UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO
INSTITUTO DE NEUROBIOLOGÍA

Responsable institucional:
Dirección del Instituto de Neurobiología

Sistema de Gestión de Seguridad de Datos Personales (SGSDP)

Coordinación:
Responsable de Seguridad de Datos Personales
Instituto de Neurobiología, UNAM

VERSIÓN PÚBLICA

Clasificación:
Documento con información parcialmente reservada, conforme a la resolución CTUNAM/476/2026.

Fecha del documento original: 6 de octubre de 2026
Preparación: Segunda revisión de la versión pública

Referencia: Oficio INEU/D/598/2026, recibido el 25 de septiembre de 2026.

Contenido

I. Introducción. 3

II. Objetivo. 4

III. Términos y definiciones. 6

IV. Principios 9

V. Alcance. 12

VI. Funciones y responsabilidades. 15

VII. Sistema de Gestión de Seguridad de Datos Personales (SGSDP). 19

VIII. Políticas del SGSDP. 25

IX. Inventario de Sistemas de Tratamiento de Datos Personales 32

X. Análisis de Riesgo 36

XI. Análisis de Brecha. 42

XII. Plan de trabajo. 48

Leyenda reservada. 51

Leyenda reservada. 52

Leyenda reservada. 52

XIII. Capacitación. 54

XIV. Anexos. 59

XV. Avisos Privacidad INB UNAM 2026. 63

XVI. Formatos base alineados con el Documento de Seguridad de Datos Personales del INB y con enfoque institucional UNAM. 68

XVII. Hoja de autorización de firmas ……73

I. Introducción.

El presente Documento de Seguridad de Datos Personales del Instituto se elabora en cumplimiento del *"Acuerdo por el que se Establecen los Lineamientos para la Protección de Datos Personales en Posesión de la Universidad Nacional Autónoma de México"*, publicado en Gaceta UNAM el 25 de febrero de 2019; de las *"Normas Complementarias sobre Medidas de Seguridad Técnicas, Administrativas y Físicas para la Protección de Datos Personales en Posesión de la Universidad"*, publicadas en Gaceta UNAM el 30 de enero de 2020; así como de la *Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados* y demás disposiciones aplicables en materia de transparencia, acceso a la información pública, gestión documental, seguridad de la información y protección de datos personales.

El Instituto, como entidad académica de la Universidad Nacional Autónoma de México dedicada a la investigación científica, docencia, formación de recursos humanos especializados y prestación de servicios científicos y tecnológicos, reconoce la importancia institucional, jurídica y ética de garantizar la protección de los datos personales que obran en sus archivos, expedientes, sistemas institucionales, plataformas electrónicas y bases de datos, tanto en soportes físicos como electrónicos.

En el ejercicio de sus funciones sustantivas y administrativas, el INB realiza el tratamiento de datos personales y, en determinados casos, de datos personales sensibles, particularmente aquellos relacionados con información académica, laboral, patrimonial, biométrica, clínica y de salud, incluyendo información derivada de proyectos de investigación, actividades de enseñanza y posgrado, gestión administrativa, recursos humanos, servicios de resonancia magnética, neurodesarrollo, atención especializada y demás actividades institucionales. Asimismo, el Instituto reconoce que determinados sistemas institucionales pueden involucrar el tratamiento de datos personales de niñas, niños y adolescentes, así como información clínica y científica que requiere medidas reforzadas de seguridad, confidencialidad y control.

El presente documento tiene como finalidad describir y documentar el SGSDP implementado en el Instituto, estableciendo las medidas de seguridad administrativas, físicas y técnicas orientadas a garantizar la confidencialidad, integridad, disponibilidad y trazabilidad de los datos personales en posesión del Instituto, así como prevenir su daño, pérdida, alteración, destrucción, uso, acceso o tratamiento no autorizado.

De igual manera, el documento establece las funciones, responsabilidades, mecanismos de control, criterios de gestión de riesgos, análisis de brecha, programas de capacitación y acciones de mejora continua aplicables a las áreas académicas, administrativas, técnicas y de servicio del Instituto que intervienen en el tratamiento de datos personales, atendiendo al ciclo de vida de la información, desde su obtención, registro y almacenamiento, hasta su transferencia, conservación, bloqueo, supresión o destrucción conforme a la normatividad universitaria y archivística aplicable.

El SGSDP del INB adopta un enfoque preventivo y basado en riesgos, considerando la naturaleza de los datos tratados, el volumen de titulares, los medios de almacenamiento,

el nivel de exposición tecnológica, las posibles vulneraciones de seguridad y las consecuencias que éstas podrían representar para los titulares de los datos personales y para la Institución.

Asimismo, el Instituto impulsa una cultura institucional de protección de datos personales y seguridad de la información, promoviendo entre su comunidad universitaria el uso responsable, ético y legítimo de la información personal mediante acciones permanentes de sensibilización, capacitación, supervisión y mejora continua, por lo que el presente Documento de Seguridad constituye un instrumento institucional dinámico y sujeto a actualización permanente conforme a cambios normativos, tecnológicos, organizacionales, operativos o de riesgos identificados, con el propósito de fortalecer continuamente las capacidades institucionales del Instituto en materia de protección de datos personales y seguridad de la información, en concordancia con los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad establecidos en la normatividad aplicable.

II. Objetivo.

El presente Documento de Seguridad de Datos Personales tiene por objeto establecer, documentar y mantener el SGSDP del Instituto, así como definir las medidas de seguridad administrativas, físicas y técnicas aplicables al tratamiento de datos personales y datos personales sensibles que se encuentren en posesión del Instituto, con la finalidad de garantizar su confidencialidad, integridad, disponibilidad y trazabilidad, conforme a la normatividad universitaria y nacional aplicable.

De manera específica, el presente documento tiene los siguientes objetivos:

1. Garantizar la protección de los datos personales

Establecer mecanismos institucionales que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción, acceso, uso, divulgación o tratamiento no autorizado, durante todo su ciclo de vida, desde su obtención hasta su bloqueo, conservación, transferencia, supresión o destrucción definitiva.

2. Dar cumplimiento a la normatividad aplicable

Asegurar el cumplimiento de:

- La Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados;
- Los Lineamientos para la Protección de Datos Personales en Posesión de la Universidad Nacional Autónoma de México;
- Las Normas Complementarias sobre Medidas de Seguridad Técnicas, Administrativas y Físicas para la Protección de Datos Personales en Posesión de la Universidad;
- La normatividad universitaria, archivística, administrativa y de transparencia aplicable.

3. Establecer responsabilidades institucionales

Definir las funciones, obligaciones y responsabilidades de las personas servidoras universitarias, áreas académicas, administrativas, técnicas y de servicio que intervienen en el tratamiento de datos personales, así como de las personas responsables de seguridad, encargadas y usuarias de los sistemas de tratamiento.

4. Implementar medidas de seguridad

Determinar e implementar medidas de seguridad administrativas, físicas y técnicas orientadas a:

- Controlar el acceso a los datos personales;
- Reducir riesgos de vulneración;
- Fortalecer la seguridad de la información;
- Garantizar la continuidad operativa de los sistemas institucionales;
- Prevenir incidentes de seguridad y accesos no autorizados.

5. Identificar y gestionar riesgos

Implementar mecanismos de identificación, evaluación, análisis y tratamiento de riesgos asociados al manejo de datos personales, particularmente aquellos relacionados con:

- Datos personales sensibles;
- Información clínica y biomédica;
- Datos de niñas, niños y adolescentes;
- Sistemas institucionales electrónicos;
- Transferencias nacionales e internacionales y almacenamiento digital de información.

6. Fortalecer la seguridad de los sistemas institucionales

Promover el uso seguro de los sistemas institucionales, plataformas electrónicas, bases de datos, expedientes físicos, redes de datos y medios de almacenamiento utilizados por el Instituto, asegurando el uso legítimo y controlado de la información personal.

7. Fortalecer la mejora continua y consolidar el Sistema de Gestión de Seguridad de Datos Personales

- Promover una cultura institucional de responsabilidad, confidencialidad, legalidad y ética en el tratamiento de datos personales;
- Fortalecer la protección de los derechos de las personas titulares de la información;
- Implementar acciones permanentes de capacitación, sensibilización, monitoreo y supervisión institucional;
- Mantener procesos de actualización documental y revisión periódica de controles de seguridad;

- Establecer mecanismos para la atención, documentación y seguimiento de vulneraciones e incidentes de seguridad;
- Consolidar un modelo institucional de gestión basado en riesgos;
- Mantener actualizado el inventario de sistemas de tratamiento de datos personales;
- Implementar y fortalecer medidas de seguridad administrativas, físicas y técnicas;
- Ejecutar análisis de riesgo y análisis de brecha;
- Elaborar y dar seguimiento a planes de trabajo y acciones de mejora continua;
- Fortalecer continuamente el cumplimiento normativo y las capacidades institucionales del Instituto en materia de protección de datos personales y seguridad de la información.

8. Atender el tratamiento especializado de datos sensibles

Establecer medidas reforzadas para los sistemas institucionales que involucren:

- Datos personales sensibles;
- Información médica y biomédica;
- Neuroimagen;
- Neurodesarrollo;
- Investigación con sujetos humanos;
- Expedientes académicos y laborales;
- Información de menores de edad.

III. Términos y definiciones.

Para efectos del presente Documento de Seguridad de Datos Personales y de conformidad con la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, los Lineamientos para la Protección de Datos Personales en Posesión de la Universidad Nacional Autónoma de México y las Normas Complementarias aplicables, se entenderá por:

Anonimización: Proceso mediante el cual los datos personales son transformados de manera irreversible para impedir la identificación de la persona titular.

Activo: Todo elemento de valor para el Instituto involucrado en el tratamiento de datos personales, incluyendo bases de datos, expedientes, sistemas informáticos, infraestructura tecnológica, redes, servidores, software, equipos de cómputo, documentación física, conocimiento institucional y personal universitario.

Área Universitaria: Las áreas académicas, administrativas, técnicas y de servicio del Instituto que manejan, resguardan o realizan tratamiento de datos personales en el ejercicio de sus funciones institucionales.

Aviso de Privacidad: Documento físico, electrónico o digital puesto a disposición de las personas titulares de los datos personales, mediante el cual se informa sobre las

finalidades, fundamentos, transferencias, mecanismos de protección y derechos relacionados con el tratamiento de sus datos personales.

Bases de Datos: Conjunto organizado de datos personales, estructurados y almacenados en medios físicos, electrónicos o digitales, que permiten su consulta, acceso, utilización, organización y tratamiento.

Bitácora de Seguridad: Registro documental o electrónico mediante el cual se documentan accesos, incidentes, vulneraciones, modificaciones, transferencias, respaldos o cualquier actividad relevante relacionada con los sistemas de tratamiento de datos personales.

Borrado Seguro: Procedimiento técnico o administrativo mediante el cual los datos personales son eliminados de manera definitiva e irrecuperable de medios físicos o electrónicos, conforme a las medidas de seguridad institucionales y archivísticas aplicables.

Confidencialidad: Principio de seguridad de la información que garantiza que los datos personales únicamente sean accesibles para personas autorizadas y en el ámbito de sus funciones institucionales.

Consentimiento*:* Manifestación libre, específica, informada e inequívoca de voluntad de la persona titular, mediante la cual autoriza el tratamiento de sus datos personales para finalidades determinadas.

Datos Personales: Cualquier información concerniente a una persona física identificada o identificable, directa o indirectamente, incluyendo información académica, administrativa, laboral, biométrica, clínica, patrimonial o de contacto.

Datos Personales Sensibles: Aquellos datos personales que se refieren a la esfera más íntima de la persona titular o cuya utilización indebida pueda generar discriminación o un riesgo grave, incluyendo información relacionada con:

- Estado de salud;
- Información genética;
- Origen étnico o racial;
- Datos biométricos;
- Creencias religiosas;
- Opiniones políticas;
- Preferencia sexual;
- Información médica y clínica;
- Datos biomédicos;
- Datos de niñas, niños y adolescentes.

Derechos ARCO: Derechos de Acceso, Rectificación, Cancelación y Oposición que tienen las personas titulares respecto del tratamiento de sus datos personales.

Documento de Seguridad: Instrumento institucional que describe las medidas de seguridad administrativas, físicas y técnicas implementadas por el Instituto para garantizar la protección de los datos personales en su posesión.

Encargado: Persona física o moral, distinta del responsable, que realiza el tratamiento de datos personales a nombre del Instituto, conforme a las instrucciones autorizadas y mediante los instrumentos jurídicos correspondientes.

Evaluación de Impacto en Protección de Datos Personales (EIDP): Análisis técnico y normativo que permite identificar, evaluar y mitigar riesgos derivados del tratamiento intensivo o relevante de datos personales, particularmente cuando se involucran datos sensibles o sistemas tecnológicos especializados.

Integridad: Principio de seguridad de la información que garantiza que los datos personales permanezcan exactos, completos y sin alteraciones no autorizadas.

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

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

Medidas de Seguridad Administrativas: Conjunto de políticas, procedimientos, lineamientos, controles, programas de capacitación y mecanismos organizacionales orientados a proteger los datos personales y regular su tratamiento institucional.

Medidas de Seguridad Físicas: Conjunto de acciones y mecanismos destinados a proteger físicamente las instalaciones, archivos, expedientes, equipos y áreas donde se resguardan datos personales.

Medidas de Seguridad Técnicas: Conjunto de mecanismos tecnológicos aplicados a sistemas informáticos, redes, servidores, equipos y bases de datos para prevenir accesos no autorizados, pérdida de información o vulneraciones de seguridad.

Persona Titular: Persona física a quien corresponden los datos personales objeto de tratamiento.

Responsable: Instancia, área universitaria o autoridad del Instituto que decide sobre el tratamiento, uso, resguardo y protección de los datos personales.

Responsable de Seguridad de Datos Personales: Persona designada por el Instituto encargada de coordinar, supervisar y verificar la implementación y cumplimiento de las medidas de seguridad aplicables al tratamiento de datos personales.

Riesgo: Probabilidad de que ocurra una vulneración de seguridad que afecte la confidencialidad, integridad o disponibilidad de los datos personales.

Seudonimización: Tratamiento de datos personales mediante el cual la información deja de atribuirse directamente a una persona titular sin utilizar información adicional separada y protegida.

Sistema de Gestión de Seguridad de Datos Personales (SGSDP): Conjunto de elementos, políticas, procesos, procedimientos, controles y actividades interrelacionadas orientadas a proteger los datos personales en posesión del Instituto.

Sistemas de Tratamiento: Conjunto de procedimientos, aplicaciones, plataformas, archivos, bases de datos o mecanismos físicos y electrónicos utilizados para obtener, registrar, almacenar, utilizar, transferir, conservar o eliminar datos personales.

Soporte Electrónico: Medio digital o tecnológico utilizado para almacenar, procesar o transmitir datos personales, incluyendo servidores, computadoras, sistemas institucionales, discos duros, servicios de nube y redes de datos.

Soporte Físico: Documentos, expedientes, archivos impresos, formularios, carpetas y demás medios materiales que contienen datos personales.

Supresión: Proceso mediante el cual los datos personales son eliminados o destruidos conforme a la normatividad archivística y de protección de datos aplicable.

Transferencia: Toda comunicación de datos personales realizada a persona física o moral distinta del titular, responsable o encargado, ya sea dentro o fuera del territorio nacional.

Tratamiento: Cualquier operación o conjunto de operaciones aplicadas a datos personales, ya sea mediante procedimientos físicos, manuales, automatizados o electrónicos, relacionadas con su obtención, uso, registro, organización, almacenamiento, consulta, transferencia, conservación, bloqueo, supresión o destrucción.

Usuario: Persona servidora universitaria, personal académico, técnico, administrativo o autorizado que accede a sistemas o información que contiene datos personales en el ejercicio de sus funciones institucionales.

Vulneración de Seguridad: Cualquier incidente que implique daño, pérdida, alteración, destrucción, acceso, divulgación, copia, robo, uso o tratamiento no autorizado de datos personales.

IV. Principios.

El Instituto, en el tratamiento de los datos personales que obran en sus archivos, expedientes, sistemas institucionales, plataformas electrónicas, bases de datos y demás medios físicos o digitales, observará en todo momento los principios establecidos en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, los

Lineamientos para la Protección de Datos Personales en Posesión de la Universidad Nacional Autónoma de México y demás normatividad aplicable.

Las áreas académicas, administrativas, técnicas y de servicio del Instituto deberán garantizar que todo tratamiento de datos personales se realice conforme a los siguientes principios:

1. Principio de Licitud. El tratamiento de datos personales deberá realizarse con estricto apego a las atribuciones, funciones y competencias conferidas al Instituto por la legislación universitaria y la normatividad aplicable.

Los datos personales deberán obtenerse y utilizarse mediante medios legales, legítimos y autorizados, evitando cualquier práctica contraria a las disposiciones jurídicas aplicables en materia de protección de datos personales, transparencia, seguridad de la información y gestión documental.

2. Principio de Finalidad. Todo tratamiento de datos personales deberá encontrarse plenamente justificado por finalidades concretas, lícitas, explícitas, legítimas e institucionalmente válidas, relacionadas con las funciones sustantivas y administrativas del Instituto.

Los datos personales únicamente podrán utilizarse para los fines específicos para los cuales fueron recabados y conforme a lo señalado en los avisos de privacidad correspondientes.

3. Principio de Lealtad. El Instituto se abstendrá de obtener o tratar datos personales mediante mecanismos engañosos, fraudulentos o contrarios a la buena fe, privilegiando en todo momento la protección de los intereses y derechos de las personas titulares, así como su expectativa razonable de privacidad.

4. Principio de Consentimiento. El tratamiento de datos personales requerirá el consentimiento previo de la persona titular cuando así lo determine la normatividad aplicable y no se actualice alguna causal de excepción prevista por la Ley.

El consentimiento deberá otorgarse de manera:

- Libre;
- Específica;
- Informada;
- Inequívoca.

Cuando resulte aplicable, el Instituto deberá obtener el consentimiento expreso y por escrito de la persona titular, salvo en los supuestos previstos en la legislación aplicable.

En el caso de niñas, niños y adolescentes, así como de personas sujetas a representación legal, el tratamiento de datos personales deberá atender las disposiciones jurídicas correspondientes y privilegiar el interés superior de la persona menor de edad.

5. Principio de Calidad. El Instituto adoptará las medidas necesarias para garantizar que los datos personales sean:

- Exactos;
- Completos;
- Correctos;
- Actualizados;
- Pertinentes.

Asimismo, se implementarán mecanismos institucionales para evitar la alteración, pérdida o utilización incorrecta de la información personal.

Los datos personales deberán dejar de tratarse cuando hayan concluido las finalidades que justificaron su obtención, debiendo observarse los plazos de conservación archivística y los procedimientos de bloqueo, supresión o destrucción establecidos por la normatividad aplicable.

6. Principio de Proporcionalidad. El Instituto únicamente tratará los datos personales que resulten adecuados, relevantes y estrictamente necesarios para cumplir con las finalidades institucionales que motivan su obtención y tratamiento.

Se evitará la recopilación excesiva o innecesaria de información personal que no guarde relación directa con los fines institucionales correspondientes.

7. Principio de Información. El Instituto pondrá a disposición de las personas titulares los avisos de privacidad simplificados e integrales correspondientes, mediante medios físicos, electrónicos o digitales accesibles.

Los avisos de privacidad deberán informar de manera clara, sencilla y transparente:

- La identidad del responsable;
- Las finalidades del tratamiento;
- Los datos personales recabados;
- Las transferencias de información;
- Los mecanismos para ejercer derechos ARCO;
- Los medios de contacto institucional.

8. Principio de Responsabilidad. El Instituto implementará y mantendrá medidas de seguridad administrativas, físicas y técnicas orientadas a garantizar la protección de los datos personales bajo su custodia.

Asimismo, las áreas responsables deberán:

- Adoptar mecanismos de control y supervisión;
- Capacitar al personal;
- Implementar acciones preventivas y correctivas;
- Gestionar riesgos;
- Documentar vulneraciones;

- Actualizar permanentemente el SGSDP.

La obligación de confidencialidad respecto de los datos personales subsistirá aun después de finalizar la relación laboral, académica, contractual o administrativa con el Instituto.

9. Principio de Confidencialidad. Todas las personas servidoras universitarias, personal académico, técnico, administrativo, prestadores de servicios y personas autorizadas que intervengan en el tratamiento de datos personales deberán guardar estricta confidencialidad respecto de la información a la que tengan acceso.

El acceso a los datos personales deberá limitarse únicamente al personal autorizado y conforme a las funciones institucionales que le hayan sido asignadas.

10. Principio de Seguridad. El Instituto implementará controles y mecanismos de seguridad administrativos, físicos y técnicos para proteger los datos personales contra:

- Daño;
- Pérdida;
- Alteración;
- Destrucción;
- Uso indebido;
- Acceso no autorizado;
- Divulgación no autorizada;
- Vulneraciones de seguridad.

Las medidas de seguridad deberán atender al nivel de riesgo, sensibilidad de los datos tratados, volumen de información, medios tecnológicos utilizados y posibles consecuencias para las personas titulares.

V. Alcance.

El presente Documento de Seguridad de Datos Personales es de observancia obligatoria para todas las áreas académicas, administrativas, técnicas y de servicio del Instituto que en el ejercicio de sus funciones realicen el tratamiento de datos personales y datos personales sensibles, ya sea en medios físicos, electrónicos, digitales o mediante redes de datos.

El alcance del presente documento comprende todas las actividades relacionadas con la obtención, uso, registro, organización, conservación, almacenamiento, consulta, acceso, manejo, aprovechamiento, transferencia, difusión, bloqueo, supresión o destrucción de datos personales que se encuentren bajo resguardo del Instituto, independientemente del formato, soporte o sistema institucional en el que se encuentren contenidos.

Asimismo, el presente documento aplica a:

- Personas servidoras universitarias;
- Personal académico;
- Personal administrativo;
- Personal técnico;
- Prestadores de servicios;
- Becarios;
- Estudiantes;
- Personas usuarias autorizadas;
- Encargados externos;
- Cualquier persona física o moral que intervenga en el tratamiento de datos personales a nombre del Instituto.

El alcance incluye los sistemas institucionales de tratamiento de datos personales actualmente identificados, así como aquellos que se incorporen posteriormente derivado de nuevas actividades académicas, administrativas, científicas, tecnológicas o de prestación de servicios especializados.

De manera enunciativa más no limitativa, el presente Documento de Seguridad aplica a las siguientes áreas y unidades institucionales:

Áreas Administrativas:

- Dirección;
- Secretaría Administrativa;
- Secretaría Académica;
- Secretaría Técnica;
- Área de Personal;
- Área de Presupuesto y Contabilidad;
- Área de Compras y Proveeduría;
- Unidad de Transparencia y Enlace de Transparencia;
- Archivo Institucional;
- Protección Civil y Seguridad;
- Servicios Generales;
- Tecnologías de la Información y Área de Cómputo.

Áreas Académicas y de Investigación

- Personal académico;
- Laboratorios de investigación;
- Proyectos de investigación científica;
- Proyectos con sujetos humanos;
- Proyectos con colaboración nacional e internacional;
- Consejo Interno;
- Comisiones evaluadoras y dictaminadoras;
- Unidad de Enseñanza y Posgrado;
- Programas de tutoría y formación académica.

Áreas Especializadas

- Unidad de Resonancia Magnética (URM);
- Unidad de Investigación en Neurodesarrollo (UIND);
- Sistemas de información radiológica (RIS);
- Sistemas relacionados con neuroimagen, neurodesarrollo y atención especializada;
- Sistemas clínicos, biomédicos y de investigación científica.

Sistemas Institucionales

El presente Documento de Seguridad comprende todos los sistemas físicos, electrónicos y digitales utilizados por el Instituto para el tratamiento de datos personales, incluyendo expedientes físicos, bases de datos, plataformas institucionales, sistemas en red, servicios institucionales de nube, servidores, dispositivos de almacenamiento, correo electrónico institucional y demás medios tecnológicos empleados para el registro, organización, consulta, uso, almacenamiento, transferencia, conservación y protección de la información personal.

El alcance del SGSDP comprende todo el ciclo de vida de los datos personales, desde:

- Su obtención y registro;
- Su almacenamiento y organización;
- Su utilización y consulta;
- Su transferencia o comunicación;
- Su conservación y respaldo;
- Su bloqueo, supresión o destrucción.

Asimismo, el presente Documento de Seguridad será aplicable a cualquier nuevo sistema, plataforma tecnológica, procedimiento institucional, proyecto de investigación o servicio especializado que implique tratamiento intensivo o relevante de datos personales, particularmente cuando involucre:

- Datos sensibles;
- Información clínica;
- Menores de edad;
- Transferencias nacionales o internacionales;
- Servicios tecnológicos especializados;
- Plataformas digitales o almacenamiento en nube.

Todas las áreas del Instituto deberán implementar y mantener las medidas de seguridad administrativas, físicas y técnicas que resulten necesarias para garantizar la protección de los datos personales bajo su responsabilidad, conforme al nivel de riesgo identificado y a la normatividad aplicable.

VI. Funciones y responsabilidades

El Instituto establecerá y mantendrá una estructura organizacional orientada a garantizar el adecuado cumplimiento del SGSDP, definiendo claramente las funciones, obligaciones, niveles de responsabilidad y mecanismos de coordinación de las personas servidoras universitarias, áreas institucionales y usuarios que intervienen en el tratamiento de datos personales.

Todas las personas que tengan acceso, intervención o participación en el tratamiento de datos personales deberán actuar conforme a los principios de legalidad, confidencialidad, responsabilidad, seguridad y protección de datos personales establecidos en la normatividad aplicable.

1. Responsable Institucional

Titular: Dirección del Instituto

Funciones y responsabilidades: La Dirección del Instituto será la autoridad responsable de supervisar el cumplimiento institucional del SGSDP y tendrá las siguientes atribuciones:

- Aprobar y promover la implementación del SGSDP;
- Impulsar el cumplimiento de la normatividad aplicable en materia de protección de datos personales;
- Designar a la persona Responsable de Seguridad de Datos Personales;
- Autorizar políticas, procedimientos y medidas institucionales de seguridad;
- Promover la asignación de recursos para fortalecer la seguridad de la información;
- Supervisar la atención de vulneraciones o incidentes de seguridad relevantes;
- Promover una cultura institucional de protección de datos personales;
- Coordinar acciones con la Unidad de Transparencia, DGTIC y autoridades universitarias competentes.

2. Responsable de Seguridad de Datos Personales

Titular: Persona designada por la Dirección del Instituto.

Funciones y responsabilidades: La persona Responsable de Seguridad de Datos Personales será la encargada de coordinar técnicamente el SGSDP y tendrá las siguientes funciones:

- Coordinar la implementación y actualización del presente Documento de Seguridad;
- Supervisar el cumplimiento de los Lineamientos y Normas Complementarias aplicables;
- Mantener actualizado el inventario de sistemas de tratamiento de datos personales;
- Coordinar el análisis de riesgo y análisis de brecha;

- Dar seguimiento a los planes de trabajo y acciones correctivas;
- Promover medidas de seguridad administrativas, físicas y técnicas;
- Coordinar programas de capacitación y sensibilización;
- Supervisar la documentación de incidentes y vulneraciones;
- Coordinar acciones preventivas y correctivas;
- Fungir como enlace técnico institucional en materia de protección de datos personales;
- Promover auditorías y revisiones internas de seguridad;
- Coordinar la actualización periódica del SGSDP.

3. Enlace de Transparencia

Titular o área designada como Enlace de Transparencia del Instituto o Campus: Oficina Jurídica del Campus.

Funciones y responsabilidades:

- Atender solicitudes relacionadas con derechos ARCO;
- Coordinar acciones con la Unidad de Transparencia de la UNAM;
- Orientar a las áreas institucionales sobre obligaciones de transparencia y protección de datos personales;
- Dar seguimiento a requerimientos institucionales relacionados con protección de datos personales;
- Colaborar en la atención de incidentes y vulneraciones cuando corresponda;
- Apoyar en la actualización de avisos de privacidad.

4. Responsables de Área
Integrantes:

- Secretaría Administrativa;
- Secretaría Académica;
- Secretaría Técnica;
- Área de Personal;
- Área de Cómputo;
- Unidad de Enseñanza y Posgrado;
- Unidad de Resonancia Magnética (URM);
- Unidad de Investigación en Neurodesarrollo (UIND);
- Responsables de laboratorios;
- Responsables de proyectos institucionales;
- Responsables de sistemas especializados.

Funciones y responsabilidades: Las personas responsables de área deberán:

- Garantizar el adecuado tratamiento de los datos personales bajo su resguardo;
- Implementar las medidas de seguridad aplicables en sus áreas;
- Mantener actualizado el inventario de sistemas y tratamientos;
- Identificar riesgos y reportar vulneraciones de seguridad;

- Limitar el acceso únicamente a personal autorizado;
- Verificar el uso legítimo de la información personal;
- Garantizar la conservación adecuada de expedientes y bases de datos;
- Supervisar respaldos y mecanismos de protección;
- Coordinar la eliminación o supresión segura de información cuando corresponda;
- Promover el cumplimiento de los avisos de privacidad;
- Informar oportunamente incidentes o vulneraciones.

5. Área de Tecnologías de la Información / Cómputo

Funciones y responsabilidades: El área de Tecnologías de la Información será responsable de:

- Administrar la infraestructura tecnológica institucional relacionada con datos personales;
- Implementar controles de acceso lógico;
- Gestionar respaldos institucionales;
- Mantener actualizados los sistemas de seguridad informática;
- Supervisar servidores, redes y plataformas institucionales;
- Implementar medidas de protección contra malware y accesos no autorizados;
- Apoyar técnicamente en incidentes de seguridad;
- Mantener bitácoras técnicas y registros de acceso cuando corresponda;
- Coordinar acciones de recuperación ante fallas o contingencias;
- Apoyar en auditorías técnicas y revisiones de seguridad.

6. Usuarios Autorizados

Definición: Toda persona servidora universitaria, personal académico, administrativo, técnico, estudiante o prestador de servicios que tenga acceso autorizado a datos personales institucionales.

Obligaciones: Las personas usuarias autorizadas deberán:

- Utilizar los datos personales únicamente para fines institucionales autorizados;
- Guardar estricta confidencialidad respecto de la información a la que tengan acceso;
- Evitar la reproducción, divulgación o transferencia no autorizada de información;
- Proteger contraseñas, dispositivos y medios de acceso;
- Reportar incidentes o vulneraciones de seguridad;
- Cumplir las políticas institucionales de seguridad de la información;
- Participar en programas de capacitación y sensibilización;
- Evitar almacenar información institucional en medios personales no autorizados.

La obligación de confidencialidad subsistirá aun después de concluir la relación laboral, académica o contractual con el Instituto.

7. Encargados Externos

Definición: Personas físicas o morales externas al Instituto que realicen tratamiento de datos personales por cuenta del INB.

Obligaciones:

- Tratar los datos personales únicamente conforme a las instrucciones autorizadas por el Instituto;
- Implementar medidas de seguridad equivalentes a las institucionales;
- Garantizar confidencialidad y protección de la información;
- Abstenerse de transferir o utilizar la información para fines distintos;
- Permitir revisiones o auditorías cuando corresponda;
- Cumplir los instrumentos jurídicos suscritos con la Universidad.

8. Comité o Grupo de Coordinación Institucional (en su caso)

El Instituto podrá integrar un grupo de trabajo o coordinación institucional en materia de protección de datos personales y seguridad de la información, con funciones de:

- Seguimiento institucional;
- Evaluación de riesgos;
- Atención de incidentes;
- Mejora continua;
- Actualización normativa;
- Coordinación interáreas;
- Revisión de controles de seguridad.

9. Responsabilidad Institucional Compartida

La protección de los datos personales constituye una responsabilidad institucional compartida entre todas las áreas, personas servidoras universitarias y usuarios autorizados que intervengan en cualquier fase del tratamiento de la información.

Todas las personas involucradas deberán actuar bajo criterios de:

- Legalidad;
- Confidencialidad;
- Ética;
- Responsabilidad;
- Seguridad;
- Prevención;
- Protección de los derechos de las personas titulares.

El incumplimiento de las obligaciones establecidas en el presente Documento de Seguridad podrá dar lugar a responsabilidades administrativas, laborales, universitarias o legales conforme a la normatividad aplicable.

VII. Sistema de Gestión de Seguridad de Datos Personales (SGSDP).

El Instituto establece y mantiene un SGSDP como el conjunto integral de políticas, procedimientos, controles, mecanismos, actividades, recursos y acciones institucionales orientadas a garantizar la protección de los datos personales y datos personales sensibles que se encuentran bajo su posesión, tratamiento, administración o resguardo.

El SGSDP tiene como finalidad asegurar la confidencialidad, integridad, disponibilidad, trazabilidad y uso legítimo de la información personal tratada por el Instituto, así como prevenir vulneraciones, accesos no autorizados, pérdida, alteración, destrucción o divulgación indebida de los datos personales.

El SGSDP del Instituto se implementa en cumplimiento de:

- La Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados;
- Los Lineamientos para la Protección de Datos Personales en Posesión de la Universidad Nacional Autónoma de México;
- Las Normas Complementarias sobre Medidas de Seguridad Técnicas, Administrativas y Físicas para la Protección de Datos Personales en Posesión de la Universidad;
- La normatividad universitaria aplicable en materia de transparencia, seguridad de la información y gestión documental.

1. Objetivos del SGSDP

El SGSDP tiene los siguientes objetivos institucionales:

- Garantizar el tratamiento lícito, controlado y seguro de los datos personales;
- Implementar medidas de seguridad administrativas, físicas y técnicas;
- Reducir riesgos asociados al tratamiento de información personal;
- Fortalecer la seguridad de los sistemas institucionales;
- Proteger datos personales sensibles y de alto riesgo;
- Establecer mecanismos de control, monitoreo y mejora continua;
- Promover una cultura institucional de protección de datos personales;
- Garantizar el cumplimiento normativo aplicable.

2. Alcance del SGSDP: aplica a:

- Todas las áreas académicas, administrativas, técnicas y de servicio del Instituto;
- Todos los sistemas físicos y electrónicos de tratamiento de datos personales;
- Todo el personal autorizado que intervenga en el tratamiento de información personal;

- Todos los medios físicos, digitales y tecnológicos utilizados para el manejo de datos personales.

Incluye los sistemas físicos, electrónicos, digitales y tecnológicos utilizados para el tratamiento institucional de datos personales.

3. Enfoque basado en riesgos

El SGSDP adopta un enfoque preventivo y basado en riesgos, considerando:

- La naturaleza de los datos personales tratados;
- El volumen de titulares;
- La sensibilidad de la información;
- El nivel de exposición tecnológica;
- Los medios de almacenamiento;
- Las posibles consecuencias de una vulneración;
- El impacto institucional y para las personas titulares.

El Instituto dará prioridad reforzada a los sistemas que involucren:

- Datos de salud;
- Información biomédica;
- Neuroimagen;
- Datos clínicos;
- Datos de niñas, niños y adolescentes;
- Información sensible;
- Sistemas electrónicos de acceso múltiple;
- Transferencias de información.

4. Componentes del SGSDP

El SGSDP del Instituto se integra, de manera enunciativa más no limitativa, por los siguientes componentes:

a) Marco normativo institucional: Conjunto de leyes, lineamientos, normas, procedimientos y políticas aplicables al tratamiento de datos personales.

b) Inventario de sistemas de tratamiento: Identificación y documentación de los sistemas físicos y electrónicos que contienen datos personales.

c) Gestión de riesgos: Procesos institucionales para identificar, analizar, evaluar y mitigar riesgos asociados al tratamiento de datos personales.

d) Medidas de seguridad: Implementación de controles administrativos, físicos y técnicos orientados a proteger la información.

e) Gestión documental y archivística: Control de expedientes, conservación documental, clasificación, resguardo y eliminación segura de información.

f) Capacitación y sensibilización: Programas permanentes de formación institucional en materia de protección de datos personales y seguridad de la información.

g) Monitoreo y mejora continua: Procesos de revisión periódica, actualización documental y fortalecimiento de controles de seguridad.

h) Atención de vulneraciones e incidentes: Mecanismos institucionales para detectar, documentar, atender y corregir incidentes de seguridad relacionados con datos personales.

i) Clasificación de información: Mecanismos institucionales para clasificar información pública, confidencial, reservada o sensible conforme a la normatividad aplicable.

5. Medidas de Seguridad Implementadas

El SGSDP contempla medidas de seguridad clasificadas en:

a) Medidas Administrativas

- Políticas institucionales;
- Designación de responsables;
- Declaratorias de confidencialidad;
- Capacitación;
- Inventarios;
- Bitácoras;
- Procedimientos internos;
- Gestión documental;
- Clasificación de información.

b) Medidas Físicas

- Control de acceso a instalaciones;
- Resguardo de expedientes;
- Archiveros con seguridad;
- Protección de equipos;
- Control de áreas restringidas;
- Vigilancia física;
- Protección de soportes físicos.

c) Medidas Técnicas

- Control de acceso lógico;
- Contraseñas robustas;
- Respaldo de información;
- Administración de servidores;
- Seguridad de redes;
- Restricción de privilegios;
- Protección antivirus;
- Actualización de sistemas;

- Monitoreo de accesos;
- Protección de plataformas institucionales;
- Autenticación reforzada o multifactor cuando resulte aplicable;
- Cifrado de información y respaldos sensibles;
- Uso de VPN institucional para accesos remotos autorizados;
- Trazabilidad y registros de acceso a sistemas críticos.

6. Ciclo de vida de los datos personales

El SGSDP considera todo el ciclo de vida de los datos personales, incluyendo:

- Obtención;
- Registro;
- Organización;
- Uso;
- Consulta;
- Transferencia;
- Almacenamiento;
- Conservación;
- Respaldo;
- Bloqueo;
- Supresión;
- Destrucción segura.

Cada etapa deberá ejecutarse bajo medidas de seguridad proporcionales al nivel de riesgo identificado.

7. Gestión de incidentes y vulneraciones

El Instituto establecerá mecanismos institucionales para:

- Detectar incidentes de seguridad;
- Reportar vulneraciones;
- Contener riesgos;
- Mitigar afectaciones;
- Documentar incidentes;
- Implementar acciones correctivas;
- Fortalecer controles preventivos.

Cuando una vulneración represente riesgo significativo para las personas titulares, el Instituto actuará conforme a la normatividad aplicable y los mecanismos institucionales correspondientes.

8. Capacitación y cultura institucional

El Instituto promoverá una cultura institucional de protección de datos personales mediante:

- Pláticas informativas;
- Cursos de capacitación;
- Material de sensibilización;
- Difusión institucional;
- Actualización normativa;
- Fortalecimiento de buenas prácticas.

La capacitación deberá considerar distintos niveles de responsabilidad y acceso a información personal.

9. Monitoreo, revisión y mejora continua

El SGSDP será objeto de:

- Monitoreo periódico;
- Evaluación de riesgos;
- Revisión de controles;
- Actualización documental;
- Auditorías internas o externas;
- Análisis de vulneraciones;
- Acciones preventivas y correctivas.

El Documento de Seguridad deberá actualizarse cuando:

- Existan cambios normativos;
- Se incorporen nuevos sistemas;
- Se modifiquen procesos institucionales;
- Se detecten vulneraciones;
- Cambie el nivel de riesgo;
- Se implementen nuevas tecnologías.

10. Compromiso institucional

El Instituto reconoce que la protección de datos personales constituye una responsabilidad institucional permanente y transversal, por lo que mantendrá acciones continuas orientadas a fortalecer la seguridad de la información, el cumplimiento normativo y la protección de los derechos de las personas titulares de los datos personales.

11. Evaluación de Impacto en Protección de Datos Personales (EIDP)

El Instituto podrá realizar Evaluaciones de Impacto en Protección de Datos Personales (EIDP) respecto de aquellos sistemas, proyectos, plataformas, procedimientos o actividades institucionales que impliquen tratamiento intensivo o relevante de datos personales, particularmente cuando involucren datos personales sensibles, información clínica, biomédica, neuroimagen, datos de niñas, niños y adolescentes, investigación científica con sujetos humanos o transferencias nacionales e internacionales de información.

La EIDP tendrá como finalidad identificar, analizar y mitigar los riesgos potenciales asociados al tratamiento de datos personales, así como fortalecer las medidas de seguridad administrativas, físicas y técnicas aplicables a los sistemas institucionales de mayor nivel de exposición o sensibilidad.

El Instituto podrá considerar, entre otros, los siguientes criterios para determinar la necesidad de realizar una EIDP:

- Tratamiento de datos personales sensibles;
- Tratamiento masivo o intensivo de información;
- Uso de plataformas tecnológicas especializadas;
- Investigación científica con sujetos humanos;
- Transferencias nacionales o internacionales de información;
- Uso de servicios en nube o plataformas compartidas;
- Integración de bases de datos interinstitucionales;
- Tratamiento de información clínica, biomédica o neuropsicológica;
- Tratamiento de datos personales de niñas, niños y adolescentes;
- Implementación de nuevas tecnologías o sistemas institucionales.

De manera prioritaria, el Instituto reconoce que los siguientes sistemas institucionales podrían requerir Evaluaciones de Impacto específicas derivadas del nivel de riesgo asociado al tratamiento de datos personales:

- Sistema RIS de la Unidad de Resonancia Magnética (URM);
- Sistemas de investigación y neurodesarrollo de la UIND;
- Sistemas de investigación científica con sujetos humanos;
- Sistemas institucionales que involucren información clínica o biomédica;
- Plataformas digitales con acceso multiusuario o transferencia de información sensible.

La coordinación de las EIDP corresponderá a la persona Responsable de Seguridad de Datos Personales en colaboración con las áreas responsables de los sistemas institucionales, el Área de Tecnologías de la Información, el Enlace de Transparencia y, en su caso, las instancias universitarias competentes.

Las Evaluaciones de Impacto podrán actualizarse cuando:

- Se incorporen nuevos sistemas;
- Cambie la naturaleza del tratamiento;
- Existan modificaciones tecnológicas relevantes;
- Se identifiquen nuevos riesgos;
- Existan vulneraciones o incidentes de seguridad;
- Cambie la normatividad aplicable.

VIII. Políticas del SGSDP.

El Instituto establece las siguientes políticas institucionales en materia de protección de datos personales y seguridad de la información, las cuales serán de observancia obligatoria para todas las áreas académicas, administrativas, técnicas y de servicio, así como para cualquier persona usuaria autorizada que intervenga en el tratamiento de datos personales bajo responsabilidad del Instituto.

Las presentes políticas tienen como finalidad establecer criterios institucionales orientados a garantizar la confidencialidad, integridad, disponibilidad, trazabilidad y uso legítimo de los datos personales y datos personales sensibles que obran en posesión del Instituto.

A. Políticas Administrativas

1. Política de legalidad y cumplimiento normativo

Todo tratamiento de datos personales deberá realizarse conforme a:

- La Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados;
- Los Lineamientos para la Protección de Datos Personales en Posesión de la Universidad Nacional Autónoma de México;
- Las Normas Complementarias sobre Medidas de Seguridad Técnicas, Administrativas y Físicas;
- La normatividad universitaria aplicable;
- Los avisos de privacidad institucionales.

Ningún área o persona usuaria podrá realizar tratamientos de datos personales fuera de las finalidades institucionales autorizadas.

2. Política de confidencialidad

Toda persona que tenga acceso a datos personales deberá guardar estricta confidencialidad respecto de la información a la que tenga acceso con motivo de sus funciones, actividades académicas, administrativas, técnicas o de prestación de servicios.

La obligación de confidencialidad subsistirá aun después de concluir la relación laboral, académica, contractual o administrativa con el Instituto.

Queda prohibido:

- Divulgar información personal sin autorización;
- Compartir contraseñas;
- Reproducir información institucional sin justificación;
- Transferir datos personales mediante medios no autorizados.

3. Política de acceso autorizado

El acceso a datos personales estará limitado exclusivamente al personal autorizado y únicamente para el desempeño de funciones institucionales específicas.

El Instituto implementará mecanismos de control de acceso físico y lógico considerando:

- Perfiles de usuario;
- Niveles de privilegio;
- Necesidad operativa;
- Sensibilidad de la información.

Cada persona usuaria será responsable del uso adecuado de sus credenciales institucionales.

4. Política de protección de datos personales sensibles

Los sistemas institucionales que involucren tratamiento de datos personales sensibles deberán contar con medidas reforzadas de seguridad administrativas, físicas y técnicas.

Particularmente se considerarán de atención prioritaria:

- Datos clínicos;
- Información médica;
- Neuroimagen;
- Datos biomédicos;
- Datos de niñas, niños y adolescentes;
- Información derivada de investigaciones con sujetos humanos;
- Datos biométricos;
- Información socioeconómica sensible.

El tratamiento de datos sensibles requerirá consentimiento expreso cuando así lo determine la normatividad aplicable.

5. Política de minimización de datos

Las áreas institucionales únicamente deberán recabar los datos personales estrictamente necesarios para cumplir con las finalidades institucionales autorizadas.

Queda prohibida la recopilación excesiva, innecesaria o desproporcionada de información personal.

6. Política de avisos de privacidad

Toda área, sistema o procedimiento institucional que implique tratamiento de datos personales deberá contar con aviso de privacidad simplificado e integral conforme a la normatividad aplicable.

Los avisos de privacidad deberán:

- Mantenerse actualizados;
- Estar disponibles para las personas titulares;
- Ser claros y accesibles;
- Informar las finalidades y mecanismos de ejercicio de derechos ARCO.

B. Políticas de Seguridad Física

7. Política de seguridad física

El Instituto implementará medidas orientadas a proteger físicamente los espacios, expedientes, archivos, equipos y medios de almacenamiento que contengan datos personales.

Las áreas responsables deberán:

- Resguardar expedientes en espacios controlados;
- Limitar acceso a áreas restringidas;
- Proteger equipos institucionales;
- Mantener controles de acceso físico;
- Evitar exposición innecesaria de información.

8. Política de uso y resguardo documental

El Instituto de Neurobiología (INb), UNAM, implementará medidas administrativas, físicas y técnicas para garantizar el adecuado uso, organización, consulta, conservación, resguardo y disposición documental de los expedientes y archivos físicos o electrónicos que contengan datos personales o datos personales sensibles.

Las áreas responsables deberán asegurar que la documentación institucional sea utilizada exclusivamente para fines académicos, científicos, administrativos o técnicos autorizados, bajo criterios de confidencialidad, integridad y seguridad de la información.

Los expedientes físicos deberán mantenerse en áreas con acceso controlado y bajo resguardo del personal autorizado. Tratándose de expedientes electrónicos, se deberán implementar controles de acceso, protección de credenciales, respaldos y mecanismos razonables de seguridad para evitar accesos no autorizados, pérdida, alteración o divulgación indebida de información.

La consulta, reproducción, préstamo, transferencia, digitalización, conservación y destrucción documental deberá realizarse conforme a la normatividad universitaria, archivística y de protección de datos personales aplicable.

Cuando los expedientes contengan datos personales sensibles, información clínica, biomédica, neuroimagen o datos de menores de edad, las áreas responsables deberán aplicar medidas reforzadas de protección y acceso restringido.

C. Políticas de Seguridad Tecnológica

9. Política de seguridad tecnológica

El Instituto implementará controles tecnológicos orientados a prevenir accesos no autorizados, pérdida o alteración de información personal.

De manera enunciativa, se deberán considerar:

- Contraseñas robustas;
- Control de privilegios;
- Actualización de sistemas;
- Protección antivirus;
- Respaldo de información;
- Monitoreo de accesos;
- Protección de redes y servidores;
- Restricción de software no autorizado.

10. Política de uso de equipos y medios institucionales

Los equipos, sistemas, redes y dispositivos institucionales utilizados para tratamiento de datos personales deberán emplearse exclusivamente para fines institucionales autorizados.

Queda prohibido:

- Instalar software no autorizado;
- Compartir dispositivos institucionales sin control;
- Almacenar información institucional en medios personales no autorizados;
- Transferir información mediante plataformas no autorizadas.

11. Política de acceso remoto y teletrabajo

El acceso remoto a sistemas institucionales que contengan datos personales deberá realizarse únicamente mediante mecanismos autorizados por el Instituto y bajo controles de seguridad adecuados.

Las personas usuarias deberán:

- Utilizar equipos autorizados;
- Proteger credenciales;
- Evitar redes inseguras;

- Abstenerse de almacenar información institucional en dispositivos personales no autorizados.

12. Política de respaldo y recuperación de información

El Instituto implementará mecanismos periódicos de respaldo y recuperación de información institucional que contenga datos personales.

Los respaldos deberán:

- Mantenerse protegidos;
- Resguardarse en medios institucionales;
- Permitir la recuperación de información ante incidentes;
- Contar con controles de acceso y conservación.

D. Políticas sobre Transferencias y Tratamiento Especializado

13. Política de conservación, bloqueo y supresión

Los datos personales deberán conservarse únicamente durante el tiempo necesario para cumplir con las finalidades institucionales y obligaciones legales aplicables.

Una vez concluido el periodo de conservación:

- La información deberá bloquearse, suprimirse o destruirse;
- Se aplicarán mecanismos de borrado seguro;
- Se atenderá la normatividad archivística y universitaria aplicable.

14. Política de transferencias de datos personales

El Instituto podrá realizar transferencias de datos personales únicamente cuando exista fundamento jurídico, finalidad institucional legítima y medidas de seguridad adecuadas que garanticen la protección de la información personal conforme a la normatividad aplicable.

Las transferencias de datos personales deberán realizarse exclusivamente para el cumplimiento de funciones académicas, científicas, administrativas, tecnológicas, clínicas o de colaboración institucional relacionadas con las atribuciones del Instituto.

Las áreas responsables deberán garantizar que toda transferencia:

- Se encuentre debidamente justificada;
- Sea proporcional y necesaria;
- Se realice mediante mecanismos seguros;
- Observe los principios de confidencialidad y minimización de datos;
- Atienda los avisos de privacidad aplicables;
- Cuente con controles de acceso y trazabilidad.

El Instituto reconoce que determinadas actividades institucionales pueden implicar transferencias nacionales o internacionales de información derivadas de:

- Proyectos de investigación científica;
- Colaboraciones académicas;
- Investigación con sujetos humanos;
- Estudios multicéntricos;
- Convenios institucionales;
- Plataformas tecnológicas compartidas;
- Servicios institucionales en nube;
- Sistemas especializados de neuroimagen y biomédicos;
- Intercambio científico y académico.

Particularmente, el Instituto prestará atención reforzada a transferencias relacionadas con:

- Datos personales sensibles;
- Información clínica;
- Neuroimagen;
- Datos biomédicos;
- Información de niñas, niños y adolescentes;
- Bases de datos científicas;
- Información derivada de investigación con sujetos humanos.

Las transferencias deberán sujetarse a:

- Instrumentos jurídicos aplicables;
- Convenios institucionales;
- Acuerdos de confidencialidad;
- Protocolos autorizados;
- Consentimientos informados, cuando corresponda;
- Medidas de seguridad administrativas, físicas y técnicas.

El Instituto procurará implementar medidas orientadas a:

- Restringir accesos no autorizados;
- Reducir riesgos de exposición;
- Controlar privilegios de usuarios;
- Fortalecer la protección de plataformas digitales;
- Supervisar el uso de servicios en nube;
- Proteger la información compartida mediante mecanismos seguros de almacenamiento y transferencia.

Las áreas responsables deberán documentar las transferencias relevantes mediante mecanismos institucionales de control y trazabilidad, incluyendo:

- Área responsable;
- Destinatario;
- Finalidad;
- Tipo de datos transferidos;
- Base jurídica;
- Medio de transferencia;
- Medidas de seguridad aplicables.

15. Política de tratamiento de datos en investigación científica

El Instituto implementará medidas específicas para garantizar la protección de los datos personales tratados en actividades de investigación científica, particularmente cuando involucren información clínica, biomédica, neuroimagen, datos personales sensibles o información de niñas, niños y adolescentes.

Las áreas responsables deberán asegurar que el tratamiento de datos personales en proyectos de investigación se realice conforme a la normatividad aplicable, los protocolos autorizados, los principios éticos y los mecanismos institucionales de confidencialidad y seguridad de la información.

El Instituto promoverá, cuando resulte procedente, mecanismos de anonimización, disociación o seudonimización de datos personales, así como controles de acceso restringido y medidas de seguridad reforzadas para proyectos de investigación con sujetos humanos, colaboración científica o transferencias nacionales e internacionales de información.

E. Políticas de Gestión Institucional y Mejora Continua

16. Política de atención de vulneraciones e incidentes

Toda persona usuaria deberá reportar inmediatamente cualquier incidente, vulneración o riesgo relacionado con datos personales.

El Instituto implementará mecanismos para:

- Detectar incidentes;
- Contener riesgos;
- Mitigar afectaciones;
- Documentar vulneraciones;
- Implementar acciones correctivas y preventivas.

17. Política de capacitación y sensibilización

El Instituto promoverá programas permanentes de:

- Capacitación;
- Sensibilización;
- Actualización normativa;
- Formación en seguridad de la información;
- Buenas prácticas institucionales.

La capacitación será obligatoria para las personas usuarias con acceso a datos personales.

18. Política de mejora continua

El SGSDP será revisado y actualizado periódicamente considerando:

- Cambios normativos;
- Actualizaciones tecnológicas;
- Riesgos identificados;
- Vulneraciones;
- Auditorías;
- Nuevos sistemas institucionales;
- Requerimientos operativos.

19. Política de responsabilidad institucional

La protección de datos personales constituye una responsabilidad institucional compartida. Todas las áreas y personas usuarias deberán actuar bajo criterios de:

- Legalidad;
- Confidencialidad;
- Responsabilidad;
- Prevención;
- Ética;
- Seguridad de la información;
- Protección de derechos de las personas titulares.

El incumplimiento de las presentes políticas podrá dar lugar a responsabilidades administrativas, universitarias, laborales o legales conforme a la normatividad aplicable.

IX. Inventario de Sistemas de Tratamiento de Datos Personales

El Instituto cuenta con un Inventario del SGSDP, mediante el cual se identifican, clasifican y documentan los sistemas físicos y electrónicos que realizan tratamiento de datos personales y datos personales sensibles en el ámbito académico, administrativo, técnico, científico y de prestación de servicios especializados.

El inventario tiene como finalidad:

- Identificar los sistemas institucionales que manejan datos personales;
- Determinar las áreas responsables;
- Identificar el tipo de datos tratados;
- Reconocer el nivel de riesgo asociado;
- Establecer medidas de seguridad aplicables;
- Facilitar el análisis de riesgo, análisis de brecha y acciones de mejora continua;
- Fortalecer el cumplimiento normativo institucional.

Cada sistema de tratamiento deberá contar, al menos, con:

- Identificación del sistema;
- Área responsable;
- Finalidad del tratamiento;
- Tipo de datos tratados;
- Clasificación de datos sensibles;
- Usuarios autorizados;
- Medios de almacenamiento;
- Ubicación física o electrónica;
- Riesgos identificados;
- Medidas de seguridad aplicables;
- Periodos de conservación;
- Transferencias de información, en su caso.

Inventario Institucional de Sistemas de Tratamiento de Datos Personales

Clave	Sistema de Tratamiento	Área Responsable	Tipo de Datos Tratados	Datos Sensibles	Medio de Almacenamiento	Nivel de Riesgo	Transferencias
INB-001-SGDP	Sistema de Información y Consulta Académica (SALVA)	Secretaría Académica / Área de Cómputo	Datos académicos, laborales y administrativos	No	Servidor institucional	Medio	
INB-002-SGDP	Expedientes para participación en convocatorias y plazas vacantes	Secretaría Académica	Datos de identificación, académicos y laborales	No	Expedientes físicos y carpetas digitales	Bajo	
INB-003-SGDP	Sistema de archivos académicos de la Secretaría Académica	Secretaría Académica	Datos académicos, administrativos y laborales	No	Expedientes físicos y electrónicos	Medio	
INB-004-SGDP	Sistema de tratamiento de la Unidad de Enseñanza y Posgrado	Unidad de Enseñanza y Posgrado	Datos escolares, académicos y becas	Parcialmente	Expedientes físicos y sistemas institucionales	Medio	
INB-005-SGDP	Sistema de Información Radiológica (RIS) de la URM	Unidad de Resonancia Magnética	Datos clínicos, médicos y biomédicos	Sí	Sistema RIS y servidores institucionales	Alto	Investigación científica y colaboración académica
INB-006-SGDP	Sistema de Neurodesarrollo de la UIND	Unidad de Investigación en Neurodesarrollo	Datos clínicos pediátricos, neurodesarrollo y socioeconómicos	Sí	Sistemas electrónicos institucionales	Alto	Estudios clínicos y colaboración interinstitucional
INB-007-SGDP	Sistema de Correo Electrónico Institucional	Área de Cómputo	Datos laborales y de identificación institucional	No	Plataforma de correo institucional	Medio	
INB-008-SGDP	Sistema Integral de Personal (SIP)	Secretaría Administrativa / Personal	Datos laborales, fiscales y administrativos	Parcialmente	Sistemas institucionales y expedientes físicos	Alto	
INB-009-SGDP	Sistema Integral de Compras (SIC)	Secretaría Administrativa / Presupuesto	Datos fiscales, patrimoniales y administrativos	No	Sistemas institucionales	Medio	

					y expedientes físicos		
INB-010-SGDP	Sistema de Expedientes Laborales y Administrativos	Área de Personal	Datos laborales, incapacidades, seguridad social	Sí	Expedientes físicos y electrónicos	Alto	
INB-011-SGDP	Sistema de Investigación Científica con Sujetos Humanos	Laboratorios y proyectos de investigación	Datos clínicos, biomédicos y protocolos de investigación	Sí	Bases de datos y sistemas especializados	Alto	Convenios nacionales e internacionales
INB-012-SGDP	Sistema de Videovigilancia y Control de Acceso (en su caso)	Seguridad / Servicios Generales	Imagen, accesos y registros de ingreso	Parcialmente	Sistemas electrónicos y servidores	Alto	
INB-013-SGDP	Sistema de Protección Civil y Atención de Emergencias	Protección Civil	Datos médicos básicos y emergencias	Sí	Expedientes físicos y electrónicos	Medio-Alto	
tINB-014-SGDP	Sistema de Gestión Jurídica y Procedimientos Institucionales	Oficina Jurídica / Enlace Jurídico	Datos laborales, disciplinarios y jurídicos	Sí	Expedientes físicos y digitales	Alto	

Contenido mínimo de cada sistema de tratamiento

Cada sistema identificado en el presente inventario deberá documentar y mantener actualizado, al menos, lo siguiente:

1. Identificación del sistema

- Nombre oficial;
- Clave institucional;
- Área responsable.

2. Finalidad del tratamiento: Descripción de las actividades institucionales que justifican el tratamiento de los datos personales.

3. Categorías de datos personales: Identificación de:

- Datos de identificación;
- Datos académicos;
- Datos laborales;
- Datos fiscales;
- Datos biométricos;
- Datos clínicos;
- Datos sensibles;
- Datos de menores de edad.

4. Usuarios autorizados
Listado del personal con acceso autorizado al sistema.

5. Soportes y almacenamiento

- Identificación de:
- Expedientes físicos;
- Servidores;
- Plataformas digitales;

- Bases de datos;
- Sistemas institucionales;
- Servicios tecnológicos utilizados.

6. Nivel de riesgo: Clasificación del nivel de riesgo conforme a:
- Sensibilidad de la información;
- Número de titulares;
- Exposición tecnológica;
- Transferencias;
- Riesgo de vulneración.

7. Medidas de seguridad: Medidas:
- Administrativas;
- Físicas;
- Técnicas.

8. Conservación y supresión: Plazos de conservación y mecanismos de bloqueo, borrado seguro o destrucción documental.

9. Transferencias de información: Identificación de:
- Destinatarios;
- Finalidades;
- Fundamento jurídico;
- Mecanismos de seguridad aplicables.

Actualización del inventario
El Inventario del SGSDP deberá actualizarse:
- Cuando se incorporen nuevos sistemas o plataformas;
- Cuando existan cambios tecnológicos;
- Cuando se modifiquen procesos institucionales;
- Cuando cambie el nivel de riesgo;
- Cuando se detecten vulneraciones;
- Cuando existan modificaciones normativas aplicables.

La actualización será coordinada por la persona Responsable de Seguridad de Datos Personales en colaboración con las áreas responsables de cada sistema institucional.

Clasificación prioritaria de sistemas de alto riesgo
El Instituto reconoce como sistemas prioritarios de atención reforzada aquellos que involucren:

- Datos personales sensibles;
- Información clínica;
- Datos biomédicos;
- Neuroimagen;
- Información de niñas, niños y adolescentes;

- Investigación científica con sujetos humanos;
- Sistemas electrónicos con múltiples accesos;
- Transferencias nacionales o internacionales de información.

Los sistemas clasificados como de alto riesgo deberán contar con controles reforzados de seguridad y mecanismos adicionales de monitoreo, supervisión y protección institucional.

10. Transferencias de información

Las áreas responsables deberán identificar y documentar las transferencias nacionales e internacionales de datos personales derivadas de actividades académicas, científicas, administrativas o tecnológicas, incluyendo destinatarios, finalidades, fundamento jurídico y medidas de seguridad aplicables.

X. Análisis de Riesgo

El Instituto realiza el presente Análisis de Riesgo como parte integral del SGSDP, con el propósito de identificar, evaluar, clasificar y mitigar los riesgos asociados al tratamiento de datos personales y datos personales sensibles que se encuentran bajo su posesión y resguardo institucional.

El análisis de riesgo permite identificar las posibles vulneraciones que podrían afectar la confidencialidad, integridad, disponibilidad y trazabilidad de los datos personales, así como establecer medidas preventivas, correctivas y de mitigación acordes al nivel de exposición y sensibilidad de la información tratada.

El presente análisis se desarrolla conforme a:

- La Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados;
- Los Lineamientos para la Protección de Datos Personales en Posesión de la Universidad Nacional Autónoma de México;
- Las Normas Complementarias sobre Medidas de Seguridad Técnicas, Administrativas y Físicas;
- Las mejores prácticas institucionales en materia de seguridad de la información y gestión de riesgos.

1. Objetivos del análisis de riesgo

El análisis de riesgo tiene como objetivos:

- Identificar amenazas y vulnerabilidades relacionadas con el tratamiento de datos personales;
- Evaluar el nivel de exposición institucional;
- Determinar el impacto potencial de una vulneración de seguridad;
- Identificar sistemas prioritarios de atención;
- Establecer controles y medidas de mitigación;

- Fortalecer la protección de datos personales sensibles;
- Reducir riesgos tecnológicos, administrativos y operativos;
- Promover acciones preventivas y de mejora continua.

2. Metodología general

El Instituto adopta un enfoque preventivo y basado en riesgos considerando:

a) Identificación de activos: Se identifican:

- Sistemas institucionales;
- Bases de datos;
- Expedientes físicos;
- Plataformas digitales;
- Infraestructura tecnológica;
- Redes;
- Servidores;
- Equipos de cómputo;
- Personal autorizado.

b) Identificación de amenazas: Se consideran amenazas de origen:

- Humano;
- Tecnológico;
- Ambiental;
- Operativo;
- Externo;
- Interno.

c) Identificación de vulnerabilidades: Se analizan debilidades relacionadas con:

- Accesos;
- Infraestructura;
- Procesos;
- Configuraciones;
- Capacitación;
- Manejo documental;
- Plataformas tecnológicas.

d) Valoración del impacto: Se evalúa el posible impacto sobre:

- Personas titulares;
- Operación institucional;
- Confidencialidad;
- Continuidad operativa;
- Cumplimiento normativo;

- Reputación institucional.

e) Determinación del nivel de riesgo: El nivel de riesgo se determina considerando:

- Probabilidad de ocurrencia;
- Impacto potencial;
- Sensibilidad de los datos;
- Exposición tecnológica;
- Número de titulares afectados.

3. Clasificación institucional de riesgos

Nivel	Descripción
Bajo	Riesgo controlado con impacto limitado y baja probabilidad de afectación
Medio	Riesgo moderado que requiere medidas preventivas y seguimiento
Alto	Riesgo significativo con potencial de afectar datos sensibles, continuidad operativa o derechos de titulares
Crítico	Riesgo severo con posibilidad de vulneración masiva, daño institucional o afectación grave a titulares

4. Principales amenazas identificadas

a) Amenazas tecnológicas

- Malware y ransomware;
- Accesos no autorizados;
- Robo de credenciales;
- Fallas de servidores;
- Pérdida de respaldos;
- Ataques a redes;
- Vulnerabilidades de software;
- Uso de dispositivos no autorizados.

b) Amenazas administrativas y operativas

- Manejo inadecuado de expedientes;
- Error humano;
- Transferencia indebida de información;
- Falta de capacitación;
- Acceso excesivo de usuarios;
- Uso de plataformas no autorizadas;
- Ausencia de controles documentales.

c) Amenazas físicas

- Robo de equipos;
- Acceso físico no autorizado;
- Incendios;
- Inundaciones;

- Sismos;
- Fallas eléctricas;
- Deterioro documental.

d) Amenazas externas

- Ataques cibernéticos;
- Fuga de información;
- Acceso de terceros;
- Vulneraciones de servicios tecnológicos externos;
- Riesgos asociados a servicios en nube.

5. Vulnerabilidades identificadas

Leyenda reservada
Partes reservadas: apartado X Análisis de riesgo; punto 5. Vulnerabilidades identificadas.
Fundamento: articulo 112, fracción VII, de la Ley General de Transparencia y Acceso a la Información pública.
Resolución: CTUNAM/476/2026, de 09 de octubre de 2026.
Plazo: cinco años, del 09 de octubre de 2026 al 09 de octubre de 2031

6. Sistemas prioritarios de atención reforzada

El Instituto identifica como sistemas de alto riesgo aquellos que manejan:

- Datos personales sensibles;
- Información clínica;
- Neuroimagen;
- Datos biomédicos;
- Datos de menores de edad;
- Información de investigación científica;

Sistemas electrónicos multiusuario.

Particularmente:

Sistema	Riesgo Identificado	Nivel
Sistema RIS de la URM	URM: Datos clínicos y neuroimagen	Alto
Sistema UIND Neurodesarrollo	UIND: Datos pediátricos y clínicos	Alto
Expedientes laborales	SA-Personal: Información médica y administrativa	Alto
Investigación con sujetos humanos	Laboratorios-Unidades: Información biomédica sensible	Alto
Videovigilancia y control de acceso	Secretaria Técnica- Unidad de Computo: Imagen y registros de acceso	Medio-Alto

Riesgos asociados a plataformas digitales, servicios en nube y colaboración científica internacional: El Instituto reconoce riesgos específicos asociados al uso de:

- Correo electrónico institucional;
- Plataformas digitales;
- Servicios compartidos;
- Sistemas en nube;
- Almacenamiento externo;
- Investigación multicéntrica;
- Transferencias electrónicas.

En particular, se deberá vigilar:

- Control de permisos;
- Accesos externos;
- Respaldo institucional;
- Transferencias internacionales;
- Protección de credenciales;
- Configuración segura de plataformas.

7. Evaluación del impacto potencial: Las vulneraciones de seguridad podrían generar:

- Afectación a la privacidad de titulares;
- Divulgación indebida de información sensible;
- Riesgos clínicos o reputacionales;
- Interrupción de operaciones institucionales;
- Responsabilidades administrativas o legales;
- Daño reputacional al Instituto y a la Universidad;
- Afectaciones a proyectos de investigación y convenios institucionales.

8. Medidas generales de mitigación: El Instituto implementará medidas orientadas a reducir riesgos mediante:

- Control de accesos;
- Restricción de privilegios;
- Respaldo periódico;
- Protección antivirus;
- Actualización tecnológica;
- Capacitación;
- Gestión documental;
- Supervisión institucional;
- Monitoreo de incidentes;
- Políticas de seguridad;
- Protección física de expedientes y equipos.

9. Monitoreo y revisión del análisis de riesgo: El análisis de riesgo deberá revisarse periódicamente o cuando:

- Existan cambios tecnológicos;
- Se incorporen nuevos sistemas;
- Se detecten vulneraciones;
- Existan incidentes de seguridad;
- Cambie la naturaleza de los datos tratados;
- Existan cambios normativos;
- Se modifiquen procesos institucionales.

La revisión será coordinada por la persona Responsable de Seguridad de Datos Personales en colaboración con las áreas responsables.

10. Enfoque de mejora continua

El Instituto mantendrá un enfoque permanente de mejora continua en materia de gestión de riesgos y protección de datos personales, fortaleciendo progresivamente:

- Sus controles de seguridad;
- Su infraestructura tecnológica;
- Sus mecanismos de supervisión;
- La capacitación institucional;
- La trazabilidad documental;
- La atención de vulneraciones e incidentes de seguridad.

11. Sistemas sujetos a posible Evaluación de Impacto

El Instituto identifica que los sistemas institucionales relacionados con neuroimagen, investigación con sujetos humanos, datos clínicos, información biomédica y datos de

menores de edad podrán requerir Evaluaciones de Impacto en Protección de Datos Personales conforme al nivel de riesgo asociado.

El análisis de riesgo constituye un instrumento dinámico que deberá actualizarse conforme a las necesidades operativas, tecnológicas y normativas del Instituto.

XI. Análisis de Brecha.

El Instituto realiza el presente Análisis de Brecha como parte integral del SGSDP, con el propósito de identificar diferencias, deficiencias, áreas de oportunidad y necesidades de fortalecimiento existentes entre las medidas de seguridad actualmente implementadas y aquellas requeridas por la normatividad aplicable en materia de protección de datos personales y seguridad de la información.

El análisis de brecha permite evaluar el nivel de madurez institucional en materia de protección de datos personales, identificar vulnerabilidades operativas, administrativas, físicas y tecnológicas, así como definir acciones de mejora orientadas al fortalecimiento continuo del SGSDP.

El presente análisis se realiza conforme a:

- La Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados;
- Los Lineamientos para la Protección de Datos Personales en Posesión de la Universidad Nacional Autónoma de México;
- Las Normas Complementarias sobre Medidas de Seguridad Técnicas, Administrativas y Físicas;
- Las mejores prácticas institucionales en materia de seguridad de la información.

1. Objetivos del análisis de brecha: El análisis de brecha tiene como objetivos:

- Identificar diferencias entre el estado actual y el estado deseado de cumplimiento normativo;
- Detectar debilidades administrativas, físicas y técnicas;
- Identificar áreas prioritarias de fortalecimiento;
- Evaluar el nivel de implementación de controles de seguridad;
- Determinar necesidades de actualización tecnológica y documental;
- Fortalecer la gestión de riesgos institucional;
- Definir acciones preventivas y correctivas;
- Establecer prioridades para el plan de trabajo institucional.

2. Metodología general: El Instituto realizó el análisis de brecha considerando:

a) Revisión normativa: Análisis de obligaciones establecidas en:
- Ley General de Protección de Datos Personales;
- Lineamientos UNAM;

- Normas Complementarias;
- Disposiciones institucionales aplicables.

b) Revisión documental: Evaluación de:
- Inventarios;
- Avisos de privacidad;
- Procedimientos;
- Expedientes;
- Controles institucionales;
- Sistemas de tratamiento;
- Políticas de seguridad.

c) Revisión operativa y tecnológica: Evaluación de:
- Infraestructura tecnológica;
- Sistemas institucionales;
- Controles de acceso;
- Manejo documental;
- Plataformas digitales;
- Redes y respaldos;
- Medidas físicas y técnicas de seguridad.

d) Evaluación de cumplimiento: Identificación del grado de cumplimiento:
- Total;
- Parcial;
- Insuficiente;
- No implementado.

3. Resultados generales del análisis de brecha

Derivado de la evaluación institucional realizada, el Instituto identifica que actualmente cuenta con un nivel de cumplimiento parcial en materia de protección de datos personales, observándose avances relevantes en:

- Identificación de sistemas de tratamiento;
- Elaboración del Documento de Seguridad;
- Implementación básica de controles administrativos;
- Definición preliminar de responsables;
- Protección física básica de expedientes;
- Uso de infraestructura institucional de tecnologías de información.

No obstante, se identifican áreas que requieren fortalecimiento y consolidación institucional.

4. Principales brechas identificadas

A. Brechas administrativas

Brecha identificada	Situación actual	Nivel
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

Leyenda reservada
Partes reservadas: apartado XI. Análisis de Brecha, punto 4. Principales brechas identificadas; tabla A: Brechas administrativas.
Fundamento: articulo 112, fracción VII, de la Ley General de Transparencia y Acceso a la Información pública.
Resolución: CTUNAM/476/2026, de 09 de octubre de 2026.
Plazo: cinco años, del 09 de octubre de 2026 al 09 de octubre de 2031.

B. Brechas físicas

Brecha identificada	Situación actual	Nivel
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

Leyenda reservada
Partes reservadas: apartado XI. Análisis de Brecha, punto 4. Principales brechas identificadas; tabla B: Brechas físicas.
Fundamento: articulo 112, fracción VII, de la Ley General de Transparencia y Acceso a la Información pública.
Resolución: CTUNAM/476/2026, de 09 de octubre de 2026.
Plazo: cinco años, del 09 de octubre de 2026 al 09 de octubre de 2031.

C. Brechas técnicas

Brecha identificada	Situación actual	Nivel
[redacted]	[redacted]	[redacted]

Leyenda reservada
Partes reservadas: apartado XI. Análisis de Brecha, punto 4. Principales brechas identificadas; tabla C: Brechas técnicas.
Fundamento: articulo 112, fracción VII, de la Ley General de Transparencia y Acceso a la Información pública.
Resolución: CTUNAM/476/2026, de 09 de octubre de 2026.
Plazo: cinco años, del 09 de octubre de 2026 al 09 de octubre de 2031.

5. Brechas prioritarias en sistemas de alto riesgo: [redacted]

Leyenda reservada
Partes reservadas: apartado XI. Análisis de Brecha, punto 5. Brechas prioritarias en sistemas de alto riesgo.
Fundamento: articulo 112, fracción VII, de la Ley General de Transparencia y Acceso a la Información pública.
Resolución: CTUNAM/476/2026, de 09 de octubre de 2026.
Plazo: cinco años, del 09 de octubre de 2026 al 09 de octubre de 2031.

Particularmente:

Sistema	Brecha principal
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]

Leyenda reservada
Partes reservadas: apartado XI. Análisis de Brecha, punto 5. Brechas prioritarias en sistemas de alto riesgo.
Fundamento: articulo 112, fracción VII, de la Ley General de Transparencia y Acceso a la Información pública.
Resolución: CTUNAM/476/2026, de 09 de octubre de 2026.
Plazo: cinco años, del 09 de octubre de 2026 al 09 de octubre de 2031.

6. Evaluación del nivel de madurez institucional

Componente	Nivel de madurez
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]

Leyenda reservada
Partes reservadas: apartado XI. Análisis de Brecha, punto 6. Evaluación del nivel de madurez institucional.
Fundamento: articulo 112, fracción VII, de la Ley General de Transparencia y Acceso a la Información pública.
Resolución: CTUNAM/476/2026, de 09 de octubre de 2026.
Plazo: cinco años, del 09 de octubre de 2026 al 09 de octubre de 2031.

7. Necesidades de fortalecimiento identificadas: [redacted]

[redacted]

-

Leyenda reservada
Partes reservadas: apartado XI. Análisis de Brecha. Punto 7. Necesidades de fortalecimiento identificadas.
Fundamento: articulo 112, fracción VII, de la Ley General de Transparencia y Acceso a la Información pública.
Resolución: CTUNAM/476/2026, de 09 de octubre de 2026.
Plazo: cinco años, del 09 de octubre de 2026 al 09 de octubre de 2031.

8. Acciones institucionales de mejora: Como resultado del análisis de brecha, el Instituto implementará acciones orientadas a:

- Fortalecer controles administrativos, físicos y técnicos;
- Actualizar políticas y procedimientos;
- Mejorar la infraestructura tecnológica;
- Formalizar controles documentales;
- Reforzar protección de sistemas de alto riesgo;
- Implementar capacitación especializada;
- Fortalecer supervisión y monitoreo institucional;
- Consolidar mecanismos de mejora continua.

9. Seguimiento y actualización del análisis de brecha: El análisis de brecha deberá revisarse y actualizarse periódicamente o cuando:

- Existan cambios tecnológicos;
- Se incorporen nuevos sistemas;
- Se detecten vulneraciones;
- Existan auditorías o revisiones;
- Cambie la normatividad aplicable;
- Se modifiquen procesos institucionales.

La actualización será coordinada por la persona Responsable de Seguridad de Datos Personales en colaboración con las áreas responsables.

10. Mejora continua institucional

El Instituto reconoce que el fortalecimiento de la protección de datos personales constituye un proceso permanente y progresivo, por lo que mantendrá acciones institucionales orientadas a consolidar un modelo integral de seguridad de la información basado en:

- Prevención;
- Gestión de riesgos;
- Supervisión;
- Capacitación;
- Innovación tecnológica;
- Cumplimiento normativo;
- Protección de los derechos de las personas titulares.

El presente análisis de brecha constituye una herramienta dinámica de evaluación institucional y mejora continua del SGSDP del Instituto.

XII. Plan de trabajo.

El Instituto establece el presente Plan de Trabajo como instrumento institucional de planeación, seguimiento y mejora continua del SGSDP, con la finalidad de fortalecer progresivamente las medidas de seguridad administrativas, físicas y técnicas aplicables al tratamiento de datos personales y datos personales sensibles bajo su resguardo.

El presente Plan de Trabajo se deriva del:

- Inventario de Sistemas de Tratamiento;
- Análisis de Riesgo;
- Análisis de Brecha;
- Identificación de vulnerabilidades;
- Necesidades operativas y tecnológicas institucionales;
- Requerimientos normativos aplicables.

Leyenda reservada
Partes reservadas: apartado XII. Plan de Trabajo.
Fundamento: articulo 112, fracción VII, de la Ley General de Transparencia y Acceso a la Información pública.
Resolución: CTUNAM/476/2026, de 09 de octubre de 2026.
Plazo: cinco años, del 09 de octubre de 2026 al 09 de octubre de 2031.

1. Objetivos del Plan de Trabajo: El presente Plan de Trabajo tiene como objetivos:

- Fortalecer el cumplimiento normativo institucional;
- Consolidar el SGSDP;
- Reducir riesgos y vulnerabilidades identificadas;
- Fortalecer medidas administrativas, físicas y técnicas;
- Mejorar la seguridad de sistemas institucionales;
- Incrementar la trazabilidad y control de accesos;
- Fortalecer la protección de datos sensibles;
- Implementar acciones de mejora continua;
- Consolidar una cultura institucional de protección de datos personales.

2. Ejes estratégicos de trabajo: El Instituto implementará acciones organizadas en los siguientes ejes estratégicos:

Eje 1. Fortalecimiento normativo y documental

- Actualización del Documento de Seguridad;
- Formalización de procedimientos internos;
- Actualización de avisos de privacidad;
- Integración de matrices de transferencia de datos;
- Fortalecimiento de controles documentales;
- Definición de políticas de conservación y supresión.

Eje 2. Fortalecimiento administrativo

- Designación formal de responsables;
- Consolidación del inventario institucional;
- Actualización de roles y perfiles de acceso;
- Implementación de mecanismos de supervisión;
- Homologación de procesos institucionales.

Eje 3. Fortalecimiento físico

- Mejora de resguardo documental;

- Control de acceso físico a áreas sensibles;
- Protección de expedientes físicos;
- Fortalecimiento de controles en áreas restringidas;
- Protección de infraestructura crítica.

Eje 4. Fortalecimiento tecnológico

[redacted]

Leyenda reservada
Partes reservadas: apartado XII. Plan de Trabajo. Eje 4, Fortalecimiento tecnológico.
Fundamento: articulo 112, fracción VII, de la Ley General de Transparencia y Acceso a la Información pública.
Resolución: CTUNAM/476/2026, de 09 de octubre de 2026.
Plazo: cinco años, del 09 de octubre de 2026 al 09 de octubre de 2031.

Eje 5. Capacitación y cultura institucional

- Capacitación periódica;
- Sensibilización institucional;
- Difusión de buenas prácticas;
- Capacitación especializada para áreas de alto riesgo;
- Promoción de cultura de confidencialidad y seguridad.

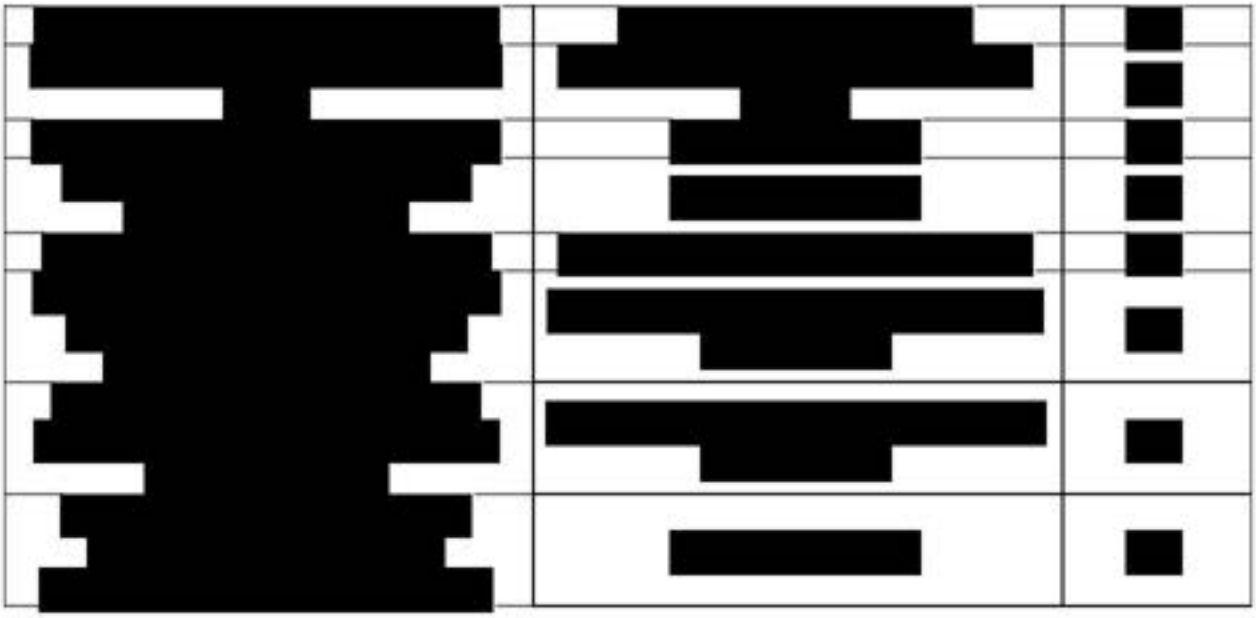
Eje 6. Gestión de incidentes y mejora continua

- Implementación de mecanismos de reporte;
- Atención y documentación de vulneraciones;
- Revisión periódica del análisis de riesgo;
- Revisión del análisis de brecha;
- Actualización continua del SGSDP.

3. Acciones prioritarias institucionales

A. Acciones de corto plazo

Acción	Responsable	Prioridad
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]



Leyenda reservada
Partes reservadas: apartado XII. Plan de trabajo. punto 3. Acciones prioritarias institucionales; tabla A. Acciones de corto plazo.
Fundamento: articulo 112, fracción VII, de la Ley General de Transparencia y Acceso a la Información pública.
Resolución: CTUNAM/476/2026, de 09 de octubre de 2026.
Plazo: cinco años, del 09 de octubre de 2026 al 09 de octubre de 2031.

B. Acciones de mediano plazo

Acción	Responsable	Prioridad

Leyenda reservada
Partes reservadas: apartado XII. Plan de trabajo. punto 3. Acciones prioritarias institucionales; tabla B. Acciones de mediano plazo
Fundamento: articulo 112, fracción VII, de la Ley General de Transparencia y Acceso a la Información pública.
Resolución: CTUNAM/476/2026, de 09 de octubre de 2026.
Plazo: cinco años, del 09 de octubre de 2026 al 09 de octubre de 2031.

C. Acciones de largo plazo

Acción	Responsable	Prioridad
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

Leyenda reservada
Partes reservadas: XII. Plan de trabajo. punto 3. Acciones prioritarias institucionales; tabla C. Acciones de largo plazo.
Fundamento: articulo 112, fracción VII, de la Ley General de Transparencia y Acceso a la Información pública.
Resolución: CTUNAM/476/2026, de 09 de octubre de 2026.
Plazo: cinco años, del 09 de octubre de 2026 al 09 de octubre de 2031.

4. Sistemas prioritarios de atención: [redacted]

Leyenda reservada
Partes reservadas: apartado XII. Plan de Trabajo. Punto 4. Sistemas prioritarios de atención.
Fundamento: articulo 112, fracción VII, de la Ley General de Transparencia y Acceso a la Información pública.
Resolución: CTUNAM/476/2026, de 09 de octubre de 2026.
Plazo: cinco años, del 09 de octubre de 2026 al 09 de octubre de 2031.

Particularmente:

- Sistema RIS de la URM;
- Sistema UIND Neurodesarrollo;
- Expedientes laborales;
- Sistemas de investigación con sujetos humanos;
- Plataformas institucionales de acceso compartido.

5. Recursos y coordinación institucional: La implementación del presente Plan de Trabajo requerirá:

- Coordinación interinstitucional;
- Participación de áreas responsables;
- Fortalecimiento organizacional;
- Capacitación especializada;
- Recursos tecnológicos y administrativos;
- Seguimiento institucional permanente.

La Dirección del Instituto promoverá las acciones necesarias para fortalecer progresivamente las capacidades institucionales en materia de protección de datos personales y seguridad de la información.

6. Seguimiento y evaluación: El seguimiento del presente Plan de Trabajo será coordinado por la persona Responsable de Seguridad de Datos Personales en colaboración con:

- Dirección;
- Área de Cómputo;
- Secretaría Administrativa;
- Secretaría Académica;
- Enlace de Transparencia;
- Responsables de sistemas institucionales.

Se realizarán revisiones periódicas para:

- Evaluar avances;
- Verificar cumplimiento;
- Identificar nuevas necesidades;

- Actualizar prioridades;
- Implementar acciones correctivas.

7. Indicadores generales de seguimiento: El Instituto podrá utilizar, entre otros, los siguientes indicadores:

- Número de sistemas inventariados;
- Número de áreas capacitadas;
- Incidentes reportados;
- Sistemas con respaldo activo;
- Sistemas con control de acceso implementado;
- Procedimientos actualizados;
- Avisos de privacidad revisados;
- Acciones correctivas implementadas.

8. Mejora continua: El presente Plan de Trabajo constituye un instrumento dinámico y sujeto a actualización permanente conforme a:

- Cambios normativos;
- Actualizaciones tecnológicas;
- Nuevos riesgos identificados;
- Vulneraciones detectadas;
- Requerimientos operativos;
- Nuevos sistemas institucionales.

El Instituto mantendrá acciones continúas orientadas al fortalecimiento progresivo de su SGSDP, privilegiando la protección de los derechos de las personas titulares y la seguridad institucional de la información.

XIII. Capacitación.

El Instituto reconoce que la capacitación y sensibilización del personal constituyen elementos fundamentales para garantizar la adecuada protección de los datos personales y fortalecer el SGSDP, por lo que establecerá programas permanentes de formación institucional en materia de protección de datos personales, seguridad de la información y manejo responsable de información institucional.

Las acciones de capacitación tendrán como finalidad fortalecer las capacidades técnicas, administrativas y operativas del personal universitario que interviene en el tratamiento de datos personales, promoviendo una cultura institucional basada en:

- Legalidad;
- Confidencialidad;
- Responsabilidad;
- Ética;
- Prevención;

- Seguridad de la información;
- Protección de derechos de las personas titulares.

1. Objetivos de la capacitación: El programa institucional de capacitación tendrá los siguientes objetivos:

- Buenas prácticas para investigación científica y colaboración internacional;
- Fortalecer el conocimiento normativo en materia de protección de datos personales;
- Sensibilizar al personal respecto de la importancia institucional y legal del tratamiento adecuado de datos personales;
- Promover buenas prácticas de seguridad de la información;
- Reducir riesgos asociados al error humano;
- Fortalecer el cumplimiento de políticas y procedimientos institucionales;
- Capacitar al personal en la atención de incidentes y vulneraciones;
- Fortalecer la protección de datos personales sensibles;
- Promover la mejora continua del SGSDP.

2. Alcance de la capacitación: Las acciones de capacitación estarán dirigidas a:

- Personal académico;
- Personal administrativo;
- Personal técnico;
- Personal de confianza;
- Prestadores de servicios;
- Becarios;
- Personas usuarias autorizadas;
- Responsables de sistemas institucionales;
- Personal con acceso a datos personales sensibles;
- Áreas de tecnologías de información;
- Responsables de investigación con sujetos humanos.

La capacitación será proporcional al nivel de acceso, responsabilidad y riesgo asociado al tratamiento de datos personales.

3. Temas generales de capacitación: El programa institucional podrá incluir, entre otros, los siguientes temas:

a) Marco normativo

- Ley General de Protección de Datos Personales;
- Lineamientos UNAM;
- Normas Complementarias;
- Derechos ARCO;
- Avisos de privacidad;
- Responsabilidades institucionales.

b) Seguridad de la información

- Protección de contraseñas;
- Seguridad en equipos institucionales;
- Protección de redes y sistemas;
- Uso seguro de plataformas digitales;
- Prevención de malware y phishing;
- Manejo seguro de información institucional.

c) Gestión documental

- Resguardo de expedientes;
- Conservación documental;
- Clasificación de información;
- Borrado seguro;
- Supresión documental.

d) Atención de incidentes

- Identificación de vulneraciones;
- Reporte de incidentes;
- Medidas preventivas;
- Acciones correctivas;
- Manejo de contingencias.

e) Protección de datos sensibles

- Datos clínicos;
- Neuroimagen;
- Datos biomédicos;
- Datos de menores de edad;
- Investigación con sujetos humanos;
- Información confidencial especializada.

4. Capacitación especializada: El Instituto implementará capacitación especializada para áreas y sistemas de alto riesgo, particularmente aquellos relacionados con:

- Unidad de Resonancia Magnética (URM);
- Unidad de Investigación en Neurodesarrollo (UIND);
- Investigación clínica y biomédica;
- Expedientes laborales;
- Sistemas tecnológicos institucionales;
- Investigación con sujetos humanos;
- Plataformas digitales y sistemas multiusuario.

La capacitación especializada podrá considerar:

- Seguridad avanzada de información;
- Manejo de datos clínicos;
- Ética y confidencialidad;
- Gestión de riesgos;

- Trazabilidad y control de accesos;
- Protección reforzada de datos sensibles.

5. Modalidades de capacitación: Las actividades de capacitación podrán realizarse mediante:

- Cursos presenciales;
- Cursos en línea;
- Talleres;
- Conferencias;
- Sesiones informativas;
- Materiales de difusión;
- Campañas institucionales;
- Capacitación autogestiva;
- Simulacros o ejercicios institucionales.

6. Periodicidad: El Instituto promoverá actividades periódicas de capacitación y sensibilización, procurando:

- Capacitación inicial para personal de nuevo ingreso;
- Actualización periódica para personal con acceso a datos personales;
- Capacitación especializada para áreas de alto riesgo;
- Actividades de actualización derivadas de cambios normativos o tecnológicos.

7. Responsables de coordinación: La coordinación de las actividades de capacitación corresponderá a:

- La persona Responsable de Seguridad de Datos Personales;
- Dirección del Instituto;
- Área de Tecnologías de la Información;
- Secretaría Administrativa;
- Enlace de Transparencia;
- Áreas responsables de sistemas institucionales.

El Instituto podrá apoyarse en:

- DGTIC;
- Unidad de Transparencia de la UNAM;
- Dependencias universitarias especializadas;
- Instancias externas autorizadas.

8. Evidencia y seguimiento: Las actividades de capacitación deberán documentarse mediante:

- Listas de asistencia;
- Constancias;
- Materiales utilizados;
- Registros institucionales;
- Evidencias electrónicas;

- Reportes de participación.

El Instituto procurará mantener mecanismos de seguimiento para:

- Identificar áreas capacitadas;
- Detectar necesidades de actualización;
- Evaluar cobertura institucional;
- Fortalecer áreas prioritarias.

9. Sensibilización institucional: El Instituto promoverá acciones permanentes de sensibilización orientadas a fortalecer una cultura institucional de:

- Protección de datos personales;
- Seguridad de la información;
- Confidencialidad;
- Prevención de riesgos;
- Responsabilidad institucional;
- Uso legítimo de información personal.

Estas acciones podrán incluir:

- Difusión electrónica;
- Carteles informativos;
- Campañas institucionales;
- Recomendaciones de seguridad;
- Buenas prácticas institucionales.

10. Evaluación y mejora continua: El programa de capacitación será objeto de revisión periódica para:

- Actualizar contenidos;
- Incorporar cambios normativos;
- Fortalecer áreas de oportunidad;
- Atender riesgos identificados;
- Mejorar la cobertura institucional.

La capacitación y sensibilización institucional constituyen medidas preventivas fundamentales para fortalecer la protección de datos personales y reducir riesgos derivados del manejo inadecuado de información institucional.

11. Compromiso institucional

El Instituto reconoce que la capacitación continua del personal es un elemento esencial para garantizar el adecuado funcionamiento del SGSDP y fortalecer la protección de los derechos de las personas titulares.

Por ello, mantendrá acciones permanentes orientadas al fortalecimiento de las capacidades institucionales en materia de:

- Protección de datos personales;
- Seguridad de la información;

- Gestión de riesgos;
- Manejo seguro de información sensible;
- Cumplimiento normativo institucional.

XIV. Anexos.

Los presentes anexos forman parte integral del Documento de SGSDP del Instituto y tienen como finalidad complementar, documentar y respaldar los procesos, medidas, controles, mecanismos y acciones institucionales relacionadas con el SGSDP.

Los anexos constituyen instrumentos técnicos, administrativos y documentales de apoyo para la implementación, seguimiento, supervisión y mejora continua de las medidas de seguridad aplicables al tratamiento de datos personales y datos personales sensibles en posesión del Instituto.

Los anexos podrán actualizarse periódicamente conforme a:

- Cambios normativos;
- Modificaciones operativas;
- Incorporación de nuevos sistemas;
- Actualizaciones tecnológicas;
- Resultados de auditorías;
- Identificación de riesgos o vulneraciones;
- Necesidades institucionales.

A) Relación de anexos

Anexo 1. Inventario detallado de sistemas de tratamiento de datos personales: Contendrá**:**

- Clave del sistema;
- Nombre del sistema;
- Área responsable;
- Finalidad;
- Categorías de datos personales;
- Clasificación de datos sensibles;
- Usuarios autorizados;
- Medio de almacenamiento;
- Nivel de riesgo;
- Transferencias;
- Periodos de conservación;
- Medidas de seguridad aplicables.

Anexo 2. Inventario de activos de información: Contendrá la identificación de:

- Servidores;
- Equipos de cómputo;
- Bases de datos;

- Plataformas institucionales;
- Redes;
- Expedientes físicos;
- Dispositivos de almacenamiento;
- Infraestructura tecnológica;
- Sistemas institucionales críticos.

Anexo 3. Matriz de riesgos institucionales: Contendrá:

- Riesgos identificados;
- Probabilidad de ocurrencia;
- Impacto;
- Nivel de riesgo;
- Medidas de mitigación;
- Responsables;
- Acciones preventivas y correctivas.

Anexo 4. Matriz de análisis de brecha: Contendrá:

- Requisitos normativos;
- Situación actual;
- Nivel de cumplimiento;
- Brechas identificadas;
- Acciones de mejora;
- Responsables;
- Prioridades institucionales.

Anexo 5. Matriz de transferencias de datos personales: [redacted]

[redacted]

Leyenda reservada
Partes reservadas: apartado XIV. Anexos. Anexo **5**. Matriz de transferencias de datos personales.
Fundamento: articulo 112, fracción VII, de la Ley General de Transparencia y Acceso a la Información pública.
Resolución: CTUNAM/476/2026, de 09 de octubre de 2026.
Plazo: cinco años, del 09 de octubre de 2026 al 09 de octubre de 2031.

Anexo 6. Avisos de privacidad: Integrará:

- Avisos de privacidad simplificados;

- Avisos de privacidad integrales;
- Identificación de sistemas asociados;
- Versiones autorizadas y vigentes.

Anexo 7. Procedimiento de atención de vulneraciones e incidentes de seguridad: Contendrá:

- Mecanismos de detección;
- Reporte institucional;
- Contención;
- Escalamiento;
- Medidas correctivas;
- Notificación;
- Seguimiento y cierre de incidentes.

Anexo 8. Procedimiento de respaldo y recuperación de información: Contendrá:

- Políticas de respaldo;
- Periodicidad;
- Responsables;
- Tipos de respaldo;
- Resguardo;
- Recuperación ante contingencias;
- Medidas de seguridad aplicables.

Anexo 9. Procedimiento de conservación, bloqueo y supresión documental: Contendrá:

- Periodos de conservación;
- Criterios archivísticos;
- Bloqueo;
- Transferencia documental;
- Borrado seguro;
- Destrucción documental.

Anexo 10. Formatos institucionales: Integrará formatos relacionados con:

- Control de accesos;
- Reporte de incidentes;
- Responsivas de confidencialidad;
- Solicitudes de acceso;
- Registro de capacitación;
- Autorizaciones institucionales;
- Bitácoras de seguridad.

Anexo 11. Programa institucional de capacitación: Contendrá:

- Calendario anual;
- Temas de capacitación;
- Áreas prioritarias;

- Mecanismos de evaluación;
- Evidencias y seguimiento.

Anexo 12. Directorio de responsables: Integrará:

- Responsables de sistemas;
- Responsables de área;
- Responsable de Seguridad de Datos Personales;
- Enlace de Transparencia;
- Contactos institucionales relacionados con seguridad y protección de datos.

Anexo 13. Relación de sistemas de alto riesgo: [redacted]

Leyenda reservada
Partes reservadas: apartado XIV. Anexos. Anexo **13**. Relación de sistemas de alto riesgo.
Fundamento: articulo 112, fracción VII, de la Ley General de Transparencia y Acceso a la Información pública.
Resolución: CTUNAM/476/2026, de 09 de octubre de 2026.
Plazo: cinco años, del 09 de octubre de 2026 al 09 de octubre de 2031.

Anexo 14. Bitácora de revisión y actualización del Documento de Seguridad: Contendrá:

- Número de versión;
- Fecha de actualización;
- Modificaciones realizadas;
- Responsables;
- Validación institucional correspondiente.

Administración y resguardo de anexos: Los anexos del presente Documento de Seguridad deberán:

- Mantenerse actualizados;
- Resguardarse de manera segura;
- Contar con controles de acceso;
- Ser administrados por las áreas responsables correspondientes;
- Estar disponibles para revisiones institucionales autorizadas.

Cuando los anexos contengan:

- Datos personales;
- Información sensible;
- Datos técnicos de seguridad;
- Infraestructura crítica;
- Configuraciones tecnológicas;
- Bitácoras o registros de incidentes, su acceso deberá restringirse exclusivamente al personal autorizado conforme a sus funciones institucionales.

Actualización de anexos: Los anexos podrán actualizarse sin necesidad de modificar integralmente el Documento de Seguridad, siempre que:

- Se mantenga congruencia normativa;
- Se documenten las modificaciones realizadas;
- Exista validación institucional correspondiente;
- Se preserve la trazabilidad documental.

La actualización de anexos será coordinada por la persona Responsable de Seguridad de Datos Personales en colaboración con las áreas responsables.

Consideraciones finales

Los anexos constituyen elementos técnicos y operativos fundamentales para la implementación efectiva del SGSDP del Instituto, por lo que deberán mantenerse permanentemente actualizados, protegidos y alineados a las necesidades operativas, tecnológicas y normativas institucionales.

El Instituto promoverá acciones permanentes orientadas al fortalecimiento progresivo de dichos instrumentos, privilegiando en todo momento la protección de los derechos de las personas titulares y la seguridad institucional de la información.

Declaración institucional de compromiso

El Instituto de Neurobiología reconoce la protección de datos personales y la seguridad de la información como elementos estratégicos para el cumplimiento de sus funciones sustantivas y administrativas, por lo que mantendrá acciones permanentes orientadas al fortalecimiento del Sistema de Gestión de Seguridad de Datos Personales, la gestión de riesgos, la mejora continua y la protección de los derechos de las personas titulares conforme a la normatividad universitaria y nacional aplicable.

XV. Avisos Privacidad INB UNAM 2026

1. AVISO DE PRIVACIDAD INTEGRAL GENERAL DEL INB

AVISO DE PRIVACIDAD INTEGRAL
DEL INSTITUTO DE NEUROBIOLOGÍA DE LA UNAM

El Instituto de Neurobiología (INB) de la Universidad Nacional Autónoma de México (UNAM), con domicilio en Boulevard Juriquilla No. 3001, Juriquilla, Querétaro, Querétaro, C.P. 76230, es responsable del tratamiento de los datos personales que recabe en el ejercicio de sus funciones académicas, administrativas, científicas, técnicas y de prestación de servicios especializados.

Datos personales recabados

El Instituto podrá recabar, de manera enunciativa más no limitativa:

- Datos de identificación;
- Datos de contacto;
- Datos académicos;
- Datos laborales y administrativos;
- Datos fiscales y patrimoniales;
- Datos biométricos;
- Datos clínicos y de salud;
- Datos relacionados con investigación científica;
- Datos de niñas, niños y adolescentes;
- Imágenes y videograbaciones;
- Información derivada de servicios especializados.

Asimismo, podrán tratarse datos personales sensibles relacionados con:

- Neuroimagen;
- Neurodesarrollo;
- Investigación científica con sujetos humanos;
- Estudios clínicos y biomédicos;
- Expedientes laborales o administrativos.

Finalidades del tratamiento

Finalidades primarias:

- Gestión académica y administrativa;
- Registro y seguimiento de estudiantes, personal académico y administrativo;
- Integración y administración de expedientes;
- Desarrollo de actividades de investigación científica;
- Prestación de servicios especializados;
- Gestión de convenios y colaboración institucional;
- Seguridad institucional y control de acceso;

- Cumplimiento de obligaciones legales y universitarias.

Finalidades secundarias:

- Generación de estadísticas institucionales;
- Actividades de difusión académica y científica;
- Elaboración de informes institucionales;
- Encuestas de calidad y mejora de servicios.

Fundamento legal

El tratamiento de datos personales se realiza conforme a:

- Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados;
- Ley General de Transparencia y Acceso a la Información Pública;
- Ley Orgánica de la UNAM;
- Estatuto General de la UNAM;
- Lineamientos para la Protección de Datos Personales en Posesión de la UNAM;
- Normas Complementarias sobre Medidas de Seguridad Técnicas, Administrativas y Físicas.
- Transferencias

El Instituto podrá realizar transferencias de datos personales cuando:

- Exista fundamento legal;
- Sea necesario para actividades académicas, científicas o administrativas;
- Existan convenios de colaboración;
- Derive de proyectos de investigación nacionales o internacionales;
- Sea requerido por autoridad competente.

Derechos ARCO

Usted podrá ejercer sus derechos de Acceso, Rectificación, Cancelación y Oposición (ARCO), así como revocar su consentimiento, ante la Unidad de Transparencia de la UNAM.

Unidad de Transparencia de la UNAM:
https://www.transparencia.unam.mx

Cambios al aviso

El presente aviso podrá modificarse derivado de cambios normativos o institucionales. Las actualizaciones serán publicadas en:
https://www.inb.unam.mx

2. AVISO DE PRIVACIDAD SIMPLIFICADO GENERAL DEL INB

AVISO DE PRIVACIDAD SIMPLIFICADO
DEL INSTITUTO DE NEUROBIOLOGÍA DE LA UNAM

El Instituto de Neurobiología (INB) de la Universidad Nacional Autónoma de México (UNAM), con domicilio en Boulevard Juriquilla No. 3001, Juriquilla, Querétaro, Querétaro, C.P. 76230, es responsable del tratamiento de los datos personales que recabe.

Los datos personales serán utilizados para actividades académicas, administrativas, científicas, tecnológicas y de prestación de servicios especializados, incluyendo gestión institucional, investigación científica, control de acceso y cumplimiento de obligaciones universitarias y legales.

El Instituto podrá realizar transferencias de datos personales conforme a la normatividad aplicable y para el cumplimiento de finalidades institucionales legítimas.

Usted podrá ejercer sus derechos ARCO ante la Unidad de Transparencia de la UNAM.

El aviso de privacidad integral podrá consultarse en:
https://www.inb.unam.mx

El INB actualmente no cuenta con sistemas interoperables, formatos estructurados y comúnmente utilizados para permitir la portabilidad de datos personales, en términos de la normatividad aplicable.

3. AVISO DE PRIVACIDAD INTEGRAL DEL CIRCUITO CERRADO DE TELEVISIÓN (CCTV)

AVISO DE PRIVACIDAD INTEGRAL
DEL CIRCUITO CERRADO DE TELEVISIÓN (CCTV)
DEL INSTITUTO DE NEUROBIOLOGÍA DE LA UNAM

El Instituto de Neurobiología (INB) de la Universidad Nacional Autónoma de México (UNAM), con domicilio en Boulevard Juriquilla No. 3001, Juriquilla, Querétaro, Querétaro, C.P. 76230, es responsable del tratamiento de los datos personales que se obtengan mediante el sistema de Circuito Cerrado de Televisión (CCTV) instalado en sus instalaciones.

Finalidades

Los datos personales recabados mediante CCTV serán utilizados para:

- Preservar la seguridad de las personas e instalaciones;
- Controlar accesos institucionales;

- Proteger el patrimonio universitario;
- Atender incidentes de seguridad;
- Prevenir riesgos, emergencias o actos ilícitos;
- Colaborar con autoridades competentes cuando exista requerimiento fundado y motivado.

Datos recabados

- Imágenes en movimiento;
- Registros de ingreso y acceso;
- Información asociada a incidentes de seguridad.

No se requerirá consentimiento para el tratamiento de los datos personales obtenidos mediante CCTV conforme a la legislación aplicable en materia de seguridad institucional y protección de datos personales.

Transferencias

No se realizarán transferencias de datos personales, salvo aquellas necesarias para atender requerimientos de autoridad competente legalmente fundada y motivada.

Derechos ARCO

Las personas titulares podrán ejercer sus derechos ARCO ante la Unidad de Transparencia de la UNAM.

Las solicitudes relacionadas con grabaciones deberán señalar:

- Fecha;
- Hora aproximada;
- Lugar específico;
- Hechos relacionados.

Las grabaciones podrán conservarse únicamente durante el periodo institucional autorizado.

Cambios al aviso

Las actualizaciones del presente aviso serán publicadas en:

https://www.inb.unam.mx

4. AVISO DE PRIVACIDAD SIMPLIFICADO DEL CCTV

AVISO DE PRIVACIDAD SIMPLIFICADO
DEL CIRCUITO CERRADO DE TELEVISIÓN (CCTV)
DEL INSTITUTO DE NEUROBIOLOGÍA DE LA UNAM

El Instituto de Neurobiología (INB) de la Universidad Nacional Autónoma de México (UNAM), con domicilio en Boulevard Juriquilla No. 3001, Juriquilla, Querétaro, Querétaro, C.P. 76230, es responsable del tratamiento de los datos personales obtenidos mediante el sistema de Circuito Cerrado de Televisión (CCTV).

Las imágenes y registros obtenidos serán utilizados para preservar la seguridad de las personas, instalaciones y bienes universitarios, así como para control de acceso y atención de incidentes de seguridad.

No se realizarán transferencias de datos personales, salvo las previstas por la normatividad aplicable o requerimientos de autoridad competente.

Usted podrá ejercer sus derechos ARCO ante la Unidad de Transparencia de la UNAM.

El aviso de privacidad integral puede consultarse en:

https://www.inb.unam.mx

XVI. Formatos base alineados con el Documento de Seguridad de Datos Personales del INB y con enfoque institucional UNAM.

1. FORMATO GENERAL INSTITUCIONAL DE CONFIDENCIALIDAD CARTA COMPROMISO DE CONFIDENCIALIDAD Y RESPONSABILIDAD EN EL MANEJO DE DATOS PERSONALES

UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO
INSTITUTO DE NEUROBIOLOGÍA
La persona que suscribe:

Nombre: _____
Cargo / Nombramiento: _____
Área de adscripción: _____
Número de trabajador / cuenta: _____

Manifiesta que, derivado de las funciones académicas, administrativas, técnicas o de servicio que desempeña en el Instituto de Neurobiología de la UNAM, puede tener acceso a datos personales y/o datos personales sensibles contenidos en expedientes físicos, electrónicos, sistemas institucionales, plataformas tecnológicas, bases de datos o cualquier otro medio de almacenamiento institucional.

Por lo anterior, se compromete a:

1. Guardar estricta confidencialidad respecto de toda la información a la que tenga acceso.
2. Utilizar los datos personales únicamente para fines institucionales autorizados.
3. Abstenerse de divulgar, compartir, reproducir, transferir o utilizar información institucional para fines distintos a los autorizados.
4. Proteger adecuadamente documentos, expedientes, equipos, contraseñas y medios de acceso institucional.
5. Reportar inmediatamente cualquier incidente, pérdida, acceso no autorizado o vulneración de seguridad.
6. Cumplir con la normatividad universitaria y disposiciones aplicables en materia de protección de datos personales y seguridad de la información.
7. Devolver o destruir, conforme a las instrucciones institucionales, cualquier información institucional que obre en su poder al concluir su relación laboral, académica o contractual.

La presente obligación de confidencialidad subsistirá aun después de concluir la relación laboral, académica, administrativa o contractual con el Instituto.

Lugar y fecha: _____
Nombre y firma: _____
Vo. Bo. Responsable del Área: _____

2. CARTA DE RESPONSABILIDAD PARA USUARIOS DE SISTEMAS INSTITUCIONALES

CARTA DE RESPONSABILIDAD PARA EL USO DE SISTEMAS INSTITUCIONALES Y ACCESO A DATOS PERSONALES

UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO
INSTITUTO DE NEUROBIOLOGÍA

Nombre del usuario: _____
Área: _____
Sistema(s) autorizado(s): _____
Perfil de acceso: _____

La persona usuaria reconoce que el acceso a los sistemas institucionales del Instituto de Neurobiología constituye una autorización restringida y controlada para el desempeño exclusivo de funciones institucionales.

Por lo anterior, se compromete a:

1. Utilizar los sistemas institucionales únicamente para actividades autorizadas.
2. No compartir usuarios, contraseñas o credenciales de acceso.
3. Mantener contraseñas seguras y actualizadas.
4. No instalar software no autorizado en equipos institucionales.

5. No almacenar información institucional en dispositivos o plataformas personales no autorizadas.
6. Utilizar exclusivamente medios institucionales autorizados para transferencia y almacenamiento de información.
7. Mantener resguardada la información institucional a la que tenga acceso.
8. Reportar inmediatamente incidentes de seguridad, accesos indebidos o posibles vulneraciones.
9. Permitir las revisiones técnicas o auditorías institucionales que correspondan.
10. Cumplir las políticas institucionales de seguridad informática y protección de datos personales.

El incumplimiento podrá generar responsabilidades administrativas, universitarias o legales conforme a la normatividad aplicable.

Lugar y fecha: _____

Firma del usuario: _____

Vo. Bo. Área de Cómputo / Responsable del Sistema:

3. CONVENIO REFORZADO PARA DATOS PERSONALES SENSIBLES
CONVENIO DE CONFIDENCIALIDAD Y RESPONSABILIDAD PARA EL TRATAMIENTO DE DATOS PERSONALES SENSIBLES

UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO
INSTITUTO DE NEUROBIOLOGÍA
Área / Proyecto: _____
Responsable del Proyecto o Unidad: _____
Nombre del usuario autorizado: _____

La persona que suscribe reconoce que, derivado de sus actividades institucionales, tendrá acceso a información considerada como datos personales sensibles, incluyendo información clínica, biomédica, neuroimagen, datos de salud, información de menores de edad y/o información derivada de investigación con sujetos humanos.

Por lo anterior, se obliga a:

1. Utilizar la información exclusivamente para las finalidades autorizadas en el protocolo, proyecto o actividad institucional correspondiente.
2. Mantener estricta confidencialidad respecto de toda la información sensible a la que tenga acceso.
3. No copiar, descargar, fotografiar, reproducir o transferir información fuera de los medios autorizados.
4. Aplicar medidas de anonimización, seudonimización o disociación cuando corresponda.
5. Limitar el acceso únicamente a personas autorizadas.
6. Utilizar exclusivamente plataformas y sistemas institucionales autorizados.

7. Cumplir los consentimientos informados, protocolos autorizados y normatividad aplicable.
8. Notificar inmediatamente cualquier vulneración, pérdida o acceso no autorizado.
9. No conservar información sensible una vez concluida la finalidad institucional autorizada.
10. Permitir auditorías, supervisiones y revisiones institucionales relacionadas con protección de datos personales.

La obligación de confidencialidad subsistirá de manera indefinida aun después de concluir la participación en el proyecto o actividad institucional.

Lugar y fecha: _____

Firma del usuario autorizado: _____

Responsable del Área / Proyecto: _____

Vo. Bo. Responsable de Seguridad de Datos Personales:

4. CONVENIO PARA ENCARGADOS EXTERNOS
CONVENIO DE CONFIDENCIALIDAD Y TRATAMIENTO DE DATOS PERSONALES PARA ENCARGADOS EXTERNOS

UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO
INSTITUTO DE NEUROBIOLOGÍA
Proveedor / Empresa: _____
Representante: _____
Servicio contratado: _____

La persona física o moral que suscribe reconoce que, derivado de la prestación de servicios al Instituto de Neurobiología, puede tener acceso a información institucional y datos personales.

Por lo anterior, se obliga a:

1. Tratar los datos personales únicamente conforme a las instrucciones autorizadas por el Instituto.
2. No utilizar la información para fines distintos a los establecidos contractualmente.
3. Implementar medidas de seguridad equivalentes a las institucionales.
4. Garantizar la confidencialidad de la información institucional.
5. No transferir información a terceros sin autorización expresa y por escrito.
6. Informar inmediatamente cualquier incidente de seguridad o vulneración.
7. Permitir revisiones o auditorías institucionales relacionadas con seguridad de la información.
8. Destruir o devolver la información institucional una vez concluido el servicio contratado.
9. Garantizar que su personal cumpla obligaciones equivalentes de confidencialidad.

10. Cumplir la normatividad aplicable en materia de protección de datos personales.

Lugar y fecha: _____

Representante del proveedor: _____

Firma: _____

Representante del INB: _____

5. CARTA PARA ESTUDIANTES, BECARIOS Y TESISTAS

CARTA COMPROMISO DE CONFIDENCIALIDAD PARA ESTUDIANTES, BECARIOS Y TESISTAS

UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO
INSTITUTO DE NEUROBIOLOGÍA

Nombre: _____
Programa académico: _____
Laboratorio / Área: _____
Responsable académico: _____

La persona que suscribe reconoce que durante su estancia académica podrá tener acceso a información institucional y datos personales relacionados con actividades de investigación, expedientes, proyectos académicos o sistemas institucionales.

Por lo anterior, se compromete a:

1. Guardar estricta confidencialidad respecto de toda la información institucional.
2. Utilizar la información únicamente para fines académicos autorizados.
3. No compartir información, imágenes, bases de datos o documentos institucionales sin autorización.
4. Respetar las políticas institucionales de protección de datos personales y seguridad de la información.
5. No utilizar dispositivos, plataformas o medios no autorizados para almacenar información institucional.
6. Reportar incidentes o accesos indebidos que detecte.
7. Devolver cualquier documentación o información institucional al concluir su estancia.

La obligación de confidencialidad continuará aun después de concluir la estancia académica.

Lugar y fecha: _____
Nombre y firma: _____
Responsable académico: _____

UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO
INSTITUTO DE NEUROBIOLOGÍA

DOCUMENTO DE SEGURIDAD DE DATOS PERSONALES

XVII. Hoja de Autorización y Firmas

Por medio de la presente, se hace constar que el **Documento de Seguridad de Datos Personales del Instituto de Neurobiología de la Universidad Nacional Autónoma de México** ha sido revisado y validado para su presentación, de conformidad con las funciones y atribuciones correspondientes.

Para constancia y efectos administrativos, se recaban las firmas de las personas que intervienen en su autorización, revisión y seguimiento:

Dra. María Teresa Morales Guzmán
Directora del Instituto de Neurobiología

Firma: _____

MVZ Alejandro Javier Mata Acosta
Responsable de Seguridad de Datos Personales

Firma: _____

I.S.C. Ramón Martínez Olvera
Responsable de Seguridad de Datos Personales

Firma: _____

Lugar: Juriquilla, Querétaro.
Fecha: Querétaro, Querétaro a 06 de octubre de 2026.

COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

RESOLUCIÓN: CTUNAM/476/2026

FOLIO: 410031900248326

Visto el expediente relativo a la clasificación de reserva parcial de la información para la elaboración de la versión pública determinada por el **Instituto de Biotecnología**, por la **Coordinación de Universidad Abierta y Educación Digital,** por la **Secretaría General de la UNAM**, por el **Instituto de Neurobiología**, por la **Escuela Nacional Preparatoria Plantel 1 "Gabino Barreda"** , por la **Coordinación de Planeación, Evaluación y Simplificación de la Gestión Institucional**, por la **Dirección General de Asuntos del Personal Académico**, por la **Escuela Nacional de Estudios Superiores Unidad Morelia**, por el **Centro de Física Aplicada y Tecnología Avanzada**, así como por la **Dirección General de Artes Visuales**, en relación con la solicitud de acceso a la información con número de folio **410031900248326**, se procede a dictar la presente resolución con base en los siguientes:

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

I. Con fecha 10 de septiembre de 2026, a través del Sistema de Solicitudes de Acceso a la Información de la Plataforma Nacional de Transparencia, se recibió la solicitud de acceso a la información con número de folio **410031900248326**, en la que la persona solicitante requirió lo siguiente:

> *"Solicito todos los documentos de seguridad de datos personales obligatorios por ley, previa reserva de la información. Lo solicito de todas las áreas universitarias, para que no acoten las áreas, aquí las desgloso: 1. Entidades Académicas Educación Superior: 16 Facultades (en Ciudad Universitaria y áreas metropolitanas). 10 Unidades Multidisciplinarias (5 FES: Acatlán, Aragón, Cuautitlán, Iztacala, Zaragoza; más sedes/unidades asociadas). 9 Escuelas Nacionales (incluyendo ENES Juriquilla, León, Mérida, Morelia, ENAC, ENCiT, ENCiF, ENALLT y ENTS). Bachillerato: 9 planteles de la Escuela Nacional Preparatoria (ENP). 5 planteles del Colegio de Ciencias y Humanidades (CCH). Subsistema de Investigación: 36 Institutos de investigación (25 en Ciencias y 11 en Humanidades). 13 Centros de investigación (6 en Ciencias y 7 en Humanidades). 14 Programas Universitarios multidisciplinarios. Unidades académicas y de extensión regional (Morelos, Querétaro, Yucatán, Michoacán, Chiapas, etc.). 2. Dependencias Administrativas y Centrales Rectoría, Oficinas Centrales y Abogacía General. Secretarías Generales y de Apoyo: Secretaría General. Secretaría Administrativa. Secretaría de Desarrollo Institucional. Secretaría de Prevención y Apoyo a la Movilidad y Seguridad Universitaria. Secretaría de Servicio y Atención a la Comunidad Universitaria. Direcciones Generales y Coordinaciones: Más de 50 direcciones generales y coordinaciones (DGAE, DGAPA, DGCS, DGTIC, DGPe, DGPO, Deporte Universitario, Difusión Cultural con sus distintas direcciones de Danza, Música, Teatro, Artes Visuales, TV UNAM, Radio UNAM, etc.). Sedes de la UNAM en el Extranjero: 12 sedes internacionales (Centros de Estudios Mexicanos / UNAM Boston, Canadá, China, España, Francia, Alemania, UK, etc.). Servicios e Instalaciones Nacionales: Servicio Sismológico Nacional (SSN), Observatorio Astronómico Nacional (OAN), Jardín Botánico, Biblioteca y Hemeroteca Nacionales, Red Mareográfica, entre otros. Resumen La cifra aproximada a la que haces referencia (~220 a 230 unidades operativas / centros de adscripción) corresponde a la suma consolidada de todas las unidades con clave presupuestal y estructura orgánica propia (entidades académicas, planteles*

foráneos y dependencias centrales) registradas en el catálogo institucional y presupuestal de la UNAM" (sic).

II. En la solicitud de acceso a la información se estableció como modalidad de entrega de la información por medio electrónico, a través del Sistema de Solicitudes de Acceso a la Información de la Plataforma Nacional de Transparencia.

III. En cumplimiento a lo dispuesto en el punto Segundo, fracción II del Acuerdo por el que se constituyen la Unidad de Transparencia y el Comité de Transparencia de la Universidad Nacional Autónoma de México, mediante correos electrónicos de fecha 14 de septiembre de 2026, la Unidad de Transparencia remitió la solicitud de acceso a la información con número de folio **410031900248326,** entre otras áreas universitarias, al **Instituto de Biotecnología,** a la **Coordinación de Universidad Abierta y Educación Digital**, a la **Secretaría General de la UNAM**, al **Instituto de Neurobiología,** a la **Escuela Nacional Preparatoria Plantel 1 "Gabino Barreda"**, a la **Coordinación de Planeación, Evaluación y Simplificación de la Gestión Institucional,** a la **Dirección General de Asuntos del Personal Académico,** a la **Escuela Nacional de Estudios Superiores Unidad Morelia,** al **Centro de Física Aplicada y Tecnología Avanzada**, así como a la **Dirección General de Artes Visuales**.

IV. A través de correo electrónico**,** recibido con fecha 14 de septiembre de 2026, dirigido a la Presidencia del Comité de Transparencia, la **Unidad de Transparencia** solicitó la ampliación de plazo para dar respuesta.

Derivado de lo anterior, con fecha 18 de septiembre de 2026 y con fundamento en los artículos 6, apartado A de la Constitución Política de los Estados Unidos Mexicanos; 134, segundo párrafo de la Ley General de Transparencia y Acceso a la Información Pública; 1, 11, 15, fracción X y 58, fracción I del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México, se amplió el plazo para emitir la respuesta a la solicitud por 10 días más, contados a partir del día hábil siguiente a su vencimiento.

V. Mediante oficio **IBIT/D/450/2026**, recibido con fecha 18 de septiembre de 2026, dirigido a la Presidencia del Comité de Transparencia, el **Instituto de Biotecnología** señaló lo siguiente:

" l ocu e to de seguridad es el instrumento que describe y da cuenta de manera general de las medidas de seguridad técnicas, físicas y administrativas adoptadas por el responsable para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que posee un área universitaria, cuya versión se integra por siete elementos o apartados, de los cuales, por lo menos tres, se ajustan al supuesto de reserva contemplado en los artículos 29 y 30 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO); así como en los numerales 112, fracción VII en relación con el 103, fracción 1, de la Ley General de Transparencia y Acceso a la Información Pública (Ley General), ya que su divulgación obstruiría el deber de esta Universidad de establecer y mantener las medidas de seguridad

técnicas, administrativas y físicas de los datos personales que resguarda esta institución.

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

Anexos o Políticas	***Contenido y su afectación***	***Páginas***
a) *Análisis de riesgos*	*El análisis de riesgos contiene información sobre las vulnerabilidades de la infraestructura tecnológica de esta área universitaria, y otorga herramientas a las personas para implementar un ataque informático a los activos críticos y no críticos.*	***36-51***
b) *Análisis de brecha*	*El análisis de brecha integra información relativa a la seguridad de la infraestructura tecnológica; enlista los controles de seguridad con los que cuenta esta área; y menciona las herramientas que se deben adquirir para garantizar un nivel más alto de seguridad de los sistemas de información.*	***53-64***
c) *Plan de Trabajo*	*El plan de trabajo define los controles de seguridad a implementar de acuerdo con el resultado del análisis de riesgos y del análisis de brecha, priorizando las medidas de seguridad más relevantes con base en el riesgo real detectado. El uso de esta información permite inferir nuestros riesgos, por cuánto tiempo seguirán así hasta el*	***65-73***

	momento en que se implementen nuevos controles.	
d) *Acceso a las instalaciones*	*Describe los protocolos de seguridad física, los controles de ingreso, los mecanismos de identificación y las áreas restringidas donde se resguardan los soportes de datos personales. Su divulgación expone las vulnerabilidades de los accesos físicos, facilitando intrusiones no autorizadas o la sustracción de documentos e infraestructura crítica.*	***81***

Los fundamentos y motivos se exponen a continuación:

i te u rie o re l e o tr le e i entificable respecto del nexo causal que prevé la hipótesis de reserva ahora analizada contemplada en el artículo 112, fracción VII, de la Ley General, pues la información contenida en los apartados relativos al análisis de riesgo, el análisis de brecha, el plan de trabajo y acceso a las instalaciones de esta dependencia contiene información sobre la forma en que de cómo se protegen los datos personales de los titulares que nos confiaron su información personal y que es nuestra responsabilidad garantizar. Es un riesgo real el hecho de que toda persona que quiera ocasionar la pérdida, destrucción, robo, copia, uso, acceso o tratamiento no autorizado, daño, alteración o modificación no autorizada de datos personales, podría hacerlo si cuenta con la información exacta de las vulnerabilidades de un área universitaria, información que esta serie de documentos les otorga directamente si se difundiera la información.

i ul r el li i e rie o el li i e rec el pl e tr jo y los controles de acceso a las instalaciones evidencia los nuevos controles que estamos pendientes de implementar, describen la forma en que almacenamos técnicamente los datos personales, cómo protegemos los sistemas automatizados de información, qué medidas de seguridad administrativas, físicas y técnicas planeamos establecer de manera gradual y de conformidad con las prioridades y los presupuestos otorgado.

e te e ti o l re el ci e l i or ci ue o r e el li i e riesgos, el análisis de brecha, el plan de trabajo y los controles de acceso de esta área revela y hace identificables las formas en que es posible atacar o vulnerar nuestros sistemas de información que resguardan datos personales

que obran en nuestros archivos y dejaría imposibilitada a esta área para reaccionar ante posibles amenazas.

La prueba de daño precitada, colma los extremos establecidos en las tres fracciones del artículo 107 de la Ley General de Transparencia y Acceso a la Información Pública; dado que podrá considerarse como información reservada aquella que obstruya la prevención de delitos al obstaculizar las acciones implementadas por las autoridades para evitar su comisión, o menoscabar o limitar la capacidad de estas para evitar la comisión de delitos.

En esa inteligencia, el dar a conocer el análisis de riesgos, el análisis de brecha y el plan de trabajo de esta área universitaria, afectaría la prevención de actos ilícitos que pudieran realizarse en contra de los sistemas de información y de tratamiento de datos personales, así como en contra de los activos e infraestructura crítica de esta dependencia; por lo que es posible advertir que algunas de las posibles consecuencias de divulgar dicha información podrían derivar en la comisión de diversos delitos tipificados en el Código Penal Federal, como acceso no autorizado a los sistemas, el robo de información, la suplantación de identidad, entre otros. Es decir, se advierte que la negativa de acceso a la información se motiva en evitar o prevenir la comisión de delitos al no revelar las vulnerabilidades de las medidas de seguridad establecidas por esta Área Universitaria, con relación al cumplimiento de los principios de protección de datos personales previstos en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

En tal sentido, proteger la información de los documentos relativos al análisis de riesgos, al análisis de brecha y al plan de trabajo de esta área se adecua al principio de proporcionalidad y se justifica negar su divulgación, toda vez que la pretensión de fondo que persigue la reserva de la información consiste en prevenir las conductas antijurídicas tipificadas, aunado a que la restricción es temporal, hasta en tanto las medidas implementadas caduquen o bien se implementen otras diversas. De igual manera, con la no divulgación de la información se contribuye a garantizar la protección de los datos personales de la comunidad universitaria, así como de cualquier persona que deposite su confianza en esta Universidad para resguardar sus datos personales.

Por tales motivos, se propone la reserva total de cada uno de esos apartados del documento de seguridad de esta área universitaria, por un periodo de 5 años, de conformidad con el segundo párrafo del artículo 104 de la Ley General, plazo considerado como necesario para la adecuada salvaguarda de la información aludida, atendiendo a que es el lapso promedio que se tiene contemplado para realizar alguna modificación sustancial o actualización del Documento de Seguridad en cita.

En virtud de lo anterior, le solicito de la manera más atenta que ese Cuerpo Colegiado tenga a bien emitir la resolución que en derecho corresponda, para lo cual se adjunta la documentación completa" (sic)

VI. Por oficio **CUAED/UJ/ADLRG/311/2026**, recibido con fecha 23 de septiembre de 2026, dirigido a la Presidencia del Comité de Transparencia, la **Coordinación de Universidad Abierta y Educación Digital** refirió lo siguiente:

> *“ l ocu e to e uri e el i tru e to ue e cri e cue t e manera general de las medidas de seguridad técnicas, físicas y administrativas adoptadas por el responsable para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que posee un área universitaria, cuya versión se integra por siete elementos o apartados, de los cuales, por lo menos tres, se ajustan al supuesto de reserva contemplado en los artículos 29 y 30 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO); así como en los numerales 112, fracción VII en relación con el 103, fracción 1, de la Ley General de Transparencia y Acceso a la Información Pública (Ley General), ya que su divulgación obstruiría el deber de esta Universidad de establecer y mantener las medidas de seguridad técnicas, administrativas y físicas de los datos personales que resguarda esta institución.*
>
> *A efecto de cumplir con lo señalado, se realiza la siguiente prueba de daño relativa al documento de seguridad de datos personales que obra en el Sistema de Gestión de Seguridad de Datos Personales de esta área universitaria. El documento de seguridad contiene los siguientes apartados, cuya autorización de reserva total se solicita a ese Comité:*

Anexos o Políticas	***Contenido y su afectación***	***Páginas***
a. *Estructura y descripción de los sistemas de tratamientos de datos personales*	*Las características del lugar donde se resguardan los soportes identifican el espacio físico, virtual y los controles de acceso para las fuentes de información de cada sistema informático*	***239***
b. *Análisis de riesgos*	*El análisis de riesgos contiene información sobre las vulnerabilidades de la infraestructura tecnológica de esta área universitaria, y otorga herramientas a las personas para implementar un ataque informático a los activos críticos y no críticos.*	
c. *Análisis de brecha*	*El análisis de brecha integra información relativa a la seguridad de*	

	la infraestructura tecnológica; enlista los controles de seguridad con los que cuenta esta área; y menciona las herramientas que se deben adquirir para garantizar un nivel más alto de seguridad de los sistemas de información.	
d. *Plan de Trabajo*	*El plan de trabajo define los controles de seguridad a implementar de acuerdo con el resultado del análisis de riesgos y del análisis de brecha, priorizando las medidas de seguridad más relevantes con base en el riesgo real detectado. El uso de esta información permite inferir nuestros riesgos, por cuánto tiempo seguirán así hasta el momento en que se implementen nuevos controles.*	
e. *Acceso a las instalaciones*	*El acceso a las instalaciones permite identificar los caminos, físicos, horarios, o áreas de la CUAED por las cuáles se podría vulnerar la seguridad en la dependencia.*	
f. *Mecanismos de Monitoreo y Revisión de las medidas de seguridad*	*Todos los mecanismos de monitoreo y revisión de las medidas de seguridad implementadas permiten identificar lo que se ha realizado y los resultados de estas acciones, lo que permite realizar ingeniería inversa para identificar brechas o riesgos y poder explotarlos.*	

Los fundamentos y motivos se exponen a continuación:

i te u rie o re l e o tr le e i e ti ic le re pecto el e o c u l ue prevé la hipótesis de reserva ahora analizada contemplada en el artículo 112, fracción VII, de la Ley General, pues la información contenida en los apartados relativos al análisis de riesgo, el análisis de brecha, el plan de trabajo, acceso a las instalaciones y mecanismos de monitoreo y revisión de las medidas de seguridad de esta dependencia contiene información sobre la forma en que de cómo se protegen los datos personales de los titulares que nos confiaron su información personal y que es nuestra responsabilidad garantizar. Es un riesgo real el hecho de que toda persona que quiera ocasionar la pérdida, destrucción, robo, copia, uso, acceso o tratamiento no autorizado, daño, alteración o modificación no autorizada de datos personales, podría hacerlo si cuenta con la información exacta de las vulnerabilidades de un área universitaria, información que esta serie de documentos les otorga directamente si se difundiera la información.

i ul r la estructura y descripción de los sistemas de tratamientos de datos personales, el análisis de riesgo, el análisis de brecha, el plan de trabajo, acceso a las instalaciones y mecanismos de monitoreo y revisión de las medidas de seguridad de esta dependencia evidencian los trayectos y áreas físicas vulnerables, los nuevos controles que estamos pendientes de implementar, describen la forma en cómo almacenamos técnicamente los datos personales, los controles y claves de acceso al centro de datos, cómo protegemos los sistemas automatizados de información, qué medidas de seguridad administrativas, físicas y técnicas planeamos establecer de manera gradual y de conformidad con las prioridades y presupuestos otorgado.

En este sentido la revelación de la información que obra estructura y descripción de los sistemas de tratamientos de datos personales, análisis de riesgo, el análisis de brecha, el plan de trabajo, acceso a las instalaciones y mecanismos de monitoreo y revisión de las medidas de seguridad de esta dependencia revela y hace identificable las formas en que es posible atacar o vulnerar física o lógicamente nuestros sistemas de información que resguardan datos personales que obran en nuestros archivos y dejaría imposibilitada a esta dependencia para reaccionar ante posibles amenazas.

La prueba de daño precitada, colma los extremos establecidos en las tres fracciones del artículo 107 de la Ley General de Transparencia y Acceso a la Información Pública; dado que podrá considerarse como información reservada aquella que obstruya la prevención de delitos al obstaculizar las acciones implementadas por las autoridades para evitar su comisión, o menoscabar o limitar la capacidad de estas para evitar la comisión de delitos.

En esa inteligencia, el dar a conocer la estructura y descripción de los sistemas de tratamientos de datos personales, el análisis de riesgo, el análisis de brecha, el plan de trabajo, acceso a las instalaciones y mecanismos de monitoreo y revisión de las medidas de seguridad de esta área universitaria, afectaría la prevención de actos ilícitos que pudieran realizarse en contra de los sistemas de información y tratamiento de datos personales, así como en contra de los activos e infraestructura crítica de esta dependencia; por lo que es

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

En tal sentido, proteger la información de los documentos relativos a la estructura y descripción de los sistemas de tratamientos de datos personales, el análisis de riesgo, el análisis de brecha, el plan de trabajo, acceso a las instalaciones y mecanismos de monitoreo y revisión de las medidas de seguridad de esta área se adecua al principio de proporcionalidad y se justifica negar su divulgación, toda vez que la pretensión de fondo que persigue la reserva de la información consiste en prevenir las conductas antijurídicas tipificadas, aunado a que la restricción es temporal, hasta en tanto las medidas tomadas caduquen, o bien, se implementen otras diversas; de igual manera, con la no divulgación de la información se contribuye a garantizar la protección de los datos personales de la comunidad universitaria, así como de cualquiera que ponga la confianza en esta Universidad para resguardar sus datos personales.

Por tales motivos, respetuosamente, se propone la reserva total de cada uno de esos apartados del documento de seguridad de esta área universitaria, por un periodo de 5 años, de conformidad con el segundo párrafo del artículo 104 de la Ley General, plazo considerado como necesario para la adecuada salvaguarda de la información aludida, atendiendo a que es el lapso promedio que se tiene contemplado para alguna modificación sustancial o actualización del Documento de Seguridad en cita.

En virtud de lo anterior, le solicito de la manera más atenta que ese Cuerpo Colegiado tenga a bien emitir la resolución que en derecho corresponda, para lo cual se adjunta la documentación completa" (sic)

VII. Mediante el oficio **SGEN/ET/015/2026**, recibido con fecha 24 de septiembre de 2026, dirigido a la Presidencia del Comité de Transparencia, la **Secretaría General de la UNAM** informó lo siguiente:

"El documento de seguridad es el instrumento que describe y da cuenta de manera general sobre las medidas de seguridad técnicas, físicas y administrativas adoptadas por el responsable para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que posee un área universitaria; cuya versión se integra de siete elementos o apartados, de los cuales, por lo menos tres, se ajustan al supuesto de reserva contemplado en los artículos 29 y 30 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO) y 112, fracción VII

en relación con el 103, fracción I, de la Ley General de Transparencia y Acceso a la Información Pública (Ley General), ya que su divulgación obstruiría el deber de esta Secretaría de mantener las medidas de seguridad técnicas, administrativas y físicas de los datos personales que resguarda.

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

Anexos o Políticas	***Contenido y su afectación***	***Páginas***
a) *Análisis de riesgos*	*El análisis de riesgos contiene información sobre las vulnerabilidades de la infraestructura tecnológica de esta área universitaria, y otorga herramientas a las personas para implementar un ataque informático a los activos críticos y no críticos.*	*48 a 50*
b) *Análisis de brecha*	*El análisis de brecha integra información relativa a la seguridad de la infraestructura tecnológica; enlista los controles de seguridad con los que cuenta esta área; y menciona las herramientas que se deben adquirir para garantizar un nivel más alto de seguridad de los sistemas de información.*	*54 a 57*
c) *Plan de Trabajo*	*El plan de trabajo define los controles de seguridad a implementar de acuerdo con el resultado del análisis de riesgos y del análisis de brecha, priorizando las medidas de seguridad más relevantes con base en el riesgo real detectado. El uso de esta información permite inferir nuestros*	*59 a 73*

	riesgos, por cuánto tiempo seguirán así hasta el momento en que se implementen nuevos controles.	

Los fundamentos y motivos se exponen a continuación:

Existe un riesgo real. demostrable e identificable en perjuicio del nexo causal que prevé la hipótesis de reserva ahora analizada contemplada en el artículo 112, fracción VII, de la Ley General, la información contenida en los apartados relativos al análisis de riesgo, el análisis de brecha y el plan de trabajo de esta Secretaría contienen información de cómo se protegen los datos personales de los titulares que nos confiaron su información personal y que es nuestra responsabilidad garantizar. Es un riesgo real el hecho de que toda persona que quiera ocasionar la pérdida, destrucción, robo, copia, uso, acceso o tratamiento no autorizado, daño, alteración o modificación no autorizada de datos personales, puede hacerlo si cuenta con la información exacta de las vulnerabilidades de un área universitaria.

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

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

La prueba de daño precitada, colma los extremos establecidos en las tres fracciones del artículo 107 de la Ley General de Transparencia y Acceso a la Información Pública; dado que podrá considerarse como información reservada aquélla que obstruya la prevención de delitos al obstaculizar las acciones implementadas por las autoridades para evitar su comisión, o menoscabar o limitar la capacidad de estas para evitar la comisión de delitos.

En esa inteligencia, el dar a conocer el análisis de riesgo, el análisis de brecha y el plan de trabajo de esta Secretaría, afectaría la prevención de actos ilícitos que pudieran realizarse en contra de los sistemas de información y tratamiento de datos personales, así como en contra de los activos e infraestructura crítica de esta; por lo que es posible advertir que algunas de las posibles consecuencias de divulgar dicha información podrían derivar en la comisión de diversos delitos tipificados en el Código Penal Federal, como accesos no

autorizados a los sistemas, robos de información, suplantación de identidades, entre otros. Es decir, se advierte que la negativa de acceso a la información se motiva en evitar o prevenir la comisión del delito al no revelar las vulnerabilidades de las medidas de seguridad establecidas por esta Secretaría, con relación al cumplimiento de los principios de protección de datos personales previsto en la LGPDPPSO.

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

Por tales motivos, respetuosamente, se propone la reserva total de cada uno de esos apartados del documento de seguridad de esta Secretaría, por un periodo de 5 años, de conformidad con el segundo párrafo del artículo 104 de la Ley General, plazo considerado como necesario para la adecuada salvaguarda de la información aludida, atendiendo a que es el lapso promedio que se tiene contemplado para alguna modificación sustancial o actualización del Documento de Seguridad en cita.

En virtud de lo anterior, le solicito de la manera más atenta que ese Cuerpo Colegiado tenga a bien emitir la resolución que en derecho corresponda, para lo cu l e ju t l ocu e t ci co plet " (sic).

VIII. Por oficio **INEU/D/598/2026**, recibido con fecha 28 de septiembre de 2026, dirigido a la Presidencia del Comité de Transparencia, el **Instituto de Neurobiología** informó lo siguiente:

"El documento de seguridad es el instrumento que describe y da cuenta de manera general sobre las medidas de seguridad técnicas, físicas y administrativas adoptadas por el responsable para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que posee un área universitaria; cuyo contenido comprende diversos elementos o apartados, de los cuales al menos tres se ajustan al supuesto de reserva contemplado en los artículos 29 y 30 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados1 (LGPDPPSO) y 112, fracción Vll2 en relación con el 103, fracción 13, de la Ley General de Transparencia y Acceso a la Información Pública4 (Ley General), ya que su divulgación obstruiría el deber de esta Universidad de establecer y mantener las medidas de seguridad técnicas, administrativas y físicas de los datos personales que resguarda esta institución.

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

Anexos o Políticas	***Contenido y su afectación***	***Páginas***
a. Análisis de riesgos	*El análisis de riesgos contiene información sobre las vulnerabilidades de la infraestructura tecnológica del INB, y otorga herramientas a las personas para implementar un ataque informático a los activos críticos v no críticos.*	*36-41*
b. Análisis de brecha	*El análisis de brecha integra información relativa a la seguridad de la infraestructura tecnológica; enlista los controles de seguridad con los que cuenta esta área; y menciona las herramientas que se deben adquirir para garantizar un nivel más alto de seguridad de los sistemas de información. Es decir, detalla diferencias entre los controles existentes y los requeridos; identifica deficiencias administrativas, físicas y técnicas, así como necesidades de fortalecimiento, herramientas y controles pendientes de implementar.*	*42-46*
c. Plan de Trabajo	*El plan de trabajo define los controles de seguridad a implementar de acuerdo con el resultado del análisis de riesgos y del análisis de brecha,*	*46-51*

	priorizando las medidas de seguridad más relevantes con base en el riesgo real detectado. El uso de esta información permite inferir nuestros riesgos, por cuánto tiempo seguirán así hasta el momento en que se implementen nuevos controles.	
d. Inventario de Sistemas de Tratamiento de Datos Personales	*En el inventario de sistemas de tratamiento de datos personales se identifican sistemas físicos y electrónicos, áreas responsables, tipos de datos, medios de almacenamiento, transferencias y niveles de riesgo. Su divulgación permitiría ubicar activos, sistemas prioritarios y puntos de exposición institucional.*	*32-36*

Los fundamentos y motivos se exponen a continuación:

i te u riesgo real, demostrable e identificable en perjuicio del nexo causal que prevé la hipótesis de reserva ahora analizada contemplada en el artículo 112, fracción VII, de la Ley General. La información contenida en los apartados relativos al análisis de riesgo, el análisis de brecha, el plan de trabajo y el inventario de sistemas de tratamiento de datos personales del INB describe cómo se protegen los datos personales que los titulares han confiado al Instituto y cuya seguridad es nuestra responsabilidad garantizar. Es un riesgo real el hecho de que toda persona que quiera ocasionar la pérdida, destrucción, robo, copia, uso, acceso o tratamiento no autorizado, daño, alteración o modificación no autorizada de datos personales, puede hacerlo si cuenta con la información exacta de las vulnerabilidades de un área universitaria, lo que esta serie de documentos les otorga directamente si se difundiera la información.

i ul r el li i e rie o el li i e rec el plan de trabajo y el inventario de sistemas de tratamiento de datos personales del INB evidencia los nuevos controles pendientes de implementar, describen la forma en que almacenamos técnicamente los datos personales, cómo protegemos los sistemas automatizados de información, qué medidas de seguridad administrativas, físicas y técnicas planeamos establecer de manera gradual y de conformidad con las prioridades y recursos presupuestales otorgados.

e te e ti o l re el ci e l i or ci ue o ra en el análisis de riesgo, el análisis de brecha, el plan de trabajo y el inventario de sistemas de

tratamiento de datos personales del INB revela y hace identificable la forma en que es posible atacar o vulnerar nuestros sistemas de información que resguardan datos personales que obran en nuestros archivos y limitaría la capacidad de esta área para reaccionar ante posibles amenazas.

La prueba de daño precitada, colma los extremos establecidos en las tres fracciones del artículo 107 de la Ley General de Transparencia y Acceso a la Información Pública; dado que podrá considerarse como información reservada aquélla que obstruya la prevención de delitos al obstaculizar las acciones implementadas por las autoridades para evitar su comisión, o menoscabar o limitar la capacidad de estas para evitar la comisión de delitos.

En esa inteligencia, el dar a conocer el análisis de riesgo, el análisis de brecha, el plan de trabajo y el inventario de sistemas de tratamiento de datos personales del INB afectaría la prevención de actos ilícitos que pudieran realizarse en contra de los sistemas de información y tratamiento de datos personales, así como en contra de los activos e infraestructura crítica del INB; por lo que es posible advertir que algunas de las posibles consecuencias de divulgar dicha información podrían derivar en la comisión de diversos delitos tipificados en el Código Penal Federal, como accesos no autorizados a los sistemas, robos de información, suplantación de identidades, entre otros. Es decir, se advierte que la negativa de acceso a la información se motiva en evitar o prevenir la comisión del delito al no revelar las vulnerabilidades de las medidas de seguridad establecidas por esta Área Universitaria, con relación al cumplimiento de los principios de protección de datos personales previstos en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

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

Por tales motivos, respetuosamente, se propone la reserva total de cada uno de esos apartados del documento de seguridad de esta área universitaria, por un periodo de cinco años, de conformidad con el segundo párrafo del artículo 104 de la Ley General, plazo considerado como necesario para la adecuada salvaguarda de la información aludida, atendiendo a que es el lapso promedio que se ha previsto para alguna modificación sustancial o actualización del Documento de Seguridad en cita.

En virtud de lo anterior, le solicito atentamente que ese Cuerpo Colegiado tenga a bien emitir la resolución que en derecho corresponda, para lo cual se adjunta la documentación completa." (sic).

IX. A través del oficio **ENP-1/D/289/2026**, recibido con fecha 29 de septiembre de 2026, dirigido a la Presidencia del Comité de Transparencia, la **Escuela Nacional Preparatoria Plantel 1 "Gabino Barreda"** notificó lo siguiente:

"Por medio del presente y derivado de la Solicitud de Información con folio 410031900248326 enviada a esta Escuela Nacional Preparatoria Plantel 1 i o rre e per ito e i r el ocu e to e e uridad el cual es el instrumento que describe y da cuenta de manera general sobre las medidas de seguridad técnicas, físicas y administrativas adoptadas por el responsable para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que posee un área universitaria; cuya versión se integra de siete elementos o apartados, de los cuales, por lo menos tres, se ajustan al supuesto de reserva contemplado en los artículos 29 y 30 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO) y 112, fracción VII en relación con el 103, fracción I, de la Ley General de Transparencia y Acceso a la Información Pública (Ley General), ya que su divulgación obstruiría el deber de esta Universidad de establecer y mantener las medidas de seguridad técnicas, administrativas y físicas de los dalos personales que resguarda esta institución.

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

Anexos o Políticas	***Contenido y su afectación***	***Páginas***
a) *Análisis de riesgos*	*El análisis de riesgos contiene información sobre las vulnerabilidades de la infraestructura tecnológica de esta área universitaria, y otorga herramientas a las personas para implementar un ataque informático a los activos críticos y no críticos.*	***62-65***
b) *Análisis de brecha*	*El análisis de brecha integra información relativa a la seguridad de la infraestructura tecnológica; enlista los controles de seguridad*	***65-67***

	con los que cuenta esta área; y menciona las herramientas que se deben adquirir para garantizar un nivel más alto de seguridad de los sistemas de información.	
***c)** Plan de Trabajo*	*El plan de trabajo define los controles de seguridad a implementar de acuerdo con el resultado del análisis de riesgos y del análisis de brecha, priorizando las medidas de seguridad más relevantes con base en el riesgo real detectado. El uso de esta información permite inferir nuestros riesgos, por cuánto tiempo seguirán así hasta el momento en que se implementen nuevos controles.*	***67-68***

Los fundamentos y motivos se exponen a continuación:

i te u riesgo real, demostrable e identificable en perjuicio del nexo causal que prevé la hipótesis de reserva ahora analizada contemplada en el artículo 112, fracción VII, de la Ley General, la información contenida en los apartados relativos al análisis de riesgo, el análisis de brecha, y el plan de trabajo de esta dependencia contienen información de cómo se protegen los datos personales de los titulares que nos confiaron su información personal y que es nuestra responsabilidad garantizar. Es un riesgo real el hecho de que toda persona que quiera ocasionar la pérdida, destrucción, robo, copia, uso, acceso o tratamiento no autorizado, daño, alteración o modificación no autorizada de datos personales, puede hacerlo si cuenta con la información exacta de las vulnerabilidades de un área universitaria, lo que esta serie de documentos les otorga directamente si se difundiera la información.

i ul r el li i e rie o el li i e rec , y el plan de trabajo de esta dependencia evidencian los nuevos controles que estamos pendientes de implementar, describen la forma en cómo almacenamos técnicamente los datos personales, cómo protegemos los sistemas automatizados de información, qué medidas de seguridad administrativas, físicas y técnicas planeamos establecer de manera gradual y de conformidad con las prioridades y presupuestos otorgado.

e te e ti o l re el ci e l i or ci ue o r el li i e rie o el análisis de brecha y el plan de trabajo de esta área revela y hace identificable las formas en que es posible atacar o vulnerar nuestros sistemas de información que resguardan datos personales que obran en nuestros archivos y dejaría imposibilitada a esta área para reaccionar ante posibles amenazas.

La prueba de daño precitada, colma los extremos establecidos en las tres fracciones del artículo 107 de la Ley General de Transparencia y Acceso a la Información Pública; dado que podrá considerarse como información reservada aquélla que obstruya la prevención de delitos al obstaculizar las acciones implementadas por las autoridades para evitar su comisión, o menoscabar o limitar la capacidad de estas para evitar la comisión de delitos.

En esa inteligencia, el dar a conocer el análisis de riesgo, el análisis de brecha y el plan de trabajo de esta área universitaria, afectaría la prevención de actos ilícitos que pudieran realizarse en contra de los sistemas de información y tratamiento de datos personales, así como en contra de los activos e infraestructura crítica de esta dependencia; por lo que es posible advertir que algunas de las posibles consecuencias de divulgar dicha información podrían derivar en la comisión de diversos delitos tipificados en el Código Penal Federal, como accesos no autorizados a los sistemas, robos de información, suplantación de identidades, entre otros. Es decir, se advierte que la negativa de acceso a la información se motiva en evitar o prevenir la comisión del delito al no revelar las vulnerabilidades de las medidas de seguridad establecidas por esta Área Universitaria, con relación al cumplimiento de los principios de protección de datos personales previsto en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

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

Por tales motivos, respetuosamente, se propone la reserva total de cada uno de esos apartados del documento de seguridad de esta área universitaria, por un periodo de 5 años, de conformidad con el segundo párrafo del artículo 104 de la Ley General, plazo considerado como necesario para la adecuada salvaguarda de la información aludida, atendiendo a que es el lapso promedio que se tiene contemplado para alguna modificación sustancial o actualización del Documento de Seguridad en cita.

En virtud de lo anterior, le solicito de la manera más atenta que ese Cuerpo Colegiado tenga a bien emitir la resolución que en derecho corresponda, para lo cu l e ju t l ocu e t ci co plet " (sic).

X. Mediante oficios **CPESGI/0453/2026, DGAP/DG/DSDIA/1710/2026**, **CFAT/D/285/2026** y **DGAV/D/3074/2026**, recibidos con fechas 29 y 30 de septiembre, así como 6 de octubre de 2026, dirigidos a la Presidencia del Comité de Transparencia, la **Coordinación de Planeación, Evaluación y Simplificación de la Gestión Institucional**, la **Dirección General de Asuntos del Personal Académico**, el **Centro de Física Aplicada y Tecnología Avanzada**, así como la **Dirección General de Artes Visuales** informaron lo siguiente:

"El documento de seguridad es el instrumento que describe y da cuenta de manera general sobre las medidas de seguridad técnicas, físicas y administrativas adoptadas por el responsable para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que posee un área universitaria; cuya versión se integra de siete elementos o apartados, de los cuales, por lo menos tres, se ajustan al supuesto de reserva contemplado en los artículos 29 y 30 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO) y 112, fracción VII en relación con el 103, fracción I, de la Ley General de Transparencia y Acceso a la Información Pública4 (Ley General), ya que su divulgación obstruiría el deber de esta Universidad de establecer y mantener las medidas de seguridad técnicas, administrativas y físicas de los datos personales que resguarda esta institución.

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

Anexos o Políticas	***Contenido y su afectación***	***Páginas***
… *Análisis de riesgos*	*El análisis de riesgos contiene información sobre las vulnerabilidades de la infraestructura tecnológica de esta área universitaria, y otorga herramientas a las personas para implementar un ataque informático a los activos críticos y no críticos.*	
… *Análisis de brecha*	*El análisis de brecha integra información relativa a la seguridad de la infraestructura*	

	tecnológica; enlista los controles de seguridad con los que cuenta esta área; y menciona las herramientas que se deben adquirir para garantizar un nivel más alto de seguridad de los sistemas de información.	
***…** Plan de Trabajo*	*El plan de trabajo define los controles de seguridad a implementar de acuerdo con el resultado del análisis de riesgos y del análisis de brecha, priorizando las medidas de seguridad más relevantes con base en el riesgo real detectado. El uso de esta información permite inferir nuestros riesgos, por cuánto tiempo seguirán así hasta el momento en que se implementen nuevos controles.*	

Los fundamentos y motivos se exponen a continuación:

Existe un riesgo real, demostrable e identificable en perjuicio del nexo causal que prevé la hipótesis de reserva ahora analizada contemplada en el artículo 112, fracción VII, de la Ley General, la información contenida en los apartados relativos al análisis de riesgo, el análisis de brecha, y el plan de trabajo de esta dependencia contienen información de cómo se protegen los datos personales de los titulares que nos confiaron su información personal y que es nuestra responsabilidad garantizar. Es un riesgo real el hecho de que toda persona que quiera ocasionar la pérdida, destrucción, robo, copia, uso, acceso o tratamiento no autorizado, daño, alteración o modificación no autorizada de datos personales, puede hacerlo si cuenta con la información exacta de las vulnerabilidades de un área universitaria, lo que esta serie de documentos les otorga directamente si se difundiera la información.

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

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

La prueba de daño precitada, colma los extremos establecidos en las tres fracciones del artículo 107 de la Ley General de Transparencia y Acceso a la Información Pública; dado que podrá considerarse como información reservada aquélla que obstruya la prevención de delitos al obstaculizar las acciones implementadas por las autoridades para evitar su comisión, o menoscabar o limitar la capacidad de estas para evitar la comisión de delitos.

En esa inteligencia, el dar a conocer el análisis de riesgo, el análisis de brecha y el plan de trabajo de esta área universitaria, afectaría la prevención de actos ilícitos que pudieran realizarse en contra de los sistemas de información y tratamiento de datos personales, así como en contra de los activos e infraestructura crítica de esta dependencia; por lo que es posible advertir que algunas de las posibles consecuencias de divulgar dicha información podrían derivar en la comisión de diversos delitos tipificados en el Código Penal Federal, como accesos no autorizados a los sistemas, robos de información, suplantación de identidades, entre otros. Es decir, se advierte que la negativa de acceso a la información se motiva en evitar o prevenir la comisión del delito al no revelar las vulnerabilidades de las medidas de seguridad establecidas por esta Área Universitaria, con relación al cumplimiento de los principios de protección de datos personales previsto en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

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

Por tales motivos, respetuosamente, se propone la reserva total de cada uno de esos apartados del documento de seguridad de esta área universitaria, por un periodo de 5 años, de conformidad con el segundo párrafo del artículo 104 de la Ley General, plazo considerado como necesario para la adecuada salvaguarda de la información aludida, atendiendo a que es el lapso promedio que se tiene contemplado para alguna modificación sustancial o actualización del Documento de Seguridad en cita.

En virtud de lo anterior, le solicito de la manera más atenta que ese Cuerpo Colegiado tenga a bien emitir la resolución que en derecho corresponda, para lo cu l e ju t l ocu e t ci co plet " (sic).

XI. Por oficio **ENESM/ST/TRANS/023/2026**, recibido con fecha 2 de octubre de 2026, dirigido a la Presidencia del Comité de Transparencia, la **Escuela Nacional de Estudios Superiores Unidad Morelia** notificó lo siguiente:

"El documento de seguridad es el instrumento que describe y da cuenta de manera general sobre las medidas de seguridad técnicas, físicas y administrativas adoptadas por el responsable para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que posee un área universitaria; cuya versión se integra de siete elementos o apartados, de los cuales, por lo menos tres, se ajustan al supuesto de reserva contemplado en los artículos 29 y 30 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO) y 112, fracción VII en relación con el 103, fracción I, de la Ley General de Transparencia y Acceso a la Información Pública (Ley General), ya que su divulgación obstruiría el deber de esta Universidad de establecer y mantener las medidas de seguridad técnicas, administrativas y físicas de los datos personales que resguarda esta institución.

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

Anexos o Políticas	***Contenido y su afectación***	***Páginas***
a) *Análisis de riesgos*	*El análisis de riesgos contiene información sobre las vulnerabilidades de la infraestructura tecnológica de esta área universitaria, y otorga herramientas a las personas para implementar un ataque informático a los activos críticos y no críticos.*	*12, 38, 68, 95, 117, 140, 164, 189, 214, 237, 271, 300, 326*
b) *Análisis de brecha*	*El análisis de brecha integra información relativa a la seguridad de la infraestructura tecnológica; enlistan los controles de seguridad con los que cuenta esta área; y menciona las*	*13, 39, 69, 95, 118, 142, 165, 190, 215,*

	herramientas que se deben adquirir para garantizar un nivel más alto de seguridad de los sistemas de información.	
c) *Plan de Trabajo*	*El plan de trabajo define los controles de seguridad a implementar de acuerdo con el resultado del análisis de riesgos y del análisis de brecha, priorizando las medidas de seguridad más relevantes con base en el riesgo real detectado. El uso de esta información permite inferir nuestros riesgos, por cuánto tiempo seguirán así hasta el momento en que se implementen nuevos controles.*	*14, 40, 70, 96, 118, 142, 166, 191, 216, 240, 274, 303, 330.*
d) *Características del lugar donde se resguardan los soportes.*	*El apartado de Características del lugar donde se resguardan los soportes de cada sistema contiene información relativa a la seguridad de la infraestructura tecnológica y los controles de seguridad con los que cuenta esta área.*	*11, 37, 67, 94, 117, 140, 164, 188, 214, 236, 270, 300, 326.*

Los fundamentos y motivos se exponen a continuación:

i te u riesgo real, demostrable e identificable en perjuicio del nexo causal que prevé la hipótesis de reserva ahora analizada contemplada en el artículo 112, fracción VII, de la Ley General, la información contenida en los apartados relativos al análisis de riesgo, el análisis de brecha, y el plan de trabajo de esta dependencia contienen información de cómo se protegen los datos personales de los titulares que nos confiaron su información personal y que es nuestra responsabilidad garantizar. Es un riesgo real el hecho de que toda persona que quiera ocasionar la pérdida, destrucción, robo, copia, uso, acceso o tratamiento no autorizado, daño, alteración o modificación no autorizada de datos personales, puede hacerlo si cuenta con la información exacta de las vulnerabilidades de un área universitaria, lo que esta serie de documentos les otorga directamente si se difundiera la información.

i ul r el li i e rie o el análisis de brecha, y el plan de trabajo de esta dependencia evidencian los nuevos controles que estamos pendientes de implementar, describen la forma en cómo almacenamos técnicamente los datos personales, cómo protegemos los sistemas automatizados de información, qué medidas de seguridad administrativas, físicas y técnicas planeamos establecer de manera gradual y de conformidad con las prioridades y presupuestos otorgado.

e te e ti o l re el ci e l i or ci ue o r el li i e rie o el análisis de brecha y el plan de trabajo de esta área revela y hace identificable las formas en que es posible atacar o vulnerar nuestros sistemas de información que resguardan datos personales que obran en nuestros archivos y dejaría imposibilitada a esta área para reaccionar ante posibles amenazas.

La prueba de daño precitada, colma los extremos establecidos en las tres fracciones del artículo 107 de la Ley General de Transparencia y Acceso a la Información Pública; dado que podrá considerarse como información reservada aquélla que obstruya la prevención de delitos al obstaculizar las acciones implementadas por las autoridades para evitar su comisión, o menoscabar o limitar la capacidad de estas para evitar la comisión de delitos.

En esa inteligencia, el dar a conocer el análisis de riesgo, el análisis de brecha y el plan de trabajo de esta área universitaria, afectaría la prevención de actos ilícitos que pudieran realizarse en contra de los sistemas de información y tratamiento de datos personales, así como en contra de los activos e infraestructura crítica de esta dependencia; por lo que es posible advertir que algunas de las posibles consecuencias de divulgar dicha información podrían derivar en la comisión de diversos delitos tipificados en el Código Penal Federal, como accesos no autorizados a los sistemas, robos de información, suplantación de identidades, entre otros. Es decir, se advierte que la negativa de acceso a la información se motiva en evitar o prevenir la comisión del delito al no revelar las vulnerabilidades de las medidas de seguridad establecidas por esta Área Universitaria, con relación al cumplimiento de los principios de protección de datos personales previsto en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

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

> *Por tales motivos, respetuosamente, se propone la reserva total de cada uno de esos apartados del documento de seguridad de esta área universitaria, por un periodo de 5 años, de conformidad con el segundo párrafo del artículo 104 de la Ley General, plazo considerado como necesario para la adecuada salvaguarda de la información aludida, atendiendo a que es el lapso promedio que se tiene contemplado para alguna modificación sustancial o actualización del Documento de Seguridad en cita.*
>
> *En virtud de lo anterior, le solicito de la manera más atenta que ese Cuerpo Colegiado tenga a bien emitir la resolución que en derecho corresponda, para lo cual se adjunta la documentación completa "* (sic).

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

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

PRIMERA. De acuerdo con lo dispuesto por los artículos 1, 11 y 15, fracción X del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México, el Comité de Transparencia de la Universidad Nacional Autónoma de México es competente para analizar la **clasificación de reserva parcial de la información para la elaboración de la versión pública** determinada por el **Instituto de Biotecnología,** la **Coordinación de Universidad Abierta y Educación Digital,** la **Secretaría General de la UNAM**, el **Instituto de Neurobiología,** la **Escuela Nacional Preparatoria Plantel 1 "Gabino Barreda**, la **Coordinación de Planeación, Evaluación y Simplificación de la Gestión Institucional,** la **Dirección General de Asuntos del Personal Académico,** la **Escuela Nacional de Estudios Superiores Unidad Morelia,** el **Centro de Física Aplicada y Tecnología Avanzada,** así como la **Dirección General de Artes Visuales** para atender la solicitud de acceso a la información con número de folio **410031900248326** y determinar, en consecuencia, si la confirma, modifica o revoca.

SEGUNDA. En términos de lo previsto en los artículos 102, tercer párrafo de la Ley General de Transparencia y Acceso a la Información Pública; 33, 34, fracción I y 56, fracción II, inciso b) del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México, **los titulares de las Áreas Universitarias son responsables de clasificar la información que obre en sus archivos**, debiendo comunicar al Comité mediante oficio, de forma fundada y motivada, dicha determinación.

TERCERA. Las áreas universitarias clasificaron como reservada, por un periodo de **cinco años**, parte de la información contenida en su Documento de Seguridad correspondiente a los apartados relativos **al análisis de riesgo, al análisis de brecha, al plan de trabajo**, así como **diversa información relacionada con alguno de dichos apartados o que revele vulnerabilidades en la protección de los datos personales que obran en sus archivos**, conforme a lo expuesto en los antecedentes V, VI, VII, VIII, IX, X y XI de la presente resolución, por actualizarse el supuesto establecido en el artículo 112, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública.

Ahora bien, en el artículo 112, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública, se prevé lo siguiente:

> *“ o o información reservada podrá clasificarse aquella cuya publicación:*
>
> ***VII.** Pueda causar daño u obstruya la prevención de los delitos;*
>
> *”*

Conforme a lo anterior, la clasificación de reserva se debe asignar a aquella información que obstruya la prevención de delitos, ya sea por obstaculizar las acciones implementadas para evitar la comisión de los mismos, o bien, por menoscabar o limitar la capacidad para evitarlos.

Inicialmente, cabe tener en consideración lo establecido en el documento de trabajo del 12º. Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal de la Organización de las Naciones Unidas, en el cual se define la prevención del delito de la sig ien e anera *“La prevención del delito engloba toda la labor realizada para reducir el riesgo de que se cometan delitos y sus efectos perjudiciales en las personas y la ocie ”*

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

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

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

También, el artículo 7 del Convenio para la Protección de las Personas con Respecto al Tratamiento Automatizado de Datos de Carácter Personal, adoptado en Estrasburgo, Francia, el 28 de enero de 1981**,** publicado mediante Decreto de fecha 28 de septiembre de 2018 en el Diario Oficial de la Federación, establece que los Estados miembros deberán tomar medidas de seguridad apropiadas para la protección de datos de carácter

personal registrados en ficheros automatizados, contra la destrucción accidental o no autorizada, o la pérdida accidental, así como contra el acceso, la modificación o la difusión no autorizados.

Por su parte, el artículo 24, fracción V de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, dispone como uno de los mecanismos que deberá adoptar el responsable para cumplir con el principio de responsabilidad establecido en dicha Ley General, contar con un sistema de supervisión y vigilancia, interna y/o externa, incluidas auditorías, para comprobar el cumplimiento de las políticas de protección de datos personales.

Además, de conformidad con el artículo 27, fracción VII de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, para establecer y mantener las medidas de seguridad para la protección de los datos personales, el Sujeto Obligado deberá monitorear y revisar de manera periódica las medidas de seguridad implementadas, así como las amenazas y vulneraciones a las que están sujetos los datos personales, para lo cual es recomendable observar, lo siguiente:

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

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

En ese sentido, el artículo 29 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados establece que los sujetos obligados deben elaborar un Documento de Seguridad, entendiéndose como tal, el instrumento que describe y da cuenta de manera general sobre las medidas de seguridad técnicas, físicas y administrativas adoptadas por el responsable para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que posee; mismo que deberá contener, cuando menos:

1. El inventario de datos personales y de los sistemas de tratamiento.

2. Las funciones y obligaciones de las personas que traten datos personales.
3. El análisis de riesgo.
4. El análisis de brecha.
5. El plan de trabajo.
6. Los mecanismos de monitoreo y revisión de las medidas de seguridad.
7. El programa general de capacitación.

Dicho documento deberá actualizarse cuando se produzcan modificaciones sustanciales al tratamiento de datos personales que deriven en un cambio de nivel de riesgo; como resultado de un proceso de mejora continua, derivado del monitoreo y revisión del sistema de gestión; como resultado de un proceso de mejora para mitigar el impacto de una vulneración a la seguridad ocurrida; así como con la implementación de acciones correctivas y preventivas ante una vulneración de seguridad, en términos del artículo 30 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

En tal orden de ideas, el segundo párrafo del artículo 5 de las Normas Complementarias sobre Medidas de Seguridad Técnicas, Administrativas y Físicas para la Protección de Datos Personales en Posesión de la Universidad, dispone que el documento de seguridad, deberá contener las medidas de seguridad administrativas, físicas y técnicas aplicables a los sistemas de tratamiento de datos personales de las Áreas Universitarias, con el fin de asegurar la integridad, confidencialidad y disponibilidad de la información personal que éstos contienen.

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

Por ende, de difundirse la información contenida en los apartados relativos al **análisis de riesgo**, al **análisis de brecha** y al **plan de trabajo**; así como **toda aquella información que se encuentre directamente relacionada con alguno de dichos apartados** o que **revele vulnerabilidades en la protección de los datos personales en poder de las áreas universitarias,** se haría del conocimiento público la falta o debilidad de seguridad en un activo o grupo de activos, físicos o electrónicos, que puede ser explotada por una o más amenazas, lo que conllevaría a la materialización de las mismas y, derivado de ello, ocasionar la pérdida, destrucción no autorizada o incluso la sustracción de los datos personales en posesión de la Universidad, así como el robo, extravío o copia no autorizada de los mismos, su uso, acceso o tratamiento no autorizado, además del daño, alteración o modificación no autorizada, incluso impidiendo su recuperación, vulnerando así la seguridad de los datos personales.

Bajo estos argumentos se advierte que la clasificación de la información contenida en el **análisis de riesgo**, el **análisis de brecha**, el **plan de trabajo**; así como de **toda aquella información que se encuentre directamente relacionada con alguno de dichos**

apartados o que **revele vulnerabilidades en la protección de los datos personales en poder de las áreas universitarias**, tiene como propósito evitar o prevenir la comisión de conductas delictivas, tales como el acceso ilícito a equipos y sistemas de informática, la cual se encuentra prevista en el Título Noveno, Revelación de Secretos y Acceso Ilícito a sistemas y equipos de informática, Capítulo II, Acceso Ilícito a sistemas y equipos de informática, del Código Penal Federal en el cual se dispone lo siguiente:

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

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

Por lo que de darse a conocer la información objeto de reserva se expondrían las acciones implementadas o por implementar, anticipando las medidas de seguridad más relevantes e inmediatas a establecer, así como las amenazas y vulnerabilidades existentes para los datos personales y los recursos involucrados en su tratamiento, como pueden ser: hardware, software, manejo de documentos físicos y/o electrónicos, entre otros, lo que representa para las áreas universitarias un riesgo evidente para la estabilidad de la ejecución de las medidas de seguridad adoptadas para resguardar la información personal que obra en sus archivos, revelando elementos que, de manera concatenada con otra

información que pudiera generarse o que se haya generado, evidenciaría vulnerabilidades que pudieran ser aprovechadas por personas dedicadas a la comisión de conductas ilícitas y con ello poner en riesgo la seguridad de los datos personales tratados en el desempeño y/o ejercicio de sus competencias, facultades y/o funciones.

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

En este orden de ideas, la información analizada actualiza la causal de reserva prevista en el artículo 112, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública.

Consecuentemente, en términos del artículo 107 de la Ley General citada, se analiza la siguiente prueba de daño:

> *"Artículo 107. En la aplicación de la prueba de daño, el sujeto obligado deberá justificar que:*
> *I. La divulgación de la información representa un riesgo real, demostrable e identificable de perjuicio significativo al interés público o a la seguridad nacional;*
> *II. El riesgo de perjuicio que supondría la divulgación supera el interés público general de que se difunda, y*
> *III. La limitación se adecua al principio de proporcionalidad y representa el medio menos restrictivo disponible para evitar el perjuicio"*

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

Difundir la información relativa al **análisis de riesgo**, el **análisis de brecha**, el **plan de trabajo,** así como **toda aquella información que se encuentre directamente relacionada con alguno de dichos apartados** o **revele vulnerabilidades en la protección de los datos personales en poder de las áreas universitarias**, representa un riesgo potencial, pues dichos apartados contienen elementos informativos a partir de los cuales se podrían identificar vulnerabilidades que pueden ser aprovechadas para realizar conductas contrarias a derecho, tales como actos vandálicos, o bien, ataques informáticos de diversa índole en contra de los sistemas de tratamiento de datos personales y la información contenida en ellos, disminuyendo la capacidad de las áreas universitarias para prevenir y/o contrarrestar posibles amenazas.

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

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

Al verse limitada la capacidad de las áreas universitarias para prevenir y/o contrarrestar conductas que amenacen los sistemas de tratamiento de datos personales y/o su contenido, se expone a los integrantes de la comunidad universitaria, integrada por personal administrativo, académico y el estudiantado, así como a las diversas personas que proporcionan sus datos personales a las distintas entidades académicas y/o dependencias administrativas con motivo del desarrollo de las actividades que tienen encomendadas, a la comisión de diversos actos ilícitos tales como la sustracción, el ocultamiento, la alteración, mutilación, destrucción o inutilización de sus datos personales, la suplantación de identidad, extorsiones u otras conductas delictivas relacionadas con la explotación de dichos elementos informativos.

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

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

La limitación se ajusta al principio de proporcionalidad, toda vez que se justifica no difundir la información en cuestión, a cambio de garantizar la capacidad de las áreas universitarias para implementar todas aquellas medidas y acciones tendientes a reducir el riesgo de que se cometa una conducta ilícita que pudiera vulnerar los datos personales cuyo tratamiento realizan con motivo del desempeño y/o ejercicio de sus competencias, facultades o funciones.

En ese sentido, la limitación representa el medio menos restrictivo disponible para evitar el perjuicio, ya que únicamente se restringirá el acceso a la información, por un periodo de **cinco años,** que se computará a partir del **9 de octubre de 2026** y fenecerá el **9 de octubre de 2031**, o bien, se interrumpirá antes si desaparecen las causas que originaron la reserva de la información, lo que suceda primero.

Periodo que se estima pertinente, toda vez que durante el mismo podría tener lugar alguna modificación sustancial o una actualización del Documento de Seguridad de las áreas universitarias.

Ahora bien, por cuanto hace a la información que se encuentre directamente relacionada con los apartados de análisis de riesgo, análisis de brecha, y plan de trabajo o que revele vulnerabilidades en la protección de los datos personales en poder de las áreas universitarias, resulta procedente únicamente el resguardo de aquellos elementos informativos cuya divulgación ponga en riesgo los sistemas de tratamiento de datos personales o su contenido, pues de la revisión a las versiones públicas remitidas por las áreas universitaria se observa que en diversos apartados

como lo son: la estructura y la descripción de los sistemas de tratamientos de datos personales; acceso a las instalaciones; el inventario de sistemas de tratamiento de datos personales; las características del lugar donde se resguardan los soportes; las finalidades del tratamiento; el nombre de usuarios; los mecanismos de monitoreo y revisión de las medidas de seguridad, se protege información de carácter genérico que no representa una amenaza a tales sistemas ni a la información almacenada en ellos, por lo que se deberá verificar dicha circunstancia previo a realizar el testado correspondiente.

Consecuentemente, se colman las hipótesis de las fracciones I, II y III, dispuestas en el artículo 107 de la Ley General de Transparencia y Acceso a la Información Pública, siendo procedente **CONFIRMAR** la clasificación de reserva parcial de la información para la elaboración de la versión pública determinada por el **Instituto de Biotecnología,** por la **Coordinación de Universidad Abierta y Educación Digital,** por la **Secretaría General de la UNAM**, por el **Instituto de Neurobiología,** por la **Escuela Nacional Preparatoria Plantel 1 "Gabino Barreda"**, por la **Coordinación de Planeación, Evaluación y Simplificación de la Gestión Institucional,** por la **Dirección General de Asuntos del Personal Académico**, por la **Escuela Nacional de Estudios Superiores Unidad Morelia,** por el **Centro de Física Aplicada y Tecnología Avanzada**, así como por la **Dirección General de Artes Visuales**, por un periodo de **cinco años**, mismo que fenecerá el **9 de octubre del 2031**, de conformidad con lo establecido en el artículo 112, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública.

CUARTA. En relación con el contenido del Documento de Seguridad y la versión pública correspondiente, **las áreas universitarias deberán**:

1. Verificar que su Documento de Seguridad cuenta con los apartados previstos en el artículo 29 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, además de que cumpla con la información y características establecidas en el "Anexo I. Documento de Seguridad de Datos Personales" de los "Anexos de las Normas Complementarias sobre medidas de seguridad técnicas, administrativas y físicas para la protección de datos personales en posesión de la Universidad", aprobados por este Cuerpo Colegiado mediante Acuerdo de fecha 10 de enero de 2020.

2. Revisar que la información correspondiente a los apartados de "Análisis de Riesgos", de "Análisis de Brecha", de "Plan de Trabajo" del Documento de Seguridad, así como toda aquella información que se encuentre directamente relacionada con alguno de dichos apartados o revele vulnerabilidades en la protección de los datos personales en poder de las áreas universitarias sea debidamente testada, a efecto de evitar posibles vulneraciones; para tal efecto, deberán emplear un medio de testado que no permita la visualización y/o recuperación de la información objeto de reserva, pero que no impida la lectura del resto del contenido.

3. Corroborar que la información diversa a los apartados de análisis de riesgo, análisis de brecha, así como al plan de trabajo, cuyo resguardo plantean en la versión pública de su Documento de Seguridad, corresponda a **elementos informativos que efectivamente constituyan un riesgo** para los sistemas de tratamiento de datos personales y/o para su

contenido, **sin que sea dable proteger información como**: **descripciones genéricas** de los accesos a las instalaciones, de los métodos empleados para autorizar los accesos (bitácoras, identificaciones, control biométrico), de los lugares o soportes en que se almacenan los datos personales, o bien, de los mecanismos de monitoreo implementados; el **inventario y la descripción** de los sistemas referidos en el mismo; las **finalidades** del tratamiento de los datos personales; las **categorías** de los datos personales recabados; el nombre de las personas responsables, encargadas y/o usuarias de dichos sistemas, entre otra diversa, que **no actualiza el supuesto de reserva invocado**, al no corresponder a datos que comprometan las medidas de seguridad físicas, administrativas y/o técnicas implementadas para proteger los sistemas en cuestión.

4. Insertar un cuadro de texto en las hojas de la versión pública en las cuales protejan información, a fin de indicar:

a) Las partes o secciones reservadas.
b) El fundamento legal que sustenta la reserva, así como el plazo de ésta, mismos que se encuentran indicados en el último párrafo de la consideración **TERCERA** de la presente resolución.

Por lo expuesto, y de acuerdo con los artículos 6, apartado A de la Constitución Política de los Estados Unidos Mexicanos; 1, 6, 7, 8, 24, 40, fracción II, 112, fracción VII, así como 139, fracción I de la Ley General de Transparencia y Acceso a la Información Pública; 1, 15, fracción X y 37 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México, este Comité de Transparencia:

R E S U E L V E

PRIMERO. Con fundamento en lo dispuesto por los artículos 1 y 15 fracción X del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México; así como 139, fracción I de la Ley General de Transparencia y Acceso a la Información Pública, este Comité de Transparencia **CONFIRMA** la **CLASIFICACIÓN** de **RESERVA** parcial de la información para la elaboración de la versión pública determinada por el **Instituto de Biotecnología**, por la **Coordinación de Universidad Abierta y Educación Digital**, por la **Secretaría General de la UNAM**, por el **Instituto de Neurobiología,** por la **Escuela Nacional Preparatoria Plantel 1 "Gabino Barreda"**, por la **Coordinación de Planeación, Evaluación y Simplificación de la Gestión Institucional,** por la **Dirección General de Asuntos del Personal Académico,** por la **Escuela Nacional de Estudios Superiores Unidad Morelia,** por el **Centro de Física Aplicada y Tecnología Avanzada,** así como por la **Dirección General de Artes Visuales** por un periodo de **cinco años,** mismo que se computará a partir del **9 de octubre de 2026** y fenecerá el **9 de octubre de 2031,** para atender la solicitud de acceso a la información con número de folio **410031900248326.**

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

SEGUNDO. Se **instruye** a las áreas universitarias a fin de que atiendan las indicaciones enumeradas en la consideración **CUARTA** de esta resolución.

TERCERO. Se instruye a las áreas universitarias para que, **dentro de los tres días hábiles siguientes a la notificación de la presente resolución**, remitan a la Unidad de Transparencia la versión pública para su entrega a la persona solicitante, conforme a la modalidad elegida para ello.

Lo anterior, de acuerdo con los artículos 120 y 136, segundo párrafo de la Ley General de Transparencia y Acceso a la Información Pública.

CUARTO. La persona solicitante podrá interponer el recurso de revisión previsto en los artículos 144 y 145 de la Ley General de Transparencia y Acceso a la Información Pública, así como 67 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México, a través de la Plataforma Nacional de Transparencia o ante la Unidad de Transparencia de la Universidad Nacional Autónoma de México, dentro de los quince días siguientes a la fecha de la notificación de la respuesta o del vencimiento del plazo para su notificación.

QUINTO. Con fundamento en los artículos 41, fracción V y 139, último párrafo de la Ley General de Transparencia y Acceso a la Información Pública; 21, fracción V y 58, fracción II, tercer párrafo del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México, notifíquese la presente resolución por correo electrónico institucional al **Instituto de Biotecnología,** a la **Coordinación de Universidad Abierta y Educación Digital,** a la **Secretaría General de la UNAM**, al **Instituto de Neurobiología**, a la **Escuela Nacional Preparatoria Plantel 1 "Gabino Barreda"**, a la **Coordinación de Planeación, Evaluación y Simplificación de la Gestión Institucional,** a la **Dirección General de Asuntos del Personal Académico**, a la **Escuela Nacional de Estudios Superiores Unidad Morelia,** al **Centro de Física Aplicada y Tecnología Avanzada,** a la **Dirección General de Artes Visuales,** así como a la Unidad de Transparencia de esta Universidad, para que por conducto de esta última sea notificada a la persona solicitante, para los efectos procedentes.

Así lo resolvió en su Trigésima Sexta Sesión, por unanimidad de votos de sus integrantes, el Comité de Transparencia de la Universidad Nacional Autónoma de México, en términos de los artículos 1, 11, 15, 19 y 58, fracción II del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

"POR MI RAZA HABLARÁ EL ESPÍRITU"
Ciudad Universitaria, Cd. Mx., a 9 de octubre de 2026

Sistema de Firma de Documentos de Cuerpos Colegiados

Representación gráfica del acto de firma.

1 INFORMACIÓN DEL DOCUMENTO FIRMADO

Datos generales e identificadores del documento firmado.

Nombre del archivo
08-ctunam-476-2026-248326.pdf

Fecha y hora de solicitud de firma
09/10/2026 17:06:31

Fecha y hora de cierre
09/10/2026 18:27:02

Número de páginas
34

Identificador único del documento HASH

```
154eff0bffa3cba1e30de8a791f7a5cd02c60171d6c9c69cbf725695e446d63f
```

2 VALIDACIÓN DEL DOCUMENTO

Verificación mediante código QR.

La presente constancia acredita la integridad,
autenticidad y fecha de firma del documento
mediante evidencia criptográfica verificable.

SFD
09/10/2026 18:49

Validar documento

Escanee el código QR para validar la información de este documento.

Total de firmantes: **5**

3 FIRMANTES

Personas que realizaron la firma electrónica del documento.

01

Nombre
Dra. Ángela Quiroga Quiroga

Fecha y hora de firma
09/10/2026 18:27:02

Cargo
Directora General de Estudios de Legislación Universitaria y Suplente del Presidente del Comité de Transparencia

Orden de firma
1

Hash Firma

```
8c41f5112a87b16c249da6c8f9445bccb142f0755fbfcd41b9861a9d3bded78c62153f0f27adca8e1ad8e4a4f01b6455
```

02

Nombre
Mtro. Jairo Orlando Perilla Camelo

Fecha y hora de firma
09/10/2026 18:12:31

Cargo
Director General para la Prevención y Mejora de la Gestión Institucional y suplente del Contralor

Orden de firma
2

Hash Firma

```
d27afa12dddc2b2011f658e81ddb574540d4fdd012704f8034520691de94eacdbd5c17280fb614e670cfa0c412d8f942
```

03

Nombre
Lic. Lorena Orozco Novelo

Fecha y hora de firma
09/10/2026 18:06:49

Cargo
Defensora Adjunta de Derechos Universitarios y suplente de la Titular de la Defensoría de los Derechos Universitarios, Igualdad y Atención de la Violencia de Género

Orden de firma
3

Hash Firma

```
d6ee1e56fec92594d32527aa76ff1feab99d0ca439570751322e5afc8fe8cdac6b6e5dc0932ef54c6182d466946d219c
```

04	**Nombre** Mtro. Porfirio Antonio Díaz Rodríguez	**Fecha y hora de firma** 09/10/2026 17:32:26
	Cargo Titular de la Dirección General de Servicios Generales y Movilidad	**Orden de firma** 4
	Hash Firma e6140e783faa83001a740c68d480c396f6bb01c1a622218086d451d40b85360e1b1eead5072b957c4a3c4034cf1b723a	

05	**Nombre** Lic. Julio César Muñoz Bustos	**Fecha y hora de firma** 09/10/2026 17:28:47
	Cargo Titular de la Unidad de Transparencia	**Orden de firma** 5
	Hash Firma 14961780c008f6dfe2f7912241008a331538a84ecea19f0226e65319b400444cb6e19426752d6a0a47cbd0f45fb2d278	

INSTITUTO DE NEUROBIOLOGÍA

475+ UNIVERSIDAD MÉXICO

UNAM Oficina de la Abogacía General RECIBIDO 25 SEP 2026 Con anexo Oficina Central de Correspondencia Nombre: Norma Rodich Hora: 14:31 Firma

UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO
DIRECCIÓN

Oficio Núm. INEU/D/598/2026

Asunto: Reserva del Documento de Seguridad

ACUSE

U.N.A.M. UNIDAD DE TRANSPARENCIA 25 SEP 2026 RECIBIDO HORA 13:45 FIRMA

OF.DE CORRESPONDENCIA UNAM D G A J 2026 SEP 25 12:10

Mtro. Hugo Alejandro Concha Cantú
Presidente del Comité de Transparencia
P R E S E N T E

El documento de seguridad es el instrumento que describe y da cuenta de manera general sobre las medidas de seguridad técnicas, físicas y administrativas adoptadas por el responsable para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que posee un área universitaria; cuyo contenido comprende diversos elementos o apartados, de los cuales al menos tres se ajustan al supuesto de reserva contemplado en los artículos 29 y 30 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados1 (LGPDPPSO) y 112, fracción VII2 en relación con el 103, fracción I3, de la Ley General de Transparencia y Acceso a la Información Pública4 (Ley General), ya que su divulgación obstruiría el deber de esta Universidad de establecer y mantener las medidas de seguridad técnicas, administrativas y físicas de los datos personales que resguarda esta institución.

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

Anexos o Políticas	Contenido y su afectación	Páginas
a. Análisis de riesgos	El análisis de riesgos contiene información sobre las vulnerabilidades de la infraestructura tecnológica del INB, y otorga herramientas a las personas para implementar un ataque informático a los activos críticos y no críticos.	36–41
b. Análisis de brecha	El análisis de brecha integra información relativa a la seguridad de la infraestructura tecnológica; enlista los controles de seguridad con los que cuenta esta área; y menciona las herramientas que se deben adquirir para garantizar un nivel más alto de seguridad de los sistemas de información. Es decir, detalla diferencias entre los controles existentes y los requeridos; identifica deficiencias administrativas, físicas y técnicas, así como necesidades de fortalecimiento, herramientas y controles pendientes de implementar.	42–46
c. Plan de Trabajo	El plan de trabajo define los controles de seguridad a implementar de acuerdo con el resultado del análisis de riesgos y del análisis de brecha, priorizando las medidas de seguridad más relevantes con base en el riesgo real detectado. El uso de esta información permite inferir nuestros riesgos, por cuánto tiempo seguirán así hasta el momento en que se implementen nuevos controles. Es decir, define controles y acciones de seguridad por implementar, responsables, prioridades y horizontes de atención. Esta información permite inferir qué riesgos permanecerán mientras se instrumentan nuevos controles.	46–51
d. Inventario de Sistemas de Tratamiento de Datos Personales	En el inventario de sistemas de tratamiento de datos personales se identifican sistemas físicos y electrónicos, áreas responsables, tipos de datos, medios de almacenamiento, transferencias y niveles de riesgo. Su divulgación permitiría ubicar activos, sistemas prioritarios y puntos de exposición institucional.	32–36

Oficio Núm. INEU/D/598/2026

Los fundamentos y motivos se exponen a continuación:

- Existe un *riesgo real, demostrable e identificable* en perjuicio del nexo causal que prevé la hipótesis de reserva ahora analizada contemplada en el artículo 112, fracción VII, de la Ley General. La información contenida en los apartados relativos al análisis de riesgo, el análisis de brecha, el plan de trabajo y el inventario de sistemas de tratamiento de datos personales del INB describe cómo se protegen los datos personales que los titulares han confiado al Instituto y cuya seguridad es nuestra responsabilidad garantizar. Es un riesgo real el hecho de que toda persona que quiera ocasionar la pérdida, destrucción, robo, copia, uso, acceso o tratamiento no autorizado, daño, alteración o modificación no autorizada de datos personales, puede hacerlo si cuenta con la información exacta de las vulnerabilidades de un área universitaria, lo que esta serie de documentos les otorga directamente si se difundiera la información.
- Divulgar el análisis de riesgo, el análisis de brecha, el plan de trabajo y el inventario de sistemas de tratamiento de datos personales del INB evidencia los nuevos controles pendientes de implementar, describen la forma en que almacenamos técnicamente los datos personales, cómo protegemos los sistemas automatizados de información, qué medidas de seguridad administrativas, físicas y técnicas planeamos establecer de manera gradual y de conformidad con las prioridades y recursos presupuestales otorgados.
- En este sentido, la revelación de la información que obra en el análisis de riesgo, el análisis de brecha, el plan de trabajo y el inventario de sistemas de tratamiento de datos personales del INB revela y hace identificable la forma en que es posible atacar o vulnerar nuestros sistemas de información que resguardan datos personales que obran en nuestros archivos y limitaría la capacidad de esta área para reaccionar ante posibles amenazas.

La prueba de daño precitada colma los extremos establecidos en las tres fracciones del artículo 107 de la Ley General de Transparencia y Acceso a la Información Pública, dado que podrá considerarse como información reservada aquélla que obstruya la prevención de delitos al obstaculizar las acciones implementadas por las autoridades para evitar su comisión, o menoscabar o limitar la capacidad de estas para evitar la comisión de delitos.

En esa inteligencia, el dar a conocer el análisis de riesgo, el análisis de brecha, el plan de trabajo y el inventario de sistemas de tratamiento de datos personales del INB afectaría la prevención de actos ilícitos que pudieran realizarse en contra de los sistemas de información y tratamiento de datos personales, así como en contra de los activos e infraestructura crítica del INB; por lo que es posible advertir que algunas de las posibles consecuencias de divulgar dicha información podrían derivar en la comisión de diversos delitos tipificados en el Código Penal Federal, como accesos no autorizados a los sistemas, robos de información, suplantación de identidades, entre otros. Es decir, se advierte que la negativa de acceso a la información se motiva en evitar o prevenir la comisión del delito al no revelar las vulnerabilidades de las medidas de seguridad establecidas por esta Área Universitaria, con relación al cumplimiento de los principios de protección de datos personales previstos en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

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

Por tales motivos, respetuosamente, se propone la reserva total de cada uno de esos apartados del documento de seguridad de esta área universitaria, por un periodo de cinco años, de conformidad con el segundo párrafo del artículo 104 de la Ley General, plazo considerado como necesario para la adecuada salvaguarda de la información aludida, atendiendo a que es el lapso promedio que se ha previsto para alguna modificación sustancial o actualización del Documento de Seguridad en cita.

En virtud de lo anterior, le solicito atentamente que ese Cuerpo Colegiado tenga a bien emitir la resolución que en derecho corresponda, para lo cual se adjunta la documentación completa.

Sin otro particular, reciba un cordial saludo.

A t e n t a m e n t e,
"POR MI RAZA HABLARÁ EL ESPÍRITU"
Campus UNAM Juriquilla, Querétaro, a 23 de septiembre de 2026.
La Directora

Dra. María Teresa Morales Guzmán

C.c.p. **Lic. Jesús Alfredo Armendáriz López.** Secretario Técnico del Comité de Transparencia. Presente.
Lic. Julio César Muñoz Bustos. Titular de la Unidad de Transparencia. Presente.
Lic. Rodrigo García Santillán. Enlace de Transparencia del Instituto de Neurobiología. Presente.
Mtro. J. Elías Pacheco Hernández. Secretario Administrativo del Instituto de Neurobiología. Presente.