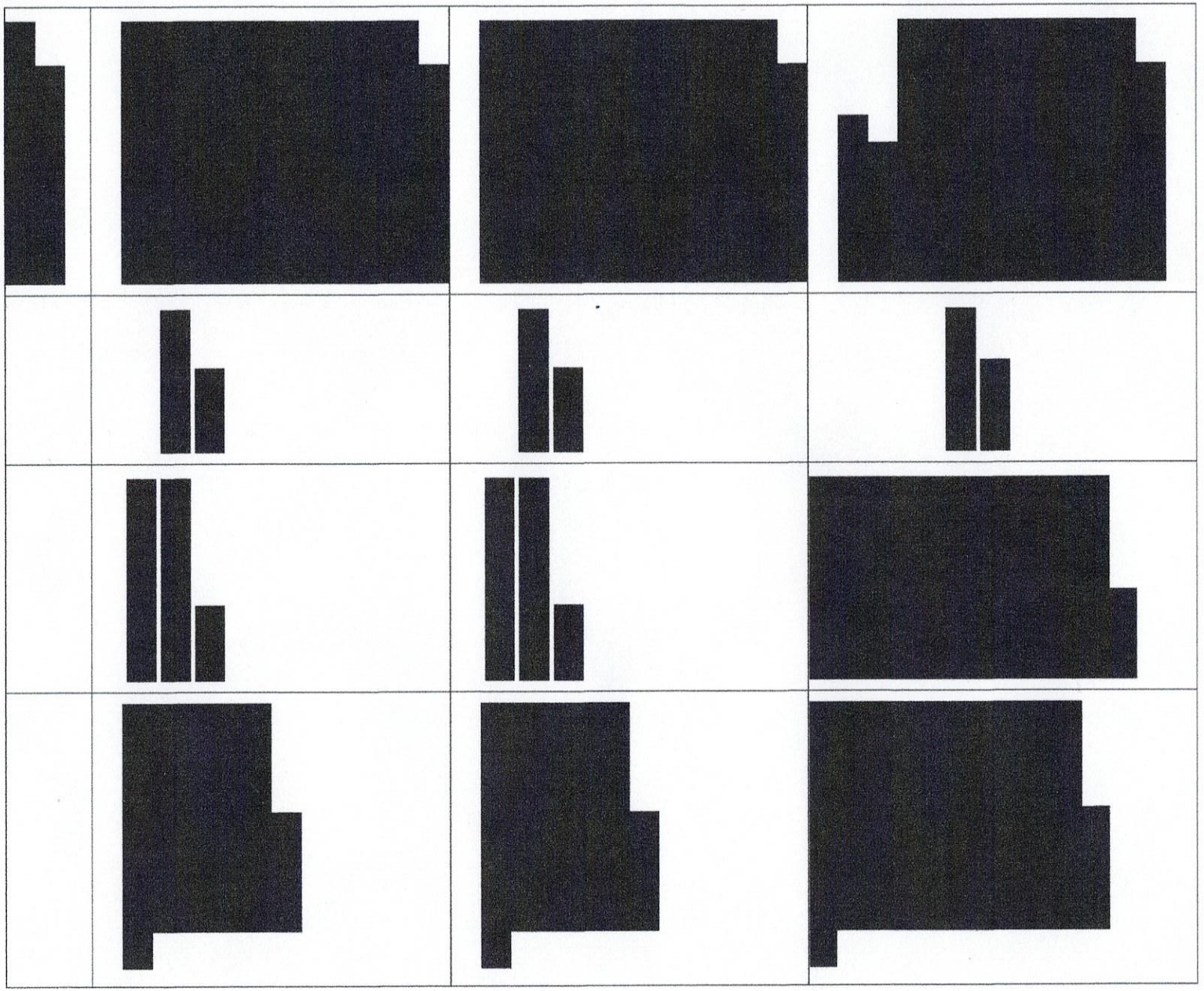
A continuación, se presenta un plan de trabajo inicial [redacted]

[redacted]

ESCUELA NACIONAL DE CIENCIAS FORENSES			
Identificador único*	ENACIF-Oficina Jurídica		
(Nombre del sistema A4) *	Orientación Jurídica		
Actividad*	Descripción*	Duración*	Cobertura*
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]

ELIMINADO: PLAN DE TRABAJO contenido en el documento de seguridad toda vez que dar a conocer dicha información potencializa el nivel de vulnerabilidad de las medidas de seguridad de los datos personales en posesión de la Escuela Nacional de Ciencias Forenses de la Universidad Nacional Autónoma de México, lo que traería como consecuencia una posible comisión de delitos tipificados en el Código Penal Federal, como lo son, acceso no autorizado a los sistemas, robos de información suplantación de identidades, entre otros. FUNDAMENTO LEGAL: Artículo 113 fracción VII de la Ley General de Transparencia y Acceso a la Información Pública, artículo 110 fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública, en correlación con el artículo 41 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México publicado en la Gaceta UNAM el 25 de agosto de 2016, así como los numerales Quincuagésimo Sexto, Sexagésimo Primero de los Lineamientos Generales en materia de Clasificación y Desclasificación de la Información, así como para la elaboración de Versiones Públicas.

ELIMINADO: PLAN DE TRABAJO contenido en el documento de seguridad toda vez que dar a conocer dicha información potencializa el nivel de vulnerabilidad de las medidas de seguridad de los datos personales en posesión de la Escuela Nacional de Ciencias Forenses de la Universidad Nacional Autónoma de México, lo que traería como consecuencia una posible comisión de delitos tipificados en el Código Penal Federal, como lo son, acceso no autorizado a los sistemas , robos de información suplantación de identidades, entre otros. FUNDAMENTO LEGAL : Artículo 113 fracción VII de la Ley General de Transparencia y Acceso a la Información Pública, artículo 110 fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública, en correlación con el artículo 41 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México publicado en la Gaceta UNAM el 25 de agosto de 2016, así como los numerales Quincuagésimo Sexto, Sexagésimo Primero de los Lineamientos Generales en materia de Clasificación y Desclasificación de la Información, así como para la elaboración de Versiones Públicas.



6.MEDIDAS DE SEGURIDAD IMPLEMENTADA

Son el conjunto de acciones, actividades, controles o **mecanismos** *técnicos*, *administrativos* y *físicos* que permitan proteger los datos personales:

Por lo anterior, y de acuerdo a lo expuesto en el apartado de análisis de brechas, se considera que se deben implementar las medidas de seguridad siguientes:

I. TRANSFERENCIA DE DATOS PERSONALES

Escuela Nacional de Ciencias Forenses	
Identificador único*	**ENACIF-Oficina Jurídica**
(Nombre del sistema A1) *	**Orientación Jurídica**
TRANSFERENCIA DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos	a) La transmisión de datos personales mediante el traslado de soportes físico se lleva a cabo por la vía elegida de común acuerdo entre las partes: mensajero oficial, asistente secretarial, o responsable de Oficina Jurídica b) El documento en sobre 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 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 documento en sobre 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 de la Oficina Jurídica. g) Estos envíos por correspondencia ordinaria sólo son aceptables si los datos personales requieren un nivel de

	protección básico o si los datos están disociados de sus titulares, en tratándose de documentos como convenios, bases de colaboración y contratos, o expedientes de procedimientos jurídicos, el envío se realiza de forma personal por la titular de la Oficina Jurídica.
Transferencias mediante el traslado de soportes electrónicos.	● no aplica para el SISTEMA- S1
Transferencias mediante el traslado sobre redes electrónicas.	● La transmisión de datos personales mediante el traslado de soportes sobre redes electrónicas se realiza a través del correo institucional debidamente acreditado. ● El remitente y/o destinatario cuentan con dispositivos que faciliten la detección de intrusiones en el canal de comunicación. ● Se acusa de recibida la información y se solicita el acuse respectivo por cada envío. ● El remitente registra las transferencias en la bitácora que se forma de manera automática mediante el sistema de correos institucional. ● Las transferencias de datos personales se formalizan en su mayoría mediante instrumento jurídico.

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

Escuela Nacional de Ciencias Forenses	
Identificador único*	**ENACIF-Oficina Jurídica**
(Nombre del sistema A1) *	**Orientación Jurídica**
RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTE FÍSICOS	
Resguardo de sistemas de tratamiento de datos personales con soporte físico	● **MEDIDAS IMPLEMENTADAS EN Archiveros en oficina** con ventilación natural, luz natural y artificial, puerta de acceso de madera y chapa, aislada de la humedad que permiten la adecuada conservación de los documentos, los cuales se encuentran bajo llave y con control de acceso al personal facultado para ello. También en **almacén de resguardo** con ventilación natural, luz artificial, puerta de acceso de madera y chapa, aislada de humedad con muebles que permiten la conservación adecuada de los documentos. ● Las únicas personas con acceso a través de llaves a los expedientes físicos del sistema de datos, que se encuentran en el **almacén de resguardo de archivos**

	son: a. Mónica Guadalupe Ramírez Monares, jefa de Oficina Jurídica, con funciones de representación legal de la entidad académica y las demás que señala la legislación universitaria; b. Karla Ivonne Vázquez Barrera, jefa de Vinculación, con las funciones que señala la legislación universitaria; c. Zoraida García Castillo, directora de la entidad, con las funciones que señala la legislación universitaria; d. Rosa Monroy Ramírez, asistente de dirección, con las funciones que señala la legislación universitaria: e. Roberto Amaro Lomelí, jefe de servicios generales, bienes y suministros, con las funciones que señala la legislación universitaria; Todos esos 5 funcionarios tienen las siguientes obligaciones: ● Asegurar el debido resguardo y tratamiento de datos personales en los términos que fije la normatividad vigente aplicable, procurando en todo momento la aplicación de las medidas de seguridad administrativas, físicas y técnicas para evitar una posible vulneración a los datos personales en posesión del área universitaria. ● Abstenerse de tratar los datos personales para finalidades distintas a las cuales fueron recabadas. ● Informar al superior jerárquico inmediato cuando ocurra una vulneración a los datos personales que obren en el sistema. ● Guardar confidencialidad respecto a los datos personales tratados. ● Abstenerse de transferir los datos personales salvo por mandato expreso de autoridad competente. Por lo que hace a la información del sistema de orientación jurídica que se encuentra **al interior de la Oficina Jurídica**, tienen acceso a los soportes físicos a través de *llaves* sólo: ● Mónica Guadalupe Ramírez Monares, jefa de Oficina Jurídica, con funciones de representación legal de la entidad académica; ● Roberto Amaro Lomelí, jefe de servicios generales,

	bienes y suministros, con las funciones que señala la legislación universitaria; Cuyas obligaciones son: ● Asegurar el debido resguardo y tratamiento de datos personales en los términos que fije la normatividad vigente aplicable, procurando en todo momento la aplicación de las medidas de seguridad administrativas, físicas y técnicas para evitar una posible vulneración a los datos personales en posesión del área universitaria. ● Abstenerse de tratar los datos personales para finalidades distintas a las cuales fueron recabadas. ● Informar al superior jerárquico inmediato cuando ocurra una vulneración a los datos personales que obren en el sistema. ● Guardar confidencialidad respecto a los datos personales tratados. ● Abstenerse de transferir los datos personales salvo por mandato expreso de autoridad competente.

III. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

Escuela Nacional de Ciencias Forenses	
Identificador único*	**ENACIF-Oficina Jurídica**
(Nombre del sistema A1) *	**Orientación Jurídica**
No aplica porque no se usa bitácora de **acceso** para la operación cotidiana del sistema de la Oficina Jurídica.	

IV. REGISTRO DE INCIDENTES

Escuela Nacional de Ciencias Forenses	
Identificador único*	**ENACIF-Oficina Jurídica**
(Nombre del sistema A1) *	**Orientación Jurídica**

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, recabando los siguientes datos:

1) Nombre de la persona que resolvió el incidente;
2) La metodología aplicada basada en lo siguiente:

(a) El incidente se registra en una hoja de cálculo anotando quién resolvió el incidente y los soportes dañados y recuperados. Dicha hoja de cálculo está protegida con una contraseña de acceso. Su integridad se garantiza generando y almacenando un resumen en la computadora, y en el sistema de almacenamiento virtual asignado para la oficina jurídica.

(b) 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 Escuela Nacional de Ciencias Forenses para su conocimiento y al titular del área jurídica Mtra. Mónica Guadalupe Ramírez Monares para presentar denuncias o querellas ante el Ministerio Público para que en el ámbito de sus competencias determine lo conducente.

(c) 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 datos personales da aviso por escrito a dichos titulares, a más tardar cinco días naturales de haber ocurrido el incidente, recabando el acuse de recibo de esta notificación. Adicionalmente se da aviso por correo electrónico o por teléfono.

3) Para los soportes físicos: los oficios, documentos, expedientes, estantes o archiveros, tanto los dañados como los recuperados.
4) Para soportes electrónicos: los campos, registros, tablas, bases de datos o archivos electrónicos tanto dañados como recuperados, el nombre de los sistemas y la infraestructura afectada, indicando si se afectó el servidor principal y los de respaldo.

b) El registro está en soporte físico o electrónico.
c) Su integridad se garantiza al restringir el acceso y uso de ésta, la cual se resguarda bajo llave, se genera y almacena un resumen creado para su respaldo en una carpeta en la nube del servidor interno de la Entidad. Para los soportes físicos se resguardan en una oficina bajo llave y con acceso restringido sólo a personal autorizado.

d) Para el caso de soportes electrónicos, quien autoriza la recuperación de datos es el responsable técnico del sistema, previa autorización de la titular de la Escuela Nacional de Ciencias Forenses.

V. ACCESO A LAS INSTALACIONES

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

   Para el control de acceso a la Escuela Nacional de Ciencias Forenses, se cuenta con un sólo punto de acceso mediante control el cual es para las personas que acceden a las instalaciones:

   a. Se identifican:
      - Personas que laboran en la Escuela Nacional de Ciencias Forenses, mediante huella dactilar
      - Personas externas a la Escuela, el personal adscrito a la ENaCiF corrobora su identidad y el motivo de su visita.

   b. Se autentifican:
      - Personas externas a la ENaCiF, con algún documento de identificación oficial, que acredite su identidad.

   c. Se autoriza el acceso de acuerdo con las:
      - Personas que laboran en la ENaCiF, automáticamente, después de corroborar su identidad y autentficarla.
      - Personas externas a la ENaCiF, después de acreditar y autentificar su identidad.

2. **Seguridad perimetral interior donde se ubica el sistema físico y electrónico.**

   Las medidas de seguridad que se han implementado para controlar el acceso a los espacios en los cuales se almacenan los soportes físicos y/o electrónicos del sistema, son las siguientes:

   - Control de entrada y salida física del personal de la ENaCiF
   - Puertas con cerradura reforzada
   - Sistema de cámaras de video vigilancia las 24 horas.

   Para las personas que acceden a los espacios interiores:

   - Se accede a través de llaves de acceso a los lugares físicos que albergan la información.

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

Escuela Nacional de Ciencias Forenses	
Identificador único*	**ENACIF-Oficina Jurídica**
(Nombre del sistema A1) *	**Orientación Jurídica**
ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES	
La actualización de la información contenida tanto en el formato físico como electrónico, se realiza de oficio por parte del responsable del Sistema de Orientación Jurídica. Para la rectificación de los datos personales contenidos en el Sistema, las personas que así lo soliciten, deberán seguir el procedimiento previsto para tal efecto en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y; en los Lineamientos para la Protección de Datos Personales en Posesión de la Universidad Nacional Autónoma de México.	

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

VII. PERFILES DE USUARIO Y CONTRASEÑAS

Escuela Nacional de Ciencias Forenses	
Identificador único*	**ENACIF-Oficina Jurídica**
(Nombre del sistema A1) *	**Orientación Jurídica**

1. Modelo de control de acceso:
    a. El modelo de control de acceso utilizado en el sistema está basado en roles, haciendo uso de una cuenta de usuario que permite el acceso a recursos específicos; por lo tanto, todos los usuarios tienen control total de los recursos y funciones, razón por lo cual únicamente los responsables de dichos sistemas tienen acceso.
2. Perfiles de usuario y contraseña en el sistema operativo de red:

    a. ¿Cuenta con un sistema operativo o red instalado en sus equipos? Estrictamente no. Sin embargo, los equipos de cómputo pueden compartir recursos y servicios como la impresora y el escaner que en sentido amplio puede considerarse una red.

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

   sí

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?

      sí

4. Administración d e perfiles de usuarios y contraseñas:
   a. ¿Quién da de alta los nuevos perfiles?

      El responsable técnico de los sistemas.

   b. ¿Quién autoriza la creación de nuevos perfiles?

      La titular de la Escuela Nacional de Ciencias Forenses.

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

      Si.

5. Acceso remoto al sistema de tratamiento de datos personales:
   a. ¿Requieren los usuarios acceso remoto al equipo de cómputo que por lo general utilizan para trabajar con el sistema?

      No.

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

      No.

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

      El servidor que aloja la base de datos únicamente permite el acceso desde los equipos conectados a la red local.

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

Escuela Nacional de Ciencias Forenses	
Identificador único*	**ENACIF-Oficina Jurídica**
(Nombre del sistema A1) *	**Orientación Jurídica**

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

1. Señalar si realiza respaldos

   a. completos X, diferenciales X , o incrementales __ ;
   (*Un backup o copia de seguridad diferencial consiste en respaldar únicamente los datos modificados o de nueva creación, partiendo de una copia de seguridad completa anterior. Por ejemplo, si el lunes realizamos una copia de seguridad completa de nuestro sistema, podemos programar una copa diferencial para el fin de mes*).

   b. De forma automática ___ o Manual X ,

   c. Periodicidad con qué los realiza:

   Se realiza un respaldo completo cada mes y respaldos diferenciados por semana.

2. El tipo de medios (por ejemplo: cintas magnéticas, discos duros, CD-ROM, entre otros)

   Todos los respaldos se almacenan en la nube del servidor local de la Escuela Nacional de Ciencias Forenses; en la nube asignada por la Oficina de la Abogacía General a través de la Coordinación de Oficinas Jurídicas; y, en disco duro mecánico.

3. ¿Cómo y dónde archiva esos medios?

   El disco Duro está alojado físicamente en el servidor donde se encuentra la base de datos, esto es en el cuarto de telecomunicaciones de la Escuela Nacional de Ciencias Forenses.

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

   El titular del Departamento de Informática es el responsable de realizar y resguardar los respaldos.

IX. PLAN DE CONTINGENCIA

Escuela Nacional de Ciencias Forenses	
Identificador único*	**ENACIF-Oficina Jurídica**
(Nombre del sistema A1) *	**Orientación Jurídica**
PLAN DE CONTINGENCIA para soporte electrónico.	

Previo a una contingencia se trabajará en entrenar y concientizar en temas de ciberseguridad a todos los empleados de la organización, no solo por la prevención, sino también por la contención a través de un escudo humano que ayude a detectar y reportar cualquier irregularidad. Seguir el principio de mínimo privilegio; es decir, que un usuario solo debe tener acceso a aquella información estrictamente necesaria para desempeñar sus funciones diarias.

El plan de contingencia consiste en:

1. Hacer un inventario

Funciona para determinar qué datos y recursos se vieron comprometidos o fueron robados, y qué procesos de operatividad se vieron afectados con esto. Al mismo tiempo, hay que analizar, qué sistemas de la arquitectura se vieron afectados.

2. Revisar los requerimientos regulatorios

Cumplir con la ley es fundamental. Por regla general los datos críticos deberían ser almacenados fuera de línea por, al menos, un año como respaldo.

3. Ubicar a las autoridades

Se trata de conocer a qué autoridades locales y ordenamientos regulatorios es necesario involucrar dentro y fuera de la Universidad Nacional Autónoma de México.

4. Recaudar toda la evidencia posible

En caso de que el incidente acarree consecuencias legales, es importante saber qué pasó y tener registro. Hacer una lista de los datos que se pueden recabar, desde antes de cualquier incidente, permite que no se olvide ninguno.

5. Tener sistemas de redundancia

Debido a que los sistemas comprometidos deberán ser puestos en cuarentena, es importante tener sistemas de redundancia, para que el análisis forense pueda llevarse a cabo. Las capacidades de cuarentena son especialmente importantes para evitar que el ataque se propague.

6. Herramientas de rastreo

Contar con las herramientas tecnológicas que permitan al equipo de Cómputo y Tecnologías de la Información rastrear el camino de ataque hacia su entrada. De este modo poder contrarrestarlo y aislarlo. además de identificar cuáles otros sistemas han sido comprometidos.

7. MECANISMOS DE MONITOREO Y REVISIÓN DE MÉTODOS DE SEGURIDAD

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

Escuela Nacional de Ciencias Forenses		
Identificador único*	**ENACIF-Oficina Jurídica**	
(Nombre del sistema A1) *	**Orientación Jurídica**	
Recurso*	**Descripción***	**Control***
Software Antivirus	El Software antivirus de protección instalado es el McAfee. Monitorea constantemente la actividad del equipo de cómputo que contiene el sistema.	Se tiene software instalado con licencia activa y con las actualizaciones automáticas en el equipo de cómputo. Se solicita a los usuarios indicar si se activa alguna alerta por contenido malicioso.

7.2 Procedimiento para la revisión de las medidas de seguridad

Escuela Nacional de Ciencias Forenses		
Identificador único*	**ENACIF-Oficina Jurídica**	
(Nombre del sistema A1) *	**Orientación Jurídica**	
Medida de seguridad*	**Procedimiento***	**Responsable***
Análisis en tiempo real del software Antivirus	Al momento de instalarse el software se activó el análisis en tiempo real, el cual se ejecuta en segundo plano en el equipo de cómputo analizando archivos y sitios web para identificar posibles amenazas a los recursos.	El Departamento de Cómputo y Telecomunicaciones revisa la correcta ejecución del antivirus en los equipos de cómputo con un monitoreo constante.

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

Escuela Nacional de Ciencias Forenses		
Identificador único*	**ENACIF-Oficina Jurídica**	
(Nombre del sistema A1) *	**Orientación Jurídica**	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***
Análisis en tiempo real del software Antivirus	No se ha detectado la presencia de virus ni software malicioso procedente de recursos de internet descargados por el equipo de cómputo.	El Departamento de Cómputo y Telecomunicaciones realiza la evaluación constante.

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

Escuela Nacional de Ciencias Forenses		
Identificador único*	**ENACIF-Oficina Jurídica**	
(Nombre del sistema A1) *	**Orientación Jurídica**	
Medida de seguridad*	**Acciones***	**Responsable***
Análisis en tiempo real del software Antivirus	Revisar la correcta instalación, activación y actualización del software antivirus en el equipo de cómputo.	El Departamento de Cómputo y Telecomunicaciones es el responsable de llevar a cabo las actualizaciones con fecha límite el 7 de junio de 2024

8. PROGRAMA DE CAPACITACIÓN

8. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

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

Escuela Nacional de Ciencias Forenses			
Identificador único*	**ENACIF-Oficina Jurídica**		
(Nombre del sister A1) *	**Orientación Jurídica**		
Actividad*	**Descripción***	**Duración ***	**Cobertura***
Capacitación sobre protección de Datos Personales en posesión de la UNAM	Conocer las obligaciones derivadas del tratamiento de datos personales en el área. 1. Introducción a la Protección de Datos Personales. ➔ Conceptos y figuras claves en la LGPDPPSO. ➔ Principios y deberes de protección de datos personales. ➔ Principios de protección de datos personales. ➔ Deberes de seguridad y confidencialidad. ➔ Obligaciones Específicas: ◆ Encargados ◆ Régimen de transferencias y ◆ Evaluaciones de impacto. 2. Elaboración de Avisos de Privacidad Integral y Simplificados de las áreas universitarias.	Duración aproximada de ocho horas, divididas en 4 días diferentes de 2 horas.	Tiene como público objetivo a las personas que participan como responsables del tratamiento de datos personales dentro de la Oficina Jurídica de la Escuela Nacional de Ciencias Forenses.

	3. Derechos ARCOP, medios de impugnación y facultad de verificación. ◆ Derechos de acceso, rectificación, cancelación, oposición y portabilidad. ◆ Formas y Plazos señalados por la LGPDPPSO para el ejercicio de estos derechos. ◆ Recursos de revisión y de inconformidad y sus etapas de sustanciación. ◆ Facultades del INAI para verificar el cumplimiento de la LGPDPPSO. ◆ Medidas cautelares y de apremio para cumplir resoluciones de la LGPDPPSO. 4. Elaboración del Documento de Seguridad y Sistema de Gestión de Seguridad de Datos Personales 5. Incidentes y vulneraciones de seguridad de datos personales 6. Análisis de riesgo y análisis de brecha.		

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

Escuela Nacional de Ciencias Forenses			
Identificador único*	**ENACIF-Oficina Jurídica**		
(Nombre del sistema A1) *	**Orientación Jurídica**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Difusión de lo que son DATOS PERSONALES, conceptos básicos, objetivos, mecanismos y herramientas en materia de protección de datos personales.	Se difundirá material visual como carteles, infografías que permita lograr una mayor comprensión del tema y el desarrollo de mecanismos y habilidades para el fortalecimiento y el mejor tratamiento de datos personales en el manejo del Sistema, para ello, se apoyará en diversos medios físicos como pizarrones, correo electrónico, publicaciones en la página web de la Escuela Nacional de Ciencias Forenses, entre otros; donde se establecerán tanto la definición como los principios y objetivos, así como las herramientas en materia de protección de datos personales.	La difusión se realizará de manera semestral durante un periodo de 5 días laborables .	Tiene como público objetivo a las personas que participan como responsables del tratamiento de datos personales dentro de la Oficina Jurídica de la Escuela Nacional de Ciencias Forenses.
Difusión de actualización del Sistema.	Se difundirá material que apoye la actualización a los usuarios que operan el Sistema, a fin de que conozcan las políticas y mecanismos de seguridad en el tratamiento de datos personales que se vayan implementando en el Sistema, e invitará al personal involucrado en el tratamiento de datos personales a los cursos de capacitación que se efectúen según se programen por la Unidad de Transparencia.	La difusión se realizará de manera semestral durante un periodo de 5 días laborables .	Tiene como público objetivo a las personas que participan como responsables del tratamiento de datos personales dentro de la Oficina Jurídica de la Escuela Nacional de Ciencias Forenses.

9. MEJORA CONTINUA

9.1 ACTUALIZACIÓN Y MANTENIMIENTO DE **SISTEMAS DE INFORMACIÓN**

Escuela Nacional de Ciencias Forenses			
Identificador único	**ENACIF-Oficina Jurídica**		
(Nombre del sistema A1) *	**Orientación Jurídica**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Actualización a las plataformas web con la digitalización de los expedientes físicos que se encuentran en la Oficina Jurídica.	Con el objetivo principal de preservar la seguridad e integridad de los datos personales almacenados en formato electrónico, así como de hacer el sistema de Orientación Jurídica más robusto, se pretende llevar a cabo la actualización de las plataformas disponibles: En la nube del servidor interno de la ENaCiF, así como en la nube proporcionada por la Oficina de la Abogacía General de la UNAM, a través de la actualización de la digitalización total de los expedientes físicos.	Se programa un día laborable cada mes durante todo el año.	La totalidad de los expedientes jurídicos físicos disponibles hasta el momento de la actualización.
Mantenimiento	Se trabaja diariamente en la actualización de la base de datos electrónica y se procura mantener lo menos posible, versiones físicas de documentos para contribuir con la política de menos papel, y con ello reducir el consumo de papel en espacios como oficinas y escuelas por medio de una estrategia integral de digitalización y automatización de procesos que requiere una combinación de hardware y software eficiente	Actividad permanente .	El 100% de los equipos a disposición de la Oficina Jurídica.

9.2 ACTUALIZACIÓN Y MANTENIMIENTO DE **EQUIPO DE CÓMPUTO**

Escuela Nacional de Ciencias Forenses			
Identificador único*	**ENACIF-Oficina Jurídica**		
(Nombre del sistema A1) *	**Orientación Jurídica**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Actualización de software.	Con el objetivo principal de preservar la seguridad e integridad de los datos personales almacenados en formato electrónico, así como de hacer el sistema de Orientación Jurídica más robusto, se pretende llevar a cabo la actualización de las plataformas disponibles: En la nube del servidor interno de la ENaCiF, así como en la nube proporcionada por la Oficina de la Abogacía General de la UNAM, a través de la actualización de la digitalización total de los expedientes físicos.	Se programa un día laborable cada mes durante todo el año.	La totalidad de los expedientes jurídicos físicos disponibles hasta el momento de la actualización.
Mantenimiento	Los equipos están configurados para recibir automáticamente las actualizaciones de software y se instalan según las horas activas del equipo, el Departamento de Cómputo y Telecomunicaciones realiza búsquedas manuales y periódicas de dichas actualizaciones.	Actividad permanente.	El 100% de los equipos a disposición de la Oficina Jurídica.

9.3 Procesos para la conservación, preservación y respaldos de información

Escuela Nacional de Ciencias Forenses		
Identificador único*	**ENACIF-Oficina Jurídica**	
(Nombre del sistema A1) *	**Orientación Jurídica**	
Proceso*	**Descripción***	**Responsable***
Estrategia integral de digitalización para respaldo de bases de datos	Se refiere a una estrategia integral de digitalización y automatización de procesos que requiere una combinación de hardware y software eficiente: A través de un multifuncional BROTHER DCP-T720DW de uso exclusivo para la Oficina Jurídica, y el equipo de cómputo DELL con acceso biométrico se realiza el proceso de digitalización periódica de los datos personales del Sistema de Orientación Jurídica. Los documentos son resguardados y respaldados en las diferentes nubes disponibles exclusivamente para la Oficina Jurídica, una dentro del servidor local de la ENaCiF, y otra en el servidor específico de la Oficina de la Abogacía General de la UNAM.	Responsable de la Oficina Jurídica de la Escuela Nacional de Ciencias Forenses.

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

Escuela Nacional de Ciencias Forenses		
Identificador único*	**ENACIF-Oficina Jurídica**	
(Nombre del sistema A1) *	**Orientación Jurídica**	
Proceso*	**Descripción***	**Responsable***
No aplica	La Oficina Jurídica no se encarga directamente del procedimiento de borrado seguro ni de la disposición final de equipos y componentes informáticos.	No aplica.

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

Cuando la totalidad de los datos personales contenidos en un sistema de datos personales que obre en los archivos de la Escuela Nacional de Ciencias Forenses hayan dejado de ser necesarios para el cumplimiento de la finalidad o finalidades para las que se recolectaron, de conformidad con lo establecido en el Aviso de Privacidad respectivo o de acuerdo con las disposiciones legales aplicables, o bien exista un sistema que otorgue un mejor tratamiento, deberán ser cancelados previo bloqueo.

El procedimiento de cancelación iniciará con el sistema de tratamiento de datos personales el cual se realizará por un periodo determinado atendiendo al sistema que se trate, tal como se detalla en el inciso E) del presente apartado. Corresponde al responsable de cada sistema identificar si los mismos han dejado de ser útiles e iniciar el bloqueo correspondiente de los sistemas de datos personales a cancelar, previa notificación que se realice a la persona titular de la Escuela Nacional de Ciencias Forenses.

La notificación que realice el responsable del sistema a cancelar deberá contener lo siguiente:

I. El nombre del sistema de datos personales a cancelar.
II. La justificación de que no existe obligación legal de mantener por más tiempo el sistema de datos personales.
III. La justificación de que el sistema de datos personales ha dejado de ser útil.
IV. Las acciones encaminadas a recuperar, cuando sea posible, las copias o reproducciones de ese sistema de datos personales, entregados a los usuarios con el fin de evitar su tratamiento.
V. Señalar las medidas de seguridad a emplear, con el objetivo de impedir el tratamiento del sistema de datos personales durante el periodo de bloqueo.

El plazo para el bloqueo de los datos personales comienza a computarse a partir del día hábil siguiente de la notificación del responsable a las personas titulares de la Escuela Nacional de Ciencias Forenses, ya que, a partir de ese día, deberá impedirse cualquier tratamiento del sistema de datos personales a cancelar.

Los Sistemas de Datos Personales electrónicos almacenados en equipos de cómputo, deberán destruirse una vez concluido el periodo de bloqueo correspondiente en presencia del responsable, de la persona titular de la Escuela Nacional de Ciencias

Forenses, de un trabajador universitario adscrito al Departamento de Cómputo y Telecomunicaciones, el responsable de seguridad de datos personales de la Escuela Nacional de Ciencias Forenses y un funcionario adscrito a la Entidad que asista como testigo, para lo cual se deberá emitir una Acta Administrativa en donde se incluyan:

- El número de reproducciones que se tengan del sistema de datos personales;
- La especificación del tipo de base de datos (física o electrónica);
- La descripción del método de destrucción;
- El día y a hora de la destrucción, y
- La firma de los presentes.

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

a) **Denominación:** Sistema de Orientación Jurídica.

b) **Motivo de la cancelación:** Cuando los datos personales contenidos en los sistemas hayan dejado de ser necesarios apra cumplir la finalidad para la que se recolectaron, exista un sistema que otorgue un mejor tratamiento según las disposiciones legales aplicables.

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

A1

Por lo que hace al Sistema de Orientación Jurídica, el periodo de bloqueo será de uno a quince años de acuerdo con los plazos institucionales de conservación en materia archivística, lo anterior debido a que los documentos que se producen:

- Son de apoyo informativo, que no se relacionan con el asunto de un expediente, carecen de valores documentales y únicamente responden a actividades asignadas al área productora (1-5 años)
- Son obligaciones de transparencia y acceso a la información pública y protección de datos personales (2-15 años)
- Asuntos Jurídicos (1-5 años)
- Asuntos de legislación universitaria, creación de instrumentos consensuales como convenios, contratos y bases de colaboración por todo el tiempo de su vigencia. (1-5 años)

Para llevar a cabo el bloqueo del Sistema, se deberán realizar las siguientes acciones:

1. Informar a los usuarios que el Sistema está bloqueado y poner aviso del tratamiento de datos que se hará cuando el sistema se retire.

2. Deshabilitar el ingreso de los usuarios al Sistema.
3. Durante el bloqueo, solamente el jefe del Departamento de Cómputo y Telecomunicaciones podrá tener acceso al Sistema, en caso de que se requiera alguna información.
4. Al término del periodo de bloqueo se deberán desactivar los últimos accesos al sistema.

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

En relación con el Sistema de información con identificador único A1 le es aplicable las medidas de seguridad y procedimiento para la supresión que a continuación se describen.

Una vez que comience el periodo de bloqueo, se pondrá fuera de línea el servidor y será resguardado físicamente por el Departamento de Cómputo y Telecomunicaciones, para tener acceso únicamente de forma local por el responsable técnico del sistema en caso de requerir información.

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

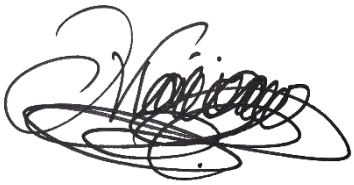
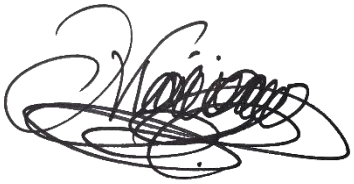
1. Se retirará el disco duro del servidor que alberga el sistema de tratamiento de los datos personales a suprimir.

2. Se elimina la información contenida en el disco duro atendiendo las recomendaciones para el borrado seguro de la información publicadas por la Dirección General de Cómputo y de Tecnologías de la Información (DGTIC) a través de la guía con el mismo nombre disponible en su sitio web.

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

En lo que respecta al Sistema de información con identificador único A1, por lo que hace a su versión electrónica alojado en disco duro, basta con la supresión a nivel de software. Y por lo que hace al sistema en soporte físico, el mecanismo de supresión corresponderá al procedimiento señalado al principio de este capítulo 10.

11. APROBACIÓN DEL DOCUMENTO DE SEGURIDAD

Responsable del Desarrollo	Mtra. Mónica Guadalupe Ramírez Monares Jefa de Oficina Jurídica de la Escuela Nacional de Ciencias Forenses Correo electrónico: oficinajuridica@enacif.unam.mx Teléfono: 55 56232300 ext. 81908	
Revisó	Mtra. Mónica Guadalupe Ramírez Monares Jefa de Oficina Jurídica de la Escuela Nacional de Ciencias Forenses Correo electrónico: oficinajuridica@enacif.unam.mx Teléfono: 55 56232300 ext. 81908	
Autorizó	Dra. Zoraida García Castillo Directora de la Escuela Nacional de Ciencias Forenses Correo electrónico: zoraidagc@unam.mx Teléfono: 55 56232300 ext. 24210	
Fecha de Aprobación por el Comité de Transparencia		

ANEXO

Resolución del Comité de Transparencia UNAM