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

CAPÍTULO I: DISPOSICIONES GENERALES

Objeto

Artículo 1. Las presentes Normas Complementarias son de observancia obligatoria y gradual conforme a la disponibilidad de recursos de las Áreas Universitarias y tienen por objeto establecer las políticas internas de gestión y tratamiento de datos personales, así como proveer los mínimos exigibles en medidas de seguridad técnicas, administrativas y físicas para la protección de datos personales en posesión de las Áreas Universitarias.

Definiciones

Artículo 2. Además de las definiciones previstas en el numeral 2 de los Lineamientos para la Protección de Datos Personales en Posesión de la Universidad Nacional Autónoma de México, para los efectos de las presentes Normas se entenderá por:

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

II. **Área productora:** Oficina del Área Universitaria a la que, atendiendo al nivel jerárquico establecido en el organigrama vigente, desde el nivel de dirección hasta jefatura de departamento o equivalente, se le asigna una clave por el Área Coordinadora de Archivos, recibe y produce documentos de archivo en el ejercicio de sus facultades, funciones o competencias, mismos que están bajo su responsabilidad, independientemente del soporte, espacio o lugar en que los resguarden.

III. **Auditoría técnica interna:** Proceso sistemático y documentado realizada por la Dirección General de Cómputo y de Tecnologías de Información y Comunicación (DGTIC) de la Universidad, o bien, por una empresa externa al Área Universitaria, para que se evalué la adaptación, adecuación y eficacia de los controles, medidas y mecanismos implementados por el Área Universitaria para el tratamiento de datos personales, para la obtención de evidencia que permita determinar su conformidad con la Ley General, los Lineamientos y las presentes Normas.

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

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

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

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

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

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

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

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

XII. **Documento de seguridad:** Instrumento que describe y da cuenta de manera general sobre las medidas de seguridad técnicas, físicas y administrativas adoptadas por el Responsable para garantizar la Confidencialidad, Integridad y Disponibilidad de los datos personales que posee.

XIII. Encargado: La persona física o jurídica distinta a las áreas, entidades o dependencias universitarias, que realizan el tratamiento de los datos personales a nombre de la Universidad, suscribiendo para tal efecto los instrumentos consensuales correspondientes acordes con la Legislación Universitaria aplicable.

XIV. Evaluación de impacto en la protección de datos personales (EIDP): Documento mediante el cual las Áreas Universitarias que pretendan poner en operación o modificar políticas públicas, programas, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento intensivo o relevante de datos personales, valoran los impactos reales sobre determinado tratamiento de datos personales, a efecto de identificar y mitigar posibles riesgos relacionados con los principios, deberes y derechos de los titulares, así como los deberes de los Responsables y Encargados, previstos en la normativa aplicable.

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

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

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

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

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

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

a) Prevenir el acceso no autorizado al perímetro de la organización, sus instalaciones físicas, áreas críticas, recursos e información;

b) Prevenir el daño o interferencia a las instalaciones físicas, áreas críticas de la organización, recursos e información;

c) Proteger los recursos móviles, portátiles y cualquier soporte físico o electrónico que pueda salir de la organización, y

d) Proveer a los equipos que contienen o almacenan datos personales de un mantenimiento eficaz, que asegure su disponibilidad e integridad.

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

a) Asegurar que el acceso a las bases de datos o a la información, así como a los recursos, sea por usuarios identificados y autorizados;

b) Generar un esquema de privilegios para que el usuario realice las actividades que requiere con motivo de sus funciones;

c) Revisar la configuración de seguridad en la adquisición, operación, desarrollo y mantenimiento del software y hardware, y

d) Gestionar las comunicaciones, operaciones y medios de almacenamiento de los recursos informáticos en el tratamiento de datos personales.

XXII. Oficial de Protección de Datos Personales: Persona designada atendiendo a sus conocimientos, cualidades profesionales, experiencia en la materia, y, en su caso, a la o las certificaciones con que cuente en materia de protección de datos personales, con la jerarquía o posición dentro de la Universidad para implementar políticas transversales en esta materia y que formará parte de la Unidad de Transparencia.

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

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

XXV. Remisión: Toda comunicación de datos personales realizada exclusivamente entre el Responsable y encargado, dentro o fuera del territorio mexicano.

XXVI. Responsable: Las Áreas Universitarias que manejan, resguardan y/o deciden sobre el tratamiento de datos personales.

XXVII. Responsable de Archivos: Persona designada por el titular de cada Área Universitaria, de entre la plantilla laboral existente, para contribuir al debido cumplimiento de los procedimientos, obligaciones, lineamientos y criterios emitidos por las figuras rectoras del Sistema Institucional de Archivos de la Universidad y funge como enlace entre el Área Universitaria y el Área Coordinadora de Archivos para la mejor organización, administración y conservación de los archivos universitarios.

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

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

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

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

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

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

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

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

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

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

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

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

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

Sistemas de tratamiento de datos personales

Artículo 3. El Área Universitaria, para implementar las medidas de seguridad aplicables a los sistemas de tratamiento de datos personales, debe considerar la modalidad en la cual operan éstos, de manera manual o automatizada, desde su obtención, registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de datos personales**,** mediante cualquiera de los siguientes tipos de soportes:

a) En soportes físicos.
b) En soportes electrónicos.
c) En redes de datos.

Destinatarios de la comunicación de datos personales

Artículo 4. En la comunicación de datos personales a una persona distinta al titular de los datos a través de soportes, se deberá identificar el tipo de destinatario:

I. Interinstitucional: comunicación a cualquier Área Universitaria;
II. Gubernamental: comunicación con los Poderes Ejecutivo, Legislativo, Judicial u Organismos Autónomos, en los distintos niveles federales, locales o municipales respectivamente;
III. Internacional: comunicación a gobiernos, instituciones educativas u organismos extranjeros, y
IV. Persona moral de derecho privado: institución, organización, asociación civil o empresa, con o sin fines de lucro.

Roles y responsabilidades específicas de los involucrados en el tratamiento de datos personales

Artículo 5. El Responsable de seguridad de datos personales documentará los roles y cadena de rendición de cuentas de las personas que traten datos personales en su Área Universitaria, conforme al sistema de gestión de seguridad implementado y materializado en el documento de seguridad a que se refieren los numerales 24 y 25 de los Lineamientos.

El documento de seguridad que elabore cada Área Universitaria será público y deberá contener las medidas de seguridad administrativa, física y técnica aplicables a los sistemas de tratamiento de datos personales del área con el fin de asegurar la integridad, confidencialidad y disponibilidad de la información personal que éstos contienen (v*er "Anexo I. Documento de seguridad de datos personales").*

Cada Área Universitaria se asegurará de que todas las personas involucradas en el tratamiento de datos personales en el Área Universitaria conozcan sus funciones para el cumplimiento de los objetivos del sistema de gestión de seguridad, así como las consecuencias de su incumplimiento.

Inventario de datos personales

Artículo 6. Toda Área Universitaria elaborará un inventario con la información básica de cada tratamiento de datos personales, considerando los siguientes elementos:

I. El catálogo de recursos a través de los cuales se obtienen los datos personales;
II. Las finalidades de cada tratamiento de datos personales;
III. El catálogo de los tipos de datos personales que se traten, indicando si son sensibles o no;
IV. El catálogo de formatos de almacenamiento, así como la descripción general de la ubicación física y/o electrónica de los datos personales;
V. La lista de funcionarios o empleados universitarios que tienen acceso a los sistemas de tratamiento;
VI. En su caso, el nombre completo o denominación o razón social del Encargado y el instrumento jurídico que formaliza la prestación de los servicios que brinda al Área Universitaria, y
VII. En su caso, los destinatarios o terceros receptores de las transferencias que se efectúen, así como las finalidades que justifican éstas.

Ciclo de vida de los datos personales

Artículo 7. En la elaboración del inventario de datos personales el Responsable deberá incluir el ciclo de vida de los datos personales conforme a las siguientes etapas:

I. La obtención de los datos personales;
II. El almacenamiento de los datos personales;
III. El uso de los datos personales conforme a su acceso, manejo, aprovechamiento, monitoreo y procesamiento, incluyendo los sistemas físicos y/o electrónicos utilizados para tal fin;
IV. La divulgación de los datos personales considerando las remisiones y transferencias que, en su caso, se efectúen;
V. El bloqueo de los datos personales, en su caso, y
VI. La cancelación, supresión o destrucción de los datos personales.

El Responsable de seguridad de datos personales identificará el riesgo inherente al tratamiento de los datos personales, contemplando su ciclo de vida y los activos involucrados.

Análisis de riesgos

Artículo 8. El funcionario universitario o empleado que detente la información en un Área Universitaria realizará un análisis de riesgos de los datos personales tratados a partir de la evaluación de impacto por su probabilidad de ocurrencia, denominado riesgo real, considerando lo siguiente:

- **I.** Los requerimientos regulatorios, códigos de conducta o mejores prácticas de un sector específico;
- **II.** El valor de los datos personales de acuerdo con su clasificación previamente definida y su ciclo de vida;
- **III.** El valor y exposición de los activos involucrados en el tratamiento de los datos personales;
- **IV.** Las consecuencias negativas para los titulares que pudieran derivar de una vulneración de seguridad ocurrida, y
- **V.** Los siguientes factores:
  - **a)** El riesgo inherente a los datos personales tratados;
  - **b)** La sensibilidad de los datos personales tratados;
  - **c)** El desarrollo tecnológico;
  - **d)** Las posibles consecuencias de una vulneración para los titulares;
  - **e)** Las transferencias de datos personales que se realicen;
  - **f)** El número de titulares;
  - **g)** Las vulneraciones previas ocurridas en los sistemas de tratamiento, y
  - **h)** El riesgo por el valor potencial cuantitativo o cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada para su posesión.

Una vez que se establezcan los controles de seguridad que mitiguen la ocurrencia del riesgo, se deberá calcular el riesgo residual, resultado de restar al riesgo real, el impacto del control de seguridad respectivo.

Evaluación de impacto en la protección de datos personales

Artículo 9. Cuando el Área Universitaria requiera poner en operación o actualizar programas, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que impliquen el tratamiento intensivo o relevante de datos personales, deberá realizar una *Evaluación de impacto en la Protección de Datos Personales (EIDP).*

Para efectos de estas Normas se considera que se está en presencia de un tratamiento intensivo o relevante de datos personales cuando:

- **I.** Existan riesgos inherentes a los datos personales a tratar, entendidos como el valor potencial cuantitativo o cualitativo que pudieran tener éstos para una tercera persona no autorizada para su posesión o uso en función de la sensibilidad de los datos personales; las categorías de titulares; el volumen total de los datos personales tratados; la cantidad de datos personales que se tratan por cada titular; la intensidad o frecuencia del tratamiento, o bien, la realización de cruces de datos personales con múltiples sistemas o plataformas informáticas;
- **II.** Se traten datos personales sensibles, y
- **III.** Se efectúen o pretendan efectuar transferencias de datos personales, entendidas como cualquier comunicación de datos personales, dentro o fuera del territorio mexicano, realizada a persona distinta del titular, Responsable o Encargado.

Artículo 10. La evaluación de impacto en la protección de datos personales deberá incluir lo siguiente *(ver diagrama 1: Metodología de Evaluación de Impacto de Datos Personales):*

- **I.** La descripción del programa, sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología que implique un tratamiento intensivo o relevante de datos personales que pretenda poner en operación o modificar;
- **II.** La justificación de la necesidad de implementar o modificar la política pública, programa, sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología que implique un tratamiento intensivo o relevante de datos personales;
- **III.** La representación del ciclo de vida de los datos personales a tratar;
- **IV.** La identificación, análisis y descripción de la gestión de los riesgos inherentes para la protección de los datos personales;

V. El análisis de cumplimiento normativo en materia de protección de datos personales de conformidad con los Lineamientos;

VI. Los resultados de la o las consultas externas que, en su caso, se efectúen; y

VII. La opinión técnica del Oficial de Protección de Datos Personales respecto del tratamiento intensivo o relevante de datos personales que implique la política pública, programa, sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología, en su caso.

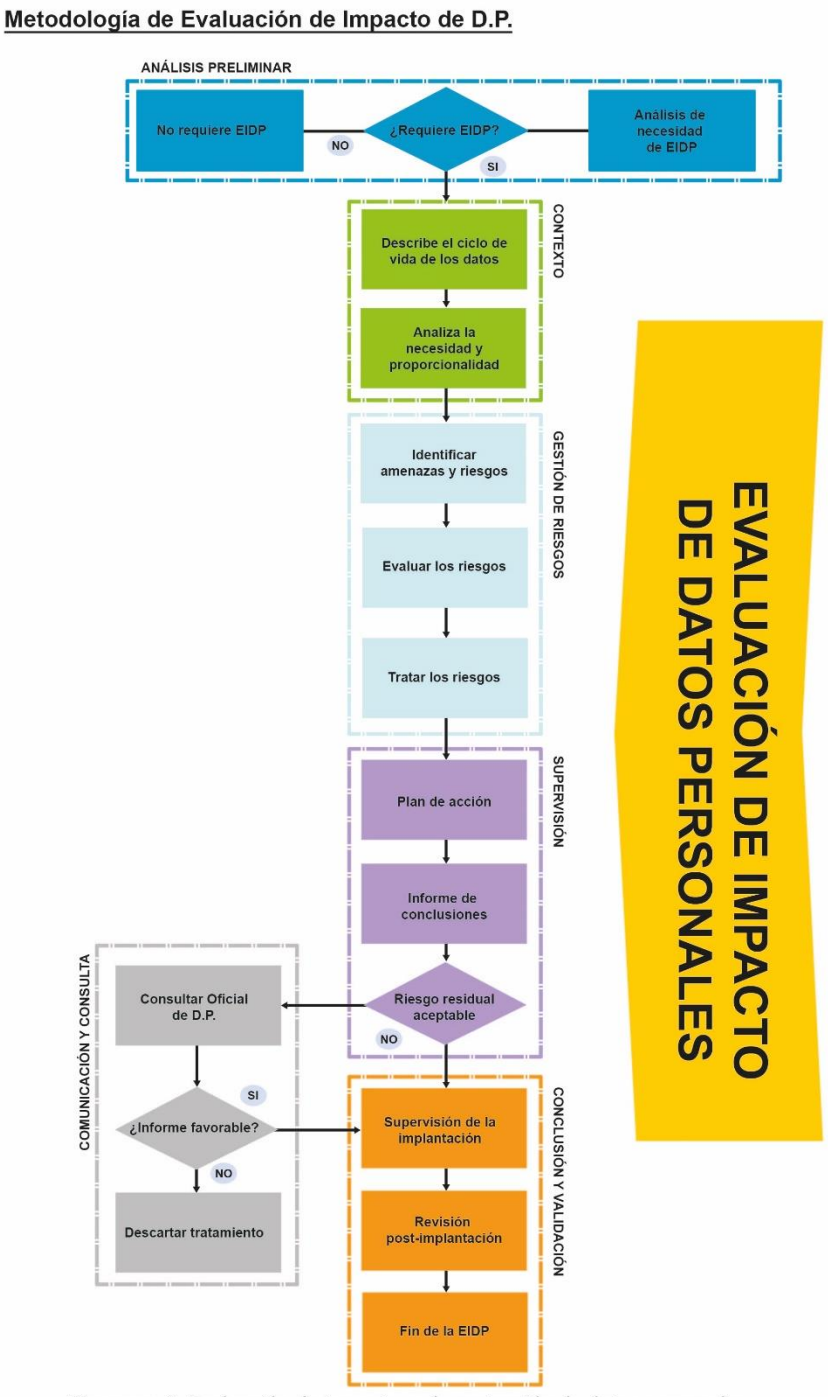

Diagrama 1. Evaluación de impacto en la protección de datos personales

Artículo 11. Los Responsables de seguridad de datos personales de las Áreas Universitarias deberán realizar constantemente un análisis de brecha de seguridad de datos personales, que es un diagnóstico por medio del cual se identifica lo siguiente:

I. Las medidas de seguridad existentes y efectivas;
II. El nivel óptimo de medidas de seguridad y
III. Las medidas de seguridad adicionales a las existentes para alcanzar el nivel óptimo.

Plan de trabajo

Artículo 12. El Área Universitaria deberá elaborar un plan de trabajo que defina 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.

Lo anterior, considerando los recursos asignados, el personal interno y externo al área, así como las fechas establecidas para la implementación de los controles de seguridad nuevos o faltantes.

Monitoreo y supervisión periódica de las medidas de seguridad

Artículo 13. El Área Universitaria deberá evaluar y medir los resultados de las políticas, planes, procesos y procedimientos implementados en materia de seguridad y tratamiento de los datos personales, a fin de verificar el cumplimiento de los objetivos propuestos y, en su caso, implementar mejoras de manera continua, a partir de medir la reducción del riesgo residual considerando los siguientes factores:

I. Los nuevos activos que se incluyan en la gestión de riesgos;
II. Las modificaciones necesarias a los activos, como podría ser el cambio o migración tecnológica, entre otras;
III. Las vulnerabilidades identificadas para determinar aquéllas expuestas a nuevas o pasadas que vuelvan a surgir;
IV. El cambio en el impacto o consecuencias de amenazas valoradas, vulnerabilidades y riesgos en conjunto, que resulten en un nivel inaceptable de riesgo, y
V. Los incidentes y vulneraciones de seguridad ocurridas.

Aunado a lo previsto en las fracciones anteriores del presente artículo, las medidas de seguridad implementadas para la protección de las bases de datos personales se someterán a una auditoría de la Dirección General de Cómputo y de Tecnologías de Información y Comunicación de la Universidad, para el monitoreo, revisión y evaluación, interna o externa y anual, para verificar el cumplimiento de la Ley.

Sistema de Gestión de Seguridad de los Datos Personales (SGSDP)

Artículo 14. El Área Universitaria deberá implementar un sistema de gestión de seguridad de los datos personales para planificar, establecer, implementar, operar, monitorear, mantener, revisar y mejorar las medidas de seguridad de carácter administrativo, físico y técnico aplicadas a los datos personales; tomando en consideración los estándares nacionales e internacionales en materia de protección de datos personales y seguridad.

CAPÍTULO II: MEDIDAS DE SEGURIDAD TÉCNICAS PARA LA PROTECCIÓN DE DATOS PERSONALES

Control de acceso en el tratamiento automatizado de datos personales

Artículo 15. Para la implementación de medidas de seguridad en etapas o capas en el control de acceso, el Responsable de seguridad de datos personales deberá considerar lo siguiente:

I. Identificar: consiste en tomar conocimiento de que una persona es quien dice ser, acredita su personalidad exhibiendo una identificación oficial y en un ambiente electrónico con el nombre de usuario que se introduce al momento de ingresar al sistema (*login*).

II. Autenticar: se refiere a comprobar que esa persona es quien dice ser a través del cotejo de uno o más datos en una identificación oficial contra:
- **a)** Los datos en alguna otra identificación, documento, certificado digital (como el de la firma electrónica) o dispositivo que tenga la persona;
- **b)** Los datos que sepa o tenga memorizados (su firma autógrafa o su contraseña, por ejemplo); o
- **c)** Una o más características que coincidan con lo que es dicha persona como fotografía o huella dactilar.

III. Autorizar: se refiere al permiso a la persona que se ha identificado y autenticado apropiadamente y depende del o de los permisos que le conceda el Responsable de autorizar los accesos.

Artículo 16. El Responsable de seguridad de datos personales deberá considerar la forma de administración de cuentas de usuario y grupos a fin de verificar que utiliza sistemas de información y recursos, ya sean físicos o lógicos, entre los cuales se incluyen archivos, directorios y dispositivos. El control de acceso a los usuarios deberá por lo menos considerar:

- **I.** Altas y bajas de usuarios.
- **II.** Recursos asignados
- **III.** Permisos sobre los recursos asignados (lectura, escritura, ejecución y propiedad).
- **IV.** Límites o cuotas en el uso de los recursos asignados.
- **V.** Monitoreo de cuentas, bitácoras y diarios.
  - **a)** Periodicidad de uso
  - **b)** Tiempo estimado en cada uso.
  - **c)** Cambios de contraseñas.
  - **d)** Eliminación de cuentas de usuario que han finalizado su labor.
  - **e)** Vigilancia en la acumulación de privilegios o de privilegios inadecuados.
  - **f)** Definición de *revocación* de privilegios.

Artículo 17. El Responsable de seguridad de los datos personales de cada Área Universitaria debe presentar evidencia del cumplimiento de estas normas complementarias a solicitud de las autoridades y en los procesos periódicos de auditoría técnica interna.

Artículo 18. Los sistemas de información desarrollados y por desarrollar en las Áreas Universitarias para el tratamiento automatizado de datos personales, independientemente de su ubicación en equipos a cargo del Área Universitaria o en servicios de nube privada, deberán cumplir con lo siguiente *(ver "Anexo IV: Ruta crítica para el cumplimiento de las Medidas de Seguridad Técnicas" y "Anexo V. Formatos para el cumplimiento de las Medidas de Seguridad Técnicas")*:

- **I.** En las bases de datos y sistemas para el tratamiento de datos personales:
  - **a)** Utilizar los datos personales preexistentes que estén disponibles, de acuerdo con sus respectivas políticas de uso y acceso, en bases de datos a cargo de otras Áreas Universitarias.
  - **b)** Contar con entornos propios para desarrollo, pruebas y operación.
  - **c)** Utilizar datos no personales durante el desarrollo y pruebas de los sistemas.
  - **d)** Permitir el acceso al código fuente de los sistemas exclusivamente a la administración del sistema y personal para el desarrollo.
  - **e)** Asignar o revocar los privilegios de acceso para los usuarios teniendo como base el principio del menor privilegio.
  - **f)** Cumplir con las especificaciones de seguridad informática previo a la puesta en operación.
  - **g)** Instalar y mantener vigentes certificados de comunicación segura SSL en el caso de servicios basados en Web.
  - **h)** Definir el plan de respaldos de la información, incluyendo periodicidad y alcance.
  - **i)** Definir el procedimiento para el borrado seguro.
  - **j)** Los sistemas de tratamiento basados en servicios web deberán ser alojados dentro del dominio unam.mx, o en su caso, si se alojan en dominios ajenos, estos deberán de ser propiedad de la universidad y no de personas físicas.
- **II.** En los sistemas operativos y servicios:
  - **a)** Sincronizar la fecha y hora con el servidor NTP (*Network Time Protocol)* oficial de la Universidad.
  - **b)** Instalar y mantener actualizado el software antimalware.
  - **c)** Instalar las actualizaciones de seguridad más recientes disponibles.
- **III.** En los equipos de cómputo:
  - **a)** Utilizar equipos con componentes actualizados, protegidos con garantías y soporte, y con la capacidad suficiente para atender la demanda del servicio y de los usuarios.
  - **b)** Definir el programa de mantenimiento preventivo.

Artículo 19. Durante el tratamiento automatizado de los datos personales, los sistemas de información deberán cumplir lo siguiente, independientemente de su ubicación en equipos a cargo del Área Universitaria o en servicios de nube privada:

- **I.** En las bases de datos y sistemas para el tratamiento, se deberá:
  - **a)** Aplicar el mecanismo de autenticación para las personas autorizadas con base en el principio del menor privilegio.
  - **b)** Establecer las medidas de seguridad en los periodos de inactividad o mantenimiento.

c) Generar respaldos y aplicar los mecanismos de control y protección para su resguardo.

d) Impedir el uso de cuentas y servicios gestionados por personas físicas para el tratamiento de los datos personales.

II. En los sistemas operativos

a) Proteger ante manipulaciones indebidas y accesos no autorizados las bitácoras y los dispositivos donde se almacenan.

b) Evitar la instalación de cualquier elemento de software que implique algún riesgo para el tratamiento de datos personales.

III. En los equipos de cómputo

a) Establecer las medidas físicas de seguridad que controlen el acceso a los equipos.

b) Restringir la salida de equipos de las instalaciones de cada Área Universitaria.

c) Aplicar el programa de mantenimiento preventivo a los equipos.

IV. En la red de datos

a) Realizar la transmisión de datos personales a través de un canal cifrado.

b) Supervisar los controles de seguridad en la red de datos donde opere el sistema para tratamiento de datos personales.

c) Proporcionar el acceso exclusivamente desde redes y servicios autorizados.

Artículo 20. Independientemente de su ubicación en equipos a cargo del Área Universitaria o en servicios de nube privada, para la eliminación de datos personales, los sistemas de información que den tratamiento automatizado aplicarán el procedimiento de borrado seguro que impida la recuperación en las bases de datos y todos sus respaldos.

Artículo 21. Para sistemas que realicen el tratamiento automatizado de datos personales solo está permitido el uso de servicios de nube pública para el resguardo de archivos cifrados que contengan respaldos de la información.

CAPÍTULO III: MEDIDAS DE SEGURIDAD ADMINISTRATIVAS PARA LA PROTECCIÓN DE DATOS PERSONALES

Notificación de vulneraciones de seguridad

Artículo 22. El área universitaria, por conducto del Responsable de seguridad de datos personales, deberá notificar al titular de los datos personales y a la Unidad de Transparencia, para que ésta informe al Instituto las vulneraciones de seguridad que de forma significativa afecten los derechos patrimoniales o morales del titular dentro de un plazo máximo de setenta y dos horas, a partir de que confirme la ocurrencia de éstas y el Responsable haya empezado a tomar las acciones encaminadas a detonar un proceso de mitigación de la afectación.

El plazo a que se refiere el párrafo anterior comenzará a correr el mismo día natural en que el Responsable confirme la vulneración de seguridad.

Se entenderá que se afectan los derechos patrimoniales del titular cuando la vulneración esté relacionada, de manera enunciativa más no limitativa, con sus bienes muebles e inmuebles, información fiscal, historial crediticio, ingresos y egresos, cuentas bancarias, seguros, afores, fianzas, servicios contratados o las cantidades o porcentajes relacionados con la situación económica del titular.

Asimismo, se entenderá que se afectan los derechos morales del titular cuando la vulneración esté relacionada, de manera enunciativa más no limitativa, con sus sentimientos, afectos, creencias, decoro, honor, reputación, vida privada, configuración y aspecto físicos, consideración que de sí mismo tienen los demás, o cuando se menoscabe ilegítimamente la libertad o la integridad física o psíquica de éste.

Artículo 23. El Área Universitaria, por conducto del Responsable de seguridad de datos personales, deberá informar mediante escrito presentado en el domicilio del Instituto por conducto de la Unidad de Transparencia, o bien, a través de cualquier otro medio que se habilite para tal efecto, al menos, lo siguiente:

I. La hora y fecha de la identificación de la vulneración;
II. La hora y fecha del inicio de la investigación sobre la vulneración;
III. La naturaleza del incidente o vulneración ocurrida;
IV. La descripción detallada de las circunstancias en torno a la vulneración ocurrida;
V. Las categorías y número aproximado de titulares afectados;
VI. Los sistemas de tratamiento y datos personales comprometidos;
VII. Las acciones correctivas realizadas de forma inmediata;

VIII. La descripción de las posibles consecuencias de la vulneración de seguridad ocurrida;
IX. Las recomendaciones dirigidas al titular;
X. El medio puesto a disposición del titular para que pueda obtener más información al respecto;
XI. El nombre completo de la o las personas designadas y sus datos de contacto, para que puedan proporcionar más información al Instituto, en caso de requerirse, y
XII. Cualquier otra información y documentación que considere conveniente hacer del conocimiento del Instituto.

Notificación al titular de las vulneraciones de seguridad

Artículo 24. En la notificación que realice el área universitaria, por conducto del Responsable de seguridad de datos personales, al titular sobre las vulneraciones de seguridad se deberá informar, al menos, lo siguiente:

I. La naturaleza del incidente o vulneración ocurrida;
II. Los datos personales comprometidos;
III. Las recomendaciones dirigidas al titular sobre las medidas que éste pueda adoptar para proteger sus intereses;
IV. Las acciones correctivas realizadas de forma inmediata;
V. Los medios puestos a disposición del titular para que pueda obtener más información al respecto;
VI. La descripción de las circunstancias generales en torno a la vulneración ocurrida, que ayuden al titular a entender el impacto del incidente, y
VII. Cualquier otra información y documentación que considere conveniente para apoyar a los titulares.

El Responsable de seguridad de datos personales deberá notificar directamente al titular la información a que se refieren las fracciones anteriores a través de los medios que establezca para tal fin. Para seleccionar y definir los medios de comunicación, el Responsable deberá considerar el perfil de los titulares, la forma en que mantiene contacto o comunicación con éstos, que sean gratuitos; de fácil acceso; con la mayor cobertura posible y que estén debidamente habilitados y disponibles en todo momento para el titular.

Procedimiento específico para el ejercicio de derechos ARCO

Artículo 25. Independientemente del procedimiento que la Universidad tiene institucionalizado para la atención de solicitudes para el ejercicio de los derechos ARCO mediante la Plataforma Nacional de Transparencia o directamente ante la Unidad de Transparencia de la Universidad, las Áreas Universitarias, particularmente las foráneas, aplicarán el trámite para ejercicio de dichos derechos a través del "Formato universitario de solicitud de ejercicio de derechos ARCO", a fin de que los titulares de los datos personales puedan acreditar su identidad y, en su caso, la personalidad con la que actúa, en la sede universitaria donde fueron recabados sus datos personales así cómo los documentos que se deben acompañar para ejercer dichos derechos *(ver Anexo II. Formato universitario de solicitud de ejercicio de derechos ARCO).*

Capacitación

Artículo 26. El Área Universitaria deberá diseñar e implementar programas a corto, mediano y largo plazo que tengan por objeto capacitar a los involucrados internos y externos en su organización, de conformidad con los programas generales de capacitación que emita el Comité de Transparencia a propuesta de la Unidad de Transparencia, considerando sus roles y responsabilidades asignadas para el tratamiento y seguridad de los datos personales y el perfil de sus puestos.

En el diseño e implementación de los programas de capacitación a que se refiere el párrafo anterior del presente artículo, la Unidad de Transparencia deberá tomar en cuenta lo siguiente:

I. Los requerimientos y actualizaciones del sistema de gestión;
II. La legislación vigente en materia de protección de datos personales y las mejores prácticas relacionadas con el tratamiento de éstos;
III. Las consecuencias del incumplimiento de los requerimientos legales o requisitos organizacionales, y
IV. Las herramientas tecnológicas relacionadas o utilizadas para el tratamiento de los datos personales y para la implementación de las medidas de seguridad.

Seguridad vinculada con los recursos humanos

Artículo 27. El secreto o sigilo profesional, así como la confidencialidad y la no divulgación de la información, constituyen una obligación legal y ética de toda persona que desempeñe algún tipo de empleo, cargo o comisión en las Áreas

Universitarias, por lo que quienes acceden a ella deben asumir el compromiso de no revelarla o difundirla, de conformidad con las necesidades internas para la protección de los datos personales *(ver Anexo III. Carta de Confidencialidad).*

Artículo 28. Las áreas administrativas de las dependencias y entidades universitarias se asegurarán de que la salida de las personas que desempeñan un empleo, cargo o comisión en la Universidad, que por algún motivo tuvieron acceso a datos personales en posesión de la Universidad, sea definida y gestionada con la devolución de todo el equipamiento y la retirada de todos los derechos de acceso.

La comunicación de la finalización de las responsabilidades debería incluir los requisitos de seguridad y las responsabilidades legales en curso, para tal efecto, el superior jerárquico de la persona que se retira gestionará los aspectos de seguridad de los respectivos procedimientos e informará a las Áreas Universitarias vinculadas con el tratamiento de datos personales y al Responsable de seguridad de datos personales, la salida de dicha persona.

Artículo 29. Las unidades administrativas de las Áreas Universitarias supervisarán la devolución de los activos de la Universidad de quien finalice su empleo, cargo o comisión; la cual deberá formalizarse para incluir la devolución de todos los componentes de software, documentos institucionales, equipos, computadoras, tarjetas de acceso, software, manuales, así como la información almacenada en soporte electrónico.

Artículo 30. El derecho de acceso a datos personales y a los recursos de tratamiento de la información que tengan las personas que finalicen un empleo, cargo o comisión darán lugar a la revocación, reducción o adaptación de todos los derechos de acceso que no hayan sido aprobados para el nuevo puesto, incluyendo accesos físicos y lógicos, claves o contraseñas para cuentas, tarjetas de identificación, recursos de tratamiento de la información, suscripciones, así como la retirada de cualquier documentación que les identifique como un miembro actual de la Universidad.

CAPÍTULO IV: MEDIDAS DE SEGURIDAD FÍSICAS PARA LA PROTECCIÓN DE DATOS PERSONALES

Responsables de los datos personales que se resguardan en los archivos universitarios

Artículo 31. En el archivo de trámite, la persona titular del área productora será la responsable de custodiar y asegurar los documentos con datos personales; en el archivo de concentración la responsabilidad recae en la persona que funge como responsable de ese archivo.

Seguridad física y del entorno

Artículo 32. Las medidas de seguridad físicas que se establezcan en cada inmueble y sobre los archivos con datos personales deben ser proporcionales a los riesgos identificados por el Área Universitaria, para lo cual se podrán considerar los siguientes criterios:

- **I.** Localización del inmueble, equipamiento del archivo y las condiciones del acervo documental;
- **II.** Reconocimiento del entorno inmediato en el que está ubicada el Área Universitaria a través del diagnóstico de la zona en donde se identifican los riesgos y recursos potenciales de la zona;
- **III.** Identificación de las personas que asisten, actividades y horario de labores;
- **IV.** Determinación de fenómenos de carácter geológico, hidrometereológico, químico, tecnológico, sanitario, ecológico y organizativo que sean un riesgo o desastre al acervo documental, y
- **V.** Descripción de la infraestructura en la que se conozcan los antecedentes del inmueble como la antigüedad del edificio y del archivo; y

Artículo 33. Para que un Área Universitaria considere viable acondicionar un espacio físico para resguardar el material documental, debe atender a lo dispuesto en los Lineamientos Generales para la Organización, Administración y Conservación de los Archivos de la Universidad Nacional Autónoma de México y procurar se instalen en áreas seguras y perímetros definidos mediante barreras de seguridad y controles de entrada adecuados.

En todo caso, se deberán identificar las barreras de seguridad y controles de entrada con que cuenta el inmueble, tales como: barreras, muros, puertas de salida de emergencia, puertas con control de acceso a través de tarjeta, puestos de control o cualquier otro medio que el avance de la tecnología permita, a fin de evitar accesos no autorizados al perímetro de los archivos institucionales.

Artículo 34. Las Áreas Universitarias deberán implementar las medidas de seguridad física siguientes:

I. Acondicionar los espacios físicos diseñados y destinados a la recepción, organización, administración, resguardo y conservación, temporal o definitiva, del acervo documental con datos personales que poseen;
II. Establecer y mantener registros de la cadena de rendición de cuentas de los documentos físicos y electrónicos que contienen datos personales, desde la recepción hasta el destino final de la documentación, estableciendo procedimientos de control en la recepción, clasificación, registro, resguardo, traslados y préstamo de documentos y expedientes físicos;
III. Determinar controles específicos para impedir fotocopiar, escanear o fotografiar mediante cualquier dispositivo móvil documentos que contengan datos personales, por lo cual debe evitarse que las personas ingresen con algún dispositivo para tal efecto;
IV. Proteger el entorno físico del manejo, traslado, resguardo y acceso a los datos personales contenidos en los documentos de archivo generados y recibidos, así como de los recursos involucrados en su tratamiento, a fin de prevenir robos, daños, pérdidas, alteraciones, destrucción o su uso, acceso o tratamiento no autorizado, para garantizar su confidencialidad, integridad y disponibilidad.

Artículo 35. Los documentos y expedientes que contengan datos personales no deben ser expuestos a la vista o proporcionarse el acceso a personas no autorizadas, para tal efecto se sugiere atiendan lo siguiente:

I. Los documentos contarán con una guarda, ya sea folder o carpeta, y se integrarán en expedientes, conforme a la normativa institucional archivística; y
II. Los expedientes se resguardarán en el mobiliario institucional y aquellos que contengan datos personales se preservarán con mecanismos idóneos.

Controles físicos de ingreso a las instalaciones, archivos y soportes físicos

Artículo 36. Las áreas en que se ubiquen archivos que resguarden datos confidenciales en instalaciones universitarias considerarán, en la medida de sus posibilidades, los siguientes tipos de controles:

I. Solicitar una identificación oficial, registrar la fecha y la hora de entrada y salida de personas externas a las instalaciones y archivos, así como comprobar la autorización de la persona a quien visita;
II. Revisar periódicamente los registros de accesos;
III. Requerir a todos los visitantes portar un gafete con la leyenda de "visitante", en caso de identificarse una persona externa a las instalaciones o al archivo sin gafete o sin acompañamiento, notificar inmediatamente al personal de vigilancia para verificar su ingreso y anotarlo en su bitácora, y en caso de no estar autorizado, solicitar se retire; y
IV. Revisar y actualizar anualmente las autorizaciones para el acceso a las áreas seguras y archivos, e informar de las personas a las que se les revocó el acceso por causas inherentes a las bajas de personas por empleo, cargo o comisión.

Transitorios

PRIMERO. Las presentes Normas Complementarias y sus Anexos Técnicos entrarán en vigor al día siguiente de su publicación en Gaceta UNAM.

SEGUNDO. Se instruye a la Unidad de Transparencia para que realice las gestiones necesarias a efecto de que las presentes Normas Complementarias y sus Anexos Técnicos, se publiquen en el Portal de Internet de Transparencia. Las presentes normas y sus anexos pueden ser consultados en la dirección electrónica siguiente: **http://transparencia.unam.mx/documentos_transparencia/NormasComplementarias.zip**

TERCERO. Las Áreas Universitarias **contarán** con un periodo de treinta días hábiles, a partir de la entrada en vigor de las presentes Normas Complementarias y sus Anexos Técnicos, para implementar al interior de su organización, las medidas de seguridad correspondientes.

Aprobado por el Comité de Transparencia de la Universidad Nacional Autónoma de México en la Décima Quinta Sesión celebrada el 10 de enero de 2020.