EDUCACIÓN
SECRETARÍA DE EDUCACIÓN PÚBLICA

UNIVERSIDAD PEDAGÓGICA NACIONAL

POLÍTICA GENERAL DE GESTIÓN Y TRATAMIENTO DE DATOS PERSONALES DE LA UNIVERSIDAD PEDAGÓGICA NACIONAL

COMITÉ DE TRANSPARENCIA DE LA
UNIVERSIDAD PEDAGÓGICA NACIONAL

Índice de Contenido

Directorio

Comité de Transparencia de la Universidad Pedagógica Nacional:

Lic. Yiseth Osorio Osorio
Titular de la Unidad de Transparencia, en su carácter de presidenta del comité de transparencia

Lic. Ofelia del Pilar Enríquez Borobia
Titular del Órgano Interno de Control en la Universidad Pedagógica Nacional, en su carácter de Persona Integrante del comité de transparencia

Lic. Juan Carlos Negrete Acosta
Responsable del Área Coordinadora de Archivos, en su carácter de Persona Integrante del comité de transparencia

Lic. Mayra Paulina Pérez Pablo
Secretaria Técnica del comité de transparencia

Universidad Pedagógica Nacional

Carretera al Ajusco # 24, Col Héroes de Padierna, C.P.14200, Tlalpan, Ciudad de México; Tel. (55) 5630 9700, Ext. 1331; www.upn.mx.

Fecha de Aprobación:

Tercera Sesión Extraordinaria del año 2023 del Comité de Transparencia, celebrada el **20 de febrero de 2023**.

POLÍTICA GENERAL DE GESTIÓN Y TRATAMIENTO DE DATOS PERSONALES EN POSESIÓN DE LA UNIVERSIDAD PEDAGÓGICA NACIONAL

I. PRESENTACIÓN

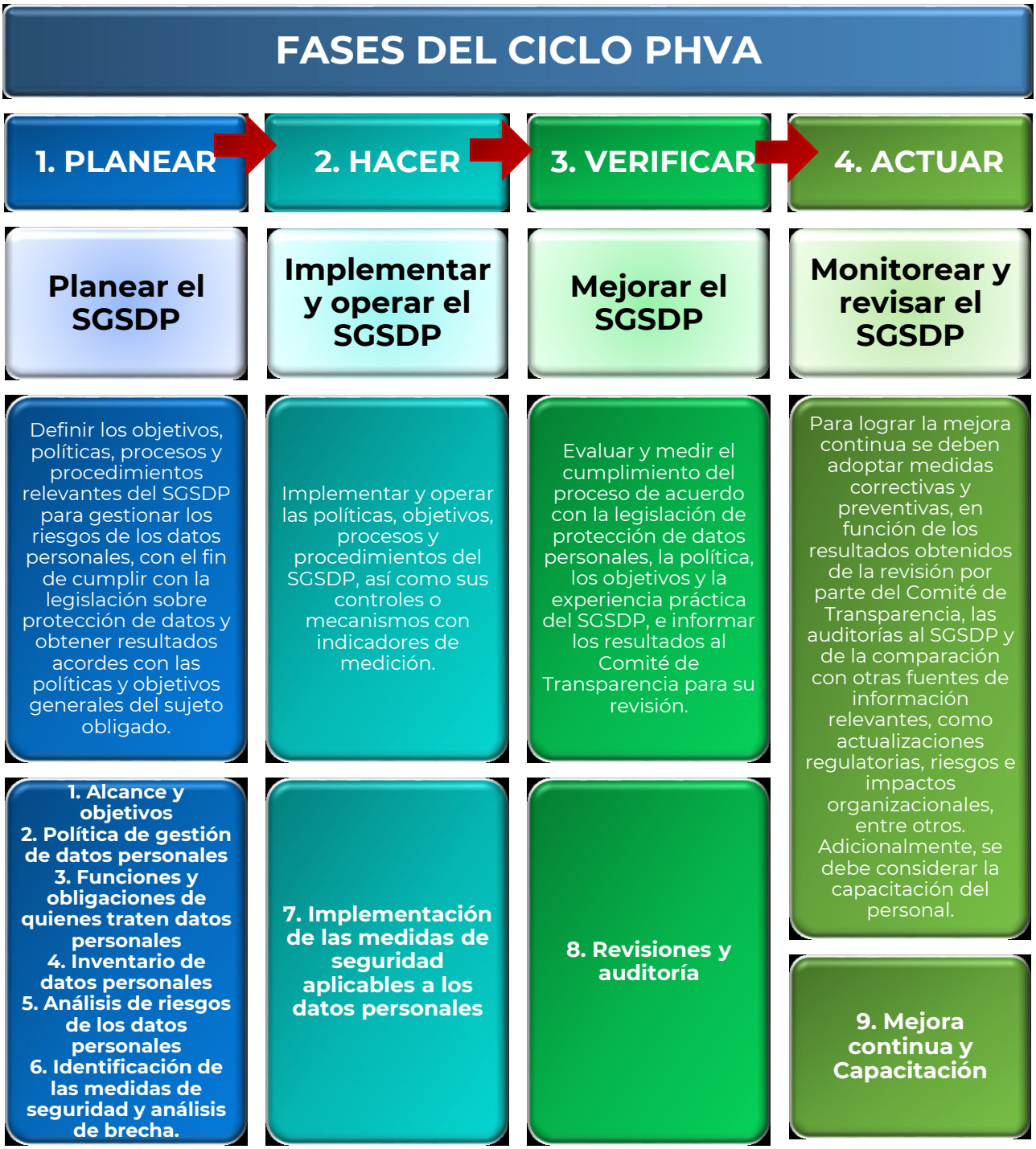
En cumplimiento a los artículos 30, fracciones II y IV, 33, fracción I, de la *Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados* (LGPDPPSO), así como los artículos 46, 47, 51 y 56 de los *Lineamientos Generales de Protección de Datos Personales para el Sector Público* (Lineamientos Generales), el presente documento establece la política general de gestión y tratamiento de datos personales en posesión de la Universidad Pedagógica Nacional.

De acuerdo con las disposiciones normativas antes invocadas, los sujetos obligados debemos incorporar a su normativa interna políticas que aseguren el buen manejo y tratamiento de los datos personales y que los sistemas que los soportan sean eficaces y útiles, de tal forma que establezcan pautas, obligaciones y responsabilidades para el personal que trata datos personales en su posesión, lo que permitirá establecer un mecanismo para el cumplimiento del **principio de responsabilidad**, pero también del **deber de seguridad** establecidos en la Ley General de la materia, ya que las políticas de gestión y tratamiento de datos personales que son obligación legal para los responsables, así como políticas de seguridad complementarias son medidas de seguridad administrativas conforme a lo establecido en el artículo 3, fracción XXI de la LGPDPPSO.

Ahora bien, no pasa desapercibido que de acuerdo con lo establecido en la normatividad aplicable a la materia, las políticas deben ser también resultado de la labor realizada durante la implementación de un **Sistema de Gestión de Seguridad de Datos Personales (SGSDP)**, en tanto que éste tiene como objetivo proveer un marco de trabajo para el tratamiento de datos personales que permita mantener vigente y mejorar la protección de datos personales para el cumplimiento de la legislación y fomentar las buenas prácticas.

Bajo este contexto, cabe señalar que el SGSDP se basa en el ciclo PDCA, por sus siglas en inglés (Plan, Do, Check, Act) y traducido al español PHVA (Planear, Hacer, Verificar, Actuar)[1], donde se consideran diferentes **pasos y objetivos de acuerdo a cada fase del ciclo**, que pueden observarse en el siguiente esquema:

[1] *Guía para implementar un Sistema de Gestión de Seguridad de Datos Personales*. Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), 2015, página 7 y 8. Disponible para consulta en: https://home.inai.org.mx/wp-content/documentos/DocumentosSectorPrivado/Gu%C3%ADa_Implementaci%C3%B3n_SGSDP(Junio2015).pdf



De lo anterior, se desprende que **la elaboración de las políticas de gestión de tratamientos de datos personales se encuentra en la primera fase de un SGSDP**, esto es, en la fase de planeación, y debe ser el

resultado de haber analizado el contexto del sujeto obligado, en este caso, de la Universidad Pedagógica Nacional, en cuanto a:

- Los procesos donde se tratan datos personales o se operan sistemas de tratamiento.
- El alcance del sistema, es decir, las áreas que participan en el tratamiento de datos u operan estos sistemas, o bien, que participan en algún momento del ciclo de vida de los datos.
- La identificación de los activos: los datos personales y los sistemas de tratamiento, así como su ciclo de vida y los custodios de éstos.
- Las personas servidoras públicas que participan en los procesos de tratamiento.
- El análisis de riesgos.
- Las medidas de seguridad actuales, así como saber identificar las que se pretenden implementar de acuerdo a los valores obtenidos del riesgo residual.

No obstante, si bien la política de gestión y tratamiento de datos personales se establece como el segundo paso a seguir del proceso de planeación de un SGSDP, no necesariamente debe finalizarse para continuar con los siguientes pasos, sino que **puede comenzar a redactarse de forma general cuando se tenga el alcance y los objetivos del SGSDP**, e irse construyendo a lo largo de todo el proceso de planeación, inclusive deben elaborarse políticas adicionales de acuerdo a las medidas de seguridad identificadas que deben comenzar a operar en la Institución como resultado del análisis de riesgos y el análisis de brecha, así como procedimientos específicos por Área como complemento a esas políticas, de acuerdo al contexto y las necesidades de esta Casa de Estudios.

Partiendo de lo dicho en el párrafo que antecede y ante la necesidad primaria que tiene la Universidad Pedagógica Nacional para regular la gestión, el tratamiento y la protección de los datos personales en posesión de esta Institución, en uso de la función contenida en la fracción I del artículo 84 de la LGPDPPSO, el Comité de Transparencia de esta Universidad considera prioritario establecer, a través del presente documento, las bases generales que permitan a cada Área, así como a cada persona servidora pública responsable del tratamiento de datos personales, dar cumplimiento a sus obligaciones que devienen de los **deberes y principios** que rigen la materia de protección de datos personales, cumplimiento que a la par debe estar documentado a través del **Documento de Seguridad** que corresponda.

Así, es importante establecer que en el ámbito de seguridad de la información, una **política de seguridad** es aquel "*…documento que describe los requisitos o reglas específicas que deben cumplirse en una organización. Presenta una declaración formal, breve y de alto nivel, que abarca las creencias generales de la organización, metas, objetivos y procedimientos aceptables para un área determinada*"[2]. Bajo este contexto, **la *Política General de Gestión y Tratamiento de Datos Personales de la Universidad Pedagógica Nacional* que se establecerá con el presente documento, describirá los requisitos o reglas específicas que deberán cumplirse al interior de esta Casa de Estudios (Unidad 092, Ajusco; y Unidades UPN, Ciudad de México), con apego a lo establecido en la LGPDPPO**.

En este sentido, la *Política General de Gestión y Tratamiento de Datos Personales de la Universidad Pedagógica Nacional* será de **observancia obligatoria y exigible** al interior de esta Casa de Estudios y, en su caso, a encargados.

[2] *Recomendaciones para la elaboración de Políticas internas de gestión y tratamiento de datos personales (Sector Público)*. Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), Mayo 2022, página 11. Disponible para consulta en: https://home.inai.org.mx//wp-content/documentos/DocumentosSectorPublico/RecomendacionesPol%C3%ADticasPDP.pdf

II. Glosario de Términos

Activo de Información (Activo): Es cualquier información o sistema relacionado con el tratamiento de la misma que tenga valor para la organización, pueden ser procesos de negocio, datos, aplicaciones, equipos informáticos, personal, soportes de información, redes, equipamiento auxiliar o instalaciones. Es susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización.[3]

Áreas: Instancias de la Universidad Pedagógica Nacional previstas en el Decreto de Creación, en el Manual de Organización de esta Casa de Estudios, o bien, en los respectivos reglamentos interiores o instrumentos equivalentes, que traten datos personales.

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 los mismos.[4]

Bases de datos. El conjunto ordenado de datos personales referentes a una persona física identificada o identificable en posesión de la Universidad Pedagógica Nacional, condicionados a criterios determinados, con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización.

Comité de Transparencia: Instancia de la Universidad Pedagógica Nacional a la que hace referencia el artículo 43 de la *Ley General de Transparencia y Acceso a la Información Pública*, cuyas funciones en materia de protección de datos personales se encuentran conferidas en el artículo 84 de la *Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados*.

Confidencialidad. Es la propiedad de la información, por la que se garantiza que está accesible únicamente a personal autorizado a acceder a dicha información. La confidencialidad de la información constituye la piedra angular de la seguridad de la información. Junto con la integridad y la disponibilidad, suponen las tres dimensiones de la seguridad de la información.[5]

Consentimiento: Manifestación de la voluntad libre, específica e informada del titular de los datos mediante la cual se efectúa el tratamiento de los mismos.[6]

Custodios. Son aquéllos con responsabilidad funcional sobre los activos, como: los responsables del departamento de datos, administradores de sistemas o responsables de un proceso o de un proyecto en específico, entre otros.[7]

---

[3] *Glosario de términos de ciberseguridad. Una guía de aproximación para el empresario*. Instituto Nacional de Ciberseguridad de España (INCIBE), 2021, página 12. Disponible para consulta en: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_2021.pdf

[4] Fracción II del artículo 3 de la LGPDPPSO.

[5] *Glosario de términos de ciberseguridad. Una guía de aproximación para el empresario*. Instituto Nacional de Ciberseguridad de España (INCIBE), 2021, página 30. Disponible para consulta en: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_2021.pdf

[6] Fracción II del artículo 3 de la LGPDPPSO.

[7] *Guía para implementar un Sistema de Gestión de Seguridad de Datos Personales*. Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), 2015, página 4. Disponible para consulta en: https://home.inai.org.mx/wp-content/documentos/DocumentosSectorPrivado/Gu%C3%ADa_Implementaci%C3%B3n_SGSDP(Junio2015).pdf

Datos personales. Cualquier información concerniente a una persona física identificada o identificable. Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información.[8]

Datos personales sensibles: Aquellos que se refieran a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. De manera enunciativa más no limitativa, se consideran sensibles los datos personales que puedan revelar aspectos como origen racial o étnico, estado de salud presente o futuro, información genética, creencias religiosas, filosóficas y morales, opiniones políticas y preferencia sexual.[9]

Derechos ARCO: Derechos de acceso, rectificación, cancelación y oposición al tratamiento de datos personales.

Días: Días hábiles.

Disociación: Procedimiento mediante el cual los datos personales no pueden asociarse a su titular, ni permitir, por su estructura, contenido o grado de desagregación, la identificación del mismo.

Disponibilidad: Se trata de la capacidad de un servicio, un sistema o una información, a ser accesible y utilizable por los usuarios o procesos autorizados cuando éstos lo requieran.[10]

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.[11]

Encargado. Persona física o jurídica, pública o privada, ajena a la organización de la Universidad Pedagógica Nacional, que sola o conjuntamente con otras, trate datos personales a nombre y por cuenta de esta Institución.

Evaluación de impacto en la protección de datos personales: Documento mediante el cual alguna área que pretenda 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, valorará los impactos reales respecto de 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.

LGPDPPSO o Ley General. Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

---

[8] Fracción IX del artículo 3 de la LGPDPPSO.
[9] Fracción X del artículo 3 de la LGPDPPSO.
[10] *Glosario de términos de ciberseguridad. Una guía de aproximación para el empresario*. Instituto Nacional de Ciberseguridad de España (INCIBE), 2021, página 38. Disponible para consulta en: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_2021.pdf
[11] Fracción XIV del artículo 3 de la LGPDPPSO.

Lineamientos Generales. Lineamientos Generales de Protección de Datos Personales para el Sector Público.

Identificar el riesgo. Proceso para encontrar, enlistar y describir los elementos del riesgo.[12]

Integridad. La Integridad es la propiedad de la información, por la que se garantiza la exactitud de los datos transportados o almacenados, asegurando que no se ha producido su alteración, pérdida o destrucción, ya sea de forma accidental o intencionada, por errores de software o hardware o por condiciones medioambientales.[13]

INAI o Instituto. Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.

Medidas compensatorias: Mecanismos alternos para dar a conocer a los titulares el aviso de privacidad, a través de su difusión por medios masivos de comunicación u otros de amplio alcance.[14]

Medidas de seguridad: Conjunto de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permitan proteger los datos personales en posesión de la Universidad Pedagógica Nacional.

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 adscrito a la Universidad Pedagógica Nacional en materia de protección de datos personales.

Medidas de seguridad físicas: Conjunto de acciones y mecanismos para proteger el entorno físico de los datos personales en posesión de las áreas que integran la Universidad Pedagógica Nacional y de los recursos involucrados en su tratamiento. De manera enunciativa más no limitativa, se describen algunas actividades a realizar:

a) Prevenir el acceso no autorizado al perímetro de la Universidad Pedagógica Nacional, sus instalaciones físicas, áreas críticas, recursos e información;
b) Prevenir el daño o interferencia a las instalaciones físicas, áreas críticas de la Universidad Pedagógica Nacional, recursos e información;
c) Proteger los recursos móviles, portátiles y cualquier soporte físico o electrónico que pueda salir de la Universidad Pedagógica Nacional, y
d) Proveer a los equipos que contienen o almacenan datos personales en posesión de la Universidad Pedagógica Nacional de un mantenimiento eficaz que asegure su disponibilidad e integridad.

[12] *Guía para implementar un Sistema de Gestión de Seguridad de Datos Personales*. Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), 2015, página 5. Disponible para consulta en: https://home.inai.org.mx/wp-content/documentos/DocumentosSectorPrivado/Gu%C3%ADa_Implementaci%C3%B3n_SGSDP(Junio2015).pdf
[13] *Glosario de términos de ciberseguridad. Una guía de aproximación para el empresario*. Instituto Nacional de Ciberseguridad de España (INCIBE), 2021, página 52. Disponible para consulta en: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_2021.pdf
[14] Fracción XIX del artículo 3 de la LGPDPPSO.

Medidas de seguridad técnicas: Conjunto de acciones y mecanismos que se valen de la tecnología relacionada con hardware y software para proteger el entorno digital de los datos personales en posesión de las áreas que integran la Universidad Pedagógica Nacional y los recursos involucrados en su tratamiento. De manera enunciativa más no limitativa, se deben considerar las siguientes actividades:

- **a)** Prevenir que el acceso a las bases de datos o a la información, así como a los recursos, sea por usuarios identificados y autorizados por la Universidad Pedagógica Nacional;
- **b)** Generar un esquema de privilegios para que el usuario lleve a cabo 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 propiedad o en posesión (bajo cualquier figura) de la Universidad Pedagógica Nacional, y
- **d)** Gestionar las comunicaciones, operaciones y medios de almacenamiento de los recursos informáticos en el tratamiento de datos personales en posesión de las áreas que integran Universidad Pedagógica Nacional.

Política: Política General de Gestión y Tratamiento de Datos Personales de la Universidad Pedagógica Nacional.

Remisión: Toda comunicación de datos personales realizada exclusivamente entre la Universidad Pedagógica Nacional y el encargado, dentro o fuera del territorio mexicano.

Responsable. Titular del área de la Universidad Pedagógica Nacional que decida sobre el tratamiento de los datos personales en su posesión.

Riesgo. Combinación de la probabilidad de un evento y su consecuencia desfavorable.[15]

Seguridad de la información. Preservación de la confidencialidad, integridad y disponibilidad de la información, así como otras propiedades delimitadas por la normatividad aplicable.

Sistema de Gestión de Seguridad de Datos Personales (SGSDP). Conjunto de elementos y actividades interrelacionadas para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el tratamiento y seguridad de los datos personales, de conformidad con lo previsto en la LGPDPSP y las demás disposiciones que le resulten aplicables en la materia de protección de datos personales.

Sujeto obligado. Universidad Pedagógica Nacional, específicamente a la Unidad 092, Ajusco, así como a las Unidades UPN Ciudad de México, que en el ejercicio de sus atribuciones y funciones llevan a cabo tratamientos de datos personales de personas físicas o jurídicas, en términos de lo dispuesto en la LGPDPPSO y los Lineamientos Generales.

Supresión: Baja archivística de los datos personales, conforme a la normativa archivística aplicable, que resulte en la eliminación, borrado o destrucción de los datos personales en posesión de alguna área de la Universidad Pedagógica Nacional, bajo las medidas de seguridad previamente establecidas.

[15] *Guía para implementar un Sistema de Gestión de Seguridad de Datos Personales*. Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), 2015, página 4. Disponible para consulta en: https://home.inai.org.mx/wp-content/documentos/DocumentosSectorPrivado/Gu%C3%ADa_Implementaci%C3%B3n_SGSDP(Junio2015).pdf

Titular: La persona física o jurídica a quien corresponden los datos personales en posesión de la Universidad Pedagógica Nacional.

Transferencia: Toda comunicación de datos personales dentro o fuera del territorio mexicano, realizada a persona distinta del titular, de la Universidad Pedagógica Nacional o del encargado.

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 en posesión de la Universidad Pedagógica Nacional, específicamente a la Unidad 092, Ajusco, así como a las Unidades UPN Ciudad de México.

Tratar el riesgo. Procesos que se realizan para modificar el nivel de riesgo.[16]

Unidad de Transparencia: Instancia a la que hace referencia el artículo 45 de la *Ley General de Transparencia y Acceso a la Información Pública*, cuyas funciones en materia de protección de datos personales se encuentran establecidas en el artículo 85 de la LGPDPPSO.

UPN. Universidad Pedagógica Nacional, específicamente a la Unidad 092, Ajusco, así como a las Unidades UPN Ciudad de México.

Valorar el riesgo. Proceso para asignar valores a la probabilidad y consecuencias del riesgo (impacto).[17]

[16] *Ibídem*
[17] *Ibídem*

III. Marco Jurídico

- Constitución Política de los Estados Unidos Mexicanos
- Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados
- Ley General de Transparencia y Acceso a la Información Pública
- Ley General de Archivos
- Ley General de Educación
- Ley General de Educación Superior
- Ley Federal de Transparencia y Acceso a la Información Pública
- Lineamientos Generales de Protección de Datos Personales para el Sector Público
- Decreto que crea la Universidad Pedagógica Nacional
- Manual de Organización de la Universidad Pedagógica Nacional

IV. OBJETIVO

La *Política General de Gestión y Tratamiento de Datos Personales de la Universidad Pedagógica Nacional* tiene como objetivo **establecer los requisitos o reglas específicas que deberán cumplirse al interior de esta Institución Educativa** (Unidad 092, Ajusco; y Unidades UPN, Ciudad de México), de tal forma que se consolide como una **declaración formal, breve y de alto nivel** al interior de este sujeto obligado de la LGPDPPSO, acorde con nuestro propio contexto, misión, finalidades y competencia como Institución, buscando así una armonización con la implementación del Sistema de Gestión de Seguridad de Datos Personales.

Asimismo, será un control o medida de seguridad a valorar en el SGSDP, permitiendo regular las acciones permitidas y no permitidas respecto al tratamiento de datos personales, los roles y responsabilidades, y las consecuencias ante el incumplimiento, así como reiterar los principios y obligaciones que tienen todas las personas servidoras públicas que realicen tratamiento de datos personales y establecer las medidas de seguridad a operar dentro de la UPN para la seguridad de la información.

En ese sentido, la *Política General de Gestión y Tratamiento de Datos Personales de la Universidad Pedagógica Nacional* **regirá en lo general**, siendo un referente para el caso de que se elaboren políticas complementarias en función de los controles o medidas de seguridad que se mantengan e implementen en la institución derivado del SGSDP, pudiéndose elaborar procedimientos o manuales por área, o bien, por proceso de tratamiento de datos, donde se establezcan los controles específicos y la forma de operarlos, en caso de ser necesario.

V. Alcances y Objetivos de la Gestión y Tratamiento de Datos Personales

En el presente apartado se definirán los alcances y objetivos de la gestión de datos personales, esto acorde a la definición de los límites en la aplicación del Sistema de Gestión de Seguridad de los Datos Personales.

Para definir los alcances y objetivos debe entenderse el contexto de esta Universidad, tanto interno como externo, además de su misión, visión y principios generales que la orientan. En el caso de la **misión**, la Universidad Pedagógica Nacional es una institución pública de educación superior, con vocación nacional y plena autonomía académica; se orienta a la formación y desarrollo de profesionales de la educación y a la generación de conocimiento de acuerdo con las necesidades del país considerando la diversidad sociocultural. A partir de sus funciones sustantivas se vincula con el sector educativo, con organizaciones sociales e instituciones nacionales e internacionales, con el fin de atender la problemática educativa y el fomento a la cultura. Respecto de la **visión**, se puede decir que esta Casa de Estudios tiene un lugar estratégico en la discusión e instrumentación crítica de las políticas públicas educativas, y la atención a temas y problemas emergentes; se distingue por su vocación social y su compromiso ético con la justicia, la equidad y su especial consideración a los grupos en situación de discriminación o exclusión social. Y, en lo relativo a los **principios generales que orientan a la UPN**, esta Universidad es una institución de educación superior, laica, pública y gratuita que atiende necesidades educativas, en congruencia con las demandas previsibles o emergentes de la sociedad, planteadas en la diversidad del contexto político, económico cultural y social del país.

Luego entonces, tomando en consideración la misión, visión y principios generales que orientan a la Universidad Pedagógica Nacional, a continuación se definen los **alcances de la gestión** de datos personales:

- Las actividades que desarrollan las Áreas de la UPN que, derivado de sus facultades y competencias, conlleven el tratamiento de datos personales.
- Todas las Áreas de la UPN que derivado del ejercicio de sus funciones y competencias deban tratar datos personales.
- Los procesos que impliquen el tratamiento de datos personales.
- La protección de los datos personales y sistemas de tratamiento en la UPN, considerando en todo momento el SGSDP y los Documentos de Seguridad que correspondan.
- La definición que cada Área deberá establecer respecto de los requisitos de seguridad de los datos personales que trata.
- La responsabilidad de cada Área de considerar la criticidad de los datos y los sistemas del tratamiento que pueden causar un gran impacto en los titulares como resultado de pérdidas de confidencialidad, integridad o disponibilidad; esto es, que cada Área deberá determinar cómo y por qué esos datos y esos sistemas son críticos. Para lo cual, deberán analizar los tipos de datos personales que tratan, es decir, si son datos personales sensibles, la cantidad de datos personales que se tratan, el posible impacto a las personas titulares.
- El alcance y los límites que cada Área que trate datos personales deberá prever respecto de la Tecnología de la Información y Comunicación (TIC) que se utilicen para el tratamiento de datos personales.

- El alcance físico y los límites de las instalaciones o ubicaciones que las Áreas deberán establecer, es decir, deberán considerar sus ubicaciones, el formato en el que se conservan (archivo físico, digitalizado o electrónico), así como el tipo de tecnologías que se utilizan.
- Cada Área deberá determinar si requiere que partes externas, como proveedores, cumplan con el SGSDP y el Documento de Seguridad, por ejemplo, si personal externo de limpieza u otro tipo de proveedores que ingresen a las instalaciones por cualquier razón, durante su ingreso o interacción con esta Universidad tienen acceso a los datos personales.
- Cuando derivado de sus actividades un Área requiera de interfaces o dependencias externas o de actividades realizadas por terceros, deberá determinar si éstos serán considerados dentro del alcance del SGSDP y del Documento de Seguridad respectivo. Debe considerarse, por ejemplo, si se ha contratado servicios en la nube, o servicios técnicos que tengan acceso remoto a los datos personales o a los sistemas de tratamiento.

Por cuanto hace a los **objetivos de seguridad**, éstos se enfocan a que con el presente instrumento se dé cumplimiento a lo establecido en la LGDPPSO y los Lineamientos Generales, principalmente el cumplimiento a obligaciones, deberes y principios contenidos en dicha normativa.

VI. Contenido de la Política General de Gestión y Tratamiento de Datos Personales de la Universidad Pedagógica Nacional

En cumplimiento a lo establecido en el artículo 56 de los Lineamientos Generales, en relación con el artículo 33, fracción I de la LGPDPPSO, la *Política General de Gestión y Tratamiento de Datos Personales de la Universidad Pedagógica Nacional* se desarrolla conforme a lo siguiente:

6.1. Cumplimiento a todos los principios, deberes, derechos y demás obligaciones en la materia, de conformidad con lo previsto en la Ley General y los Lineamientos Generales.

Todas las personas servidoras públicas y encargados involucrados en el tratamiento de datos personales, deben **comprometerse a cumplir** con la normatividad aplicable a la materia de protección de datos personales, así como atender las siguientes **reglas**:

1. Todas las personas servidoras públicas que por algún motivo traten datos personales, deberán hacerlo conforme a los **principios** que establece el artículo 16 de la Ley General: licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad, conforme a lo que señala dicho ordenamiento, los Lineamientos Generales y demás normativa aplicable.

2. Todas las personas servidoras públicas que por algún motivo traten datos personales, deberán hacerlo conforme a los **deberes** establecidos en el Capítulo II del Título Segundo de la LGPDPPSO, los Lineamientos Generales y demás normativa aplicable.

3. Tratar y recabar datos personales de manera **lícita**, conforme a las disposiciones establecidas por la Ley General, los Lineamientos Generales y demás normativa aplicable. (Principio de licitud)

4. Sujetar el tratamiento de datos personales al **consentimiento** de la persona titular, salvo las excepciones previstas por la Ley General y los Lineamientos Generales. (Principio de consentimiento)

5. Informar a las personas titulares de los datos, la información que se recaba de ellos y con qué fines, a través del **aviso de privacidad**. (Principio de información)

6. Procurar que los datos personales tratados sean **correctos, completos y actualizados**. (Principio de calidad)

7. **Suprimir** los datos personales cuando hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas en el aviso de privacidad y para las cuales se obtuvieron. (Principio de calidad)

8. Tratar datos personales estrictamente el **tiempo necesario** para propósitos legales, regulatorios o legítimos organizacionales. (Principio de calidad)

9. Limitar el tratamiento de los datos personales al cumplimiento de las **finalidades** previstas en el aviso de privacidad. (Principio de finalidad)

10. No obtener los datos personales a través de **medios fraudulentos**. (Principio de lealtad)

11. Respetar la expectativa razonable de **privacidad** de la persona titular. (Principio de lealtad)

12. Tratar los **menos datos personales posibles** y sólo aquéllos que resulten necesarios, adecuados y relevantes, en relación con las finalidades previstas en el aviso de privacidad. (Principio de proporcionalidad).

13. Velar por el **cumplimiento** de estos principios y adoptar las medidas necesarias para su aplicación. (Principio de responsabilidad)

14. Asegurarse de que, previo al tratamiento de datos personales, se cuente con el **Documento de Seguridad** respectivo.

15. Establecer y mantener **medidas de seguridad** conforme a lo establecido en el Documento de Seguridad que corresponda. (Deber de seguridad)

16. Guardar la **confidencialidad** de los datos personales. (Deber de confidencialidad)

17. Identificar el **flujo y ciclo de vida** de los datos personales: por qué medio se recaban, en qué procesos de la organización se utilizan, con quién se comparten, y en qué momento y por qué medios se suprimen.

18. Mantener un **inventario actualizado** de los datos personales o de sus categorías que maneja el responsable.

19. Respetar los **derechos** de las personas titulares en relación con sus datos personales.

20. Desarrollar e implementar un **SGSDP** de acuerdo con la política de gestión de datos personales.

21. Definir las partes interesadas y miembros de cada Área con **responsabilidades específicas** y a cargo de la rendición de cuentas para el SGSDP.

22. Las demás que deriven de cualquier normatividad que prevea la protección de datos personales en posesión de la Universidad Pedagógica Nacional.

6.2. Roles y responsabilidades específicas de los involucrados internos y externos dentro de la UPN, relacionados con los tratamientos de datos personales que se efectúen.

Todas las Áreas que integran a la UPN involucradas en cualquier tratamiento de datos personales, por conducto de las personas titulares, deberán tener el compromiso de cubrir las necesidades operativas y técnicas para mantener la adecuada seguridad de los datos personales conforme a la LGPDPPSO y los Lineamientos Generales.

Asimismo, cada Área deberá asignar las responsabilidades para llevar a cabo las tareas específicas de seguridad de los datos personales, designando a las personas servidoras públicas adecuadas, para lo cual, podrán nombrar a los responsables para la seguridad de los datos personales que traten, los responsables de los sistemas de tratamiento y custodios de la información que contiene datos personales, especificando la cadena de custodia de los mismos, conforme al artículo 57 de los Lineamientos generales, es decir, podrán establecer y documentar los roles y responsabilidades, así como la cadena de rendición de cuentas de todas las personas que traten datos personales en el Área.

En este mismo tenor, las personas titulares de cada Área deberán asegurar que todas las personas involucradas en el tratamiento de datos personales en su organización, conozcan sus funciones para el cumplimiento de los objetivos de la presente Política, de cada Documento de Seguridad que le corresponda, así como del SGSDP, así como las consecuencias de su incumplimiento.

Para atender este apartado, podrá utilizarse la documentación que integra el Documento de Seguridad, específicamente la fracción II del artículo 35 de la Ley General, que refiere a las funciones y obligaciones de las personas que tratan datos personales.

6.3. Sanciones en caso de incumplimiento.

De conformidad con lo establecido en el artículo 163 de la LGPDPPSO, serán causas de sanción por incumplimiento a las obligaciones que dicho ordenamiento legal, las siguientes:

I. Actuar con negligencia, dolo o mala fe durante la sustanciación de las solicitudes para el ejercicio de los derechos ARCO.

II. Incumplir los plazos de atención previstos en la Ley General para responder las solicitudes para el ejercicio de los derechos ARCO o para hacer efectivo el derecho de que se trate.

III. Usar, sustraer, divulgar, ocultar, alterar, mutilar, destruir o inutilizar, total o parcialmente y de manera indebida datos personales, que se encuentren bajo su custodia o a los cuales tengan acceso o conocimiento con motivo de su empleo, cargo o comisión.

IV. Dar tratamiento, de manera intencional, a los datos personales en contravención a los principios y deberes establecidos en la LGPDPPSO.

V. No contar con el aviso de privacidad, o bien, omitir en el mismo alguno de los elementos a que refiere el artículo 27 de la Ley General, según sea el caso, y demás disposiciones que resulten aplicables en la materia.

VI. Clasificar como confidencial, con dolo o negligencia, datos personales sin que se cumplan las características señaladas en las leyes que resulten aplicables. La sanción sólo procederá cuando exista una resolución previa, que haya quedado firme, respecto del criterio de clasificación de los datos personales.

VII. Incumplir el deber de confidencialidad establecido en el artículo 42 de la LGPDPPSO.

VIII. No establecer las medidas de seguridad en los términos que establecen los artículos 31, 32 y 33 de la Ley General.

IX. Presentar vulneraciones a los datos personales por la falta de implementación de medidas de seguridad según los artículos 31, 32 y 33 de la presente Ley.

X. Llevar a cabo la transferencia de datos personales, en contravención a lo previsto en la LGPDPPSO.

XI. Obstruir los actos de verificación de la autoridad.

XII. Crear bases de datos personales en contravención a lo dispuesto por el artículo 5 de la Ley General.

XIII. No acatar las resoluciones emitidas por el INAI y los Organismos garantes.

XIV. Omitir la entrega del informe anual y demás informes a que se refiere el artículo 44, fracción VII de la *Ley General de Transparencia y Acceso a la Información Pública*, o bien, entregar el mismo de manera extemporánea.

En el caso de las causas de responsabilidad previstas en las fracciones I, II, IV, VI, X, XII, y XIV del artículo 163 de la LGPDPPSO, así como la reincidencia en las conductas previstas en el resto de las fracciones de este artículo, serán consideradas como graves para efectos de su sanción administrativa.

Es importante señalar que, de acuerdo con lo referido en el artículo 165 de la LGPDPPSO, los incumplimientos de la Ley General pueden derivar, además de en faltas administrativas, en delitos y responsabilidades civiles, dichas responsabilidades se determinarán, en forma autónoma, a través de los procedimientos previstos en las leyes aplicables y las sanciones que, en su caso, se impongan por las autoridades competentes, ejecutándose de manera independiente.

Asimismo, las sanciones de carácter económico no podrán ser cubiertas con recursos públicos.

6.4. IDENTIFICACIÓN DEL CICLO DE VIDA DE LOS DATOS PERSONALES RESPECTO DE CADA TRATAMIENTO QUE SE EFECTÚE; CONSIDERANDO LA OBTENCIÓN, ALMACENAMIENTO, USO, PROCESAMIENTO, DIVULGACIÓN, RETENCIÓN, DESTRUCCIÓN O CUALQUIER OTRA OPERACIÓN REALIZADA DURANTE DICHO CICLO EN FUNCIÓN DE LAS FINALIDADES PARA LAS QUE FUERON RECABADOS.

Es responsabilidad de cada Área elaborar el **inventario de datos personales y de sistemas de tratamiento** conforme a los artículos 58 y 59 de los Lineamientos Generales, el cual debe contener la información básica de cada tratamiento de datos personales, considerando al menos los siguientes **elementos**:

1. El catálogo de los medios físicos y electrónicos a través de los cuales se obtienen los datos personales.
2. Las finalidades de cada tratamiento de datos personales.
3. El catálogo de los tipos de datos personales que se traten, indicando si son sensibles o no.
4. El catálogo de formatos de almacenamiento, así como la descripción general de la ubicación física y/o electrónica de los datos personales.
5. La lista de las personas servidoras públicas que tienen acceso a los sistemas de tratamiento.
6. 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 responsable, y
7. En su caso, los destinatarios o terceros receptores de las transferencias que se efectúen, así como las finalidades que justifican éstas.

Asimismo, de acuerdo con el artículo 59 de la LGPDPPSO, el inventario también deberá considerar el **ciclo de vida** de los datos personales conforme a lo siguiente:

a) La obtención de los datos personales.
b) El almacenamiento de los datos personales.
c) 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.
d) La divulgación de los datos personales considerando las remisiones y transferencia que, en su caso, se efectúen.
e) El bloqueo de los datos personales, en su caso, y
f) La cancelación, supresión o destrucción de los datos personales.

Una vez integrado el inventario, mismo que puede ser integrado con los insumos del Documento de Seguridad respectivo, éste deberá ser hecho del conocimiento del Comité de Transparencia, por conducto de la Unidad de Transparencia, a efecto de que sea incorporado a los registros institucionales.

En los casos de los Documentos de Seguridad que fueron expedidos con antelación a la emisión de la presente Política, con la finalidad de que éstos se encuentren debidamente **actualizados**, en este caso, principalmente **respecto del inventario de datos personales**, será responsabilidad de las Áreas actualizarlo cuando se configuren las hipótesis normativas establecidas en el artículo 36 de la LGPDPPSO:

I. Cuando se produzcan modificaciones sustanciales al tratamiento de datos personales que deriven en un cambio en el nivel de riesgo.

II. Como resultado de un proceso de mejora continua, derivado del monitoreo y revisión del sistema de gestión.
III. Como resultado de un proceso de mejora para mitigar el impacto de una vulneración a la seguridad ocurrida.
IV. Implementación de acciones correctivas y preventivas ante una vulneración de seguridad.

6.5. Proceso general para el establecimiento, actualización, monitoreo y revisión de los mecanismos y medidas de seguridad; considerando el análisis de riesgo realizado previamente al tratamiento de los datos personales.

En este apartado se establecerán las medidas de seguridad, así como el monitoreo, revisión y actualización de éstas.

En materia de seguridad de la información, el establecimiento, monitoreo, revisión y actualización debe verse como un **proceso de mejora continua**[18], bajo este contexto a continuación se establecen las pautas generales respecto a dichas acciones:

6.5.1. Establecimiento de las medidas de seguridad

Cabe recordar que las medidas de seguridad son el resultado de la elaboración del Sistema de Gestión de Seguridad de Datos Personales y el Documento de Seguridad, particularmente lo que resulta del análisis de riesgos, análisis de brecha y el plan de trabajo.

Luego entonces, para establecer y mantener las medidas de seguridad para la protección de los datos personales, de conformidad con lo establecido en el artículo 33 de la LGPDPPSO cada Área deberá realizar al menos las siguientes **actividades interrelacionadas**:

- ✓ Crear políticas técnicas complementarias de protección de datos para la gestión y tratamiento de los datos personales, considerando el contexto en el que ocurren los tratamientos y el ciclo de vida de los datos personales, es decir, su obtención, uso y posterior supresión.

- ✓ Definir las funciones y obligaciones de las personas servidoras públicas, así como personas externas, involucradas en el tratamiento de datos personales.

- ✓ Elaborar un inventario de datos personales y de los sistemas de tratamiento.

- ✓ Realizar un análisis de riesgo de los datos personales, considerando las amenazas y vulnerabilidades existentes para los datos personales y los recursos involucrados en su tratamiento, como pueden ser, de manera enunciativa más no limitativa, hardware, software, personal del área, entre otros.

[18] *Recomendaciones para la elaboración de Políticas internas de gestión y tratamiento de datos personales (Sector Público).* Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), Mayo 2022, página 27. Disponible para consulta en: https://home.inai.org.mx//wp-content/documentos/DocumentosSectorPublico/RecomendacionesPol%C3%ADticasPDP.pdf

- ✓ Realizar un análisis de brecha, comparando las medidas de seguridad existentes contra las faltantes en la organización del responsable.

- ✓ Elaborar un plan de trabajo para la implementación de las medidas de seguridad faltantes, así como las medidas para el cumplimiento cotidiano de las políticas de gestión y tratamiento de los datos personales.

- ✓ 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.

- ✓ Diseñar y aplicar diferentes niveles de capacitación del personal bajo su mando, dependiendo de sus roles y responsabilidades respecto del tratamiento de los datos personales.

Adicionalmente, con fundamento en lo establecido en el artículo 34 de la Ley General, cada Área deberá **documentar las acciones relacionadas con las medidas de seguridad para el tratamiento de los datos personales, así como prever que las mismas estén contenidas en el SGSDP**, para lo cual, la persona titular del Área deberá solicitar al Comité de Transparencia, por conducto de la Unidad de Transparencia, que se incorporen en el SGSDP institucional las acciones realizadas vinculadas con las medidas de seguridad.

Por SGSDP se entenderá al conjunto de elementos y actividades interrelacionadas para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el tratamiento y seguridad de los datos personales, de conformidad con lo previsto en la LGPDPPSO y las demás disposiciones que le resulten aplicables en la materia.

Asimismo, es importante destacar que de manera particular, cada Área deberá elaborar un **Documento de Seguridad**, preferentemente por tratamiento, que contenga, al menos lo referido en el artículo 35 de la LGPDPPSO, esto es:

I. El inventario de datos personales y de los sistemas de tratamiento.
II. Las funciones y obligaciones de las personas que traten datos personales.
III. El análisis de riesgos, conforme a lo establecido en el artículo 60 de los Lineamientos Generales.
IV. El análisis de brecha, atendiendo a lo indicado en el artículo 61 de los Lineamientos Generales.
V. El plan de trabajo, de conformidad con lo señalado en el artículo 62 de los Lineamientos Generales.
VI. Los mecanismos de monitoreo y revisión de las medidas de seguridad.
VII. El programa general de capacitación.

6.5.2. MONITOREO DE LAS MEDIDAS DE SEGURIDAD.

El monitoreo conlleva la **vigilancia de las medidas de seguridad**. Para ello, es indispensable que las Áreas lleven un control y vigilen constantemente los activos, sus vulnerabilidades, las amenazas a las que están expuestos y los riesgos; asimismo, deberán identificar el impacto de las vulneraciones ocurridas, ya que en la medida en que se tenga conocimiento de dicha información se sabrá si los activos están correctamente protegidos, si las medidas de seguridad son pertinentes y, por ende, se podrá evaluar su cumplimiento dentro de la Universidad.

Bajo este contexto, deberán **monitorizarse las medidas de seguridad** con base en el análisis de riesgo previamente elaborado y documentado a través del Documento de Seguridad que corresponda.

Cada Área 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, con fundamento en el artículo 63 de los Lineamientos Generales.

Así, cada Área será responsable de **monitorear constantemente**:

a) Los nuevos activos que se incluyan en la gestión de riesgos;
b) Las modificaciones necesarias a los activos, como podría ser el cambio o migración tecnológica, entre otras;
c) Las nuevas amenazas que podrían estar activas dentro y fuera de su organización y que no han sido valoradas;
d) La posibilidad de que vulnerabilidades nuevas o incrementadas sean explotadas por las amenazas correspondientes;
e) Las vulnerabilidades identificadas para determinar aquéllas expuestas a amenazas nuevas o pasadas que vuelvan a surgir;
f) El cambio en el impacto o consecuencias de amenazas valoradas, vulnerabilidades y riesgos en conjunto, que resulten en un nivel inaceptable de riesgo, y
g) Los incidentes y vulneraciones de seguridad ocurridas.

En conclusión, las Áreas deberán llevar a cabo la **revisión constante** del inventario de activos, la elaboración del análisis de riesgos y análisis de brecha que conlleva a su vez la revisión de nuevas amenazas, las vulnerabilidades nuevas o incrementadas, el cambio en el impacto o consecuencia de las vulneraciones en los activos y en los titulares de los datos personales, y en general la advertencia de nuevos riesgos o su incremento que deban tratarse.

6.5.3. REVISIÓN DE LAS MEDIDAS DE SEGURIDAD.

La revisión implica **evaluar las medidas de seguridad**, esto es, evaluar si las políticas y controles de seguridad realmente se están aplicando dentro de cada Área, y si éstas son necesarias y suficientes para el objetivo de tratamiento del riesgo planteado.

De este modo, en apego a lo señalado por el artículo 63 de los Lineamientos Generales, toda Área que trate datos personales 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.

Para realizar la evaluación y medición de los resultados de las medidas de seguridad es necesario previamente haber monitoreado que dichas medidas realmente estén atendiendo los riesgos analizados, para así revisar objetivamente si las medidas de seguridad son eficaces, son suficientes e idóneas.

En razón de lo anterior, el proceso general para la revisión de medidas deberá contemplar las **auditorías internas y externas** a las que refiere el artículo 30 fracciones IV y V de la Ley General, que establece que se deben revisar periódicamente las políticas y programas de seguridad de datos personales para determinar las modificaciones que se requieran y que se debe establecer un sistema de supervisión y vigilancia interna y/o externa, que incluya auditorías para comprobar el cumplimiento de las políticas de protección de datos personales.

Asimismo, no debe pasar desapercibido el artículo 49 de los Lineamientos Generales, que abunda en las fracciones IV y V del artículo 30 de la LGPDPPSO, que reitera que deberán revisarse las políticas y programas de seguridad al menos cada dos años, salvo que se realicen modificaciones sustanciales a los tratamientos de datos personales, por lo que se requieran actualizarse previamente las medidas de seguridad.

En este mismo tenor, la Ley General por medio del principio de responsabilidad establece que se debe implementar un sistema de supervisión y vigilancia para la comprobación del cumplimiento de las políticas internas de seguridad, dicha obligación debe observarse en armonía con los demás preceptos normativos que refieren a los mecanismos de monitorización de las medidas de seguridad, incluyendo las políticas internas, en tanto que estas son medidas de seguridad administrativas.

En razón de lo anterior y en cumplimiento a lo establecido en el último párrafo del artículo 63 de los Lineamientos Generales, que señala que se debe contar con un programa de auditoría, interno y/o externo, para monitorear y revisar la eficacia y eficiencia del sistema de gestión; y, tomando en cuenta que la monitorización y revisión del SGSDP no solamente involucra la monitorización y revisión de las medidas de seguridad, sino toda la planeación e implementación del propio Sistema; **cada Área deberá establecer un programa interno de auditorías** respecto de cada Documento de Seguridad con el que cuente, lo cual impactará en el SGSDP, siendo posible que los resultados de dichas auditorías incidan en la actualización de medidas de seguridad, o bien en modificaciones al SGSDP.

6.5.4. ACTUALIZACIÓN DE LAS MEDIDAS DE SEGURIDAD.

La actualización es la consecuencia lógica y congruente de las actividades descritas en los numerales anteriores. Al respecto, la LGPDPPSO y los Lineamientos Generales establecen los supuestos específicos donde se deben actualizar las medidas de seguridad que se señalarán más adelante; sin embargo, no es necesario esperar a dichos momentos para hacerlo, ya que, de implementarse bien un SGSDP y que se monitoreen debidamente los activos, sus vulnerabilidades, amenazas y el riesgo en general, es probable que las políticas de seguridad se deban actualizar incluso antes de materializarse los supuestos a que refiere la normativa en la materia.

Respecto a los supuestos de actualización establecidos en la Ley General, en primera instancia, de conformidad con lo establecido el artículo 30 fracciones IV y V de ese ordenamiento legal, cada Área deberá revisar las políticas y programas de seguridad y el sistema de supervisión y vigilancia implementado, al menos cada dos años, salvo que realice modificaciones sustanciales a los tratamientos de datos personales que lleve a cabo y, en consecuencia, amerite una actualización previa a ese establecido.

Aunado a lo anterior, cabe recordar que el artículo 36 de la LGPDPPSO, refiere específicamente los **momentos en que se debe actualizar el Documento de Seguridad**:

I. Se produzcan modificaciones sustanciales al tratamiento de datos personales que deriven en un cambio en el nivel de riesgo;
II. Como resultado de un proceso de mejora continua, derivado del monitoreo y revisión del sistema de gestión;
III. Como resultado de un proceso de mejora para mitigar el impacto de una vulneración a la seguridad ocurrida, y
IV. Cuando se implementen acciones correctivas y preventivas ante una vulneración de seguridad.

Bajo este orden de ideas, se puede concluir que las actualizaciones son consecuencia de lo realizado en la monitorización y revisión tanto de los activos y la valoración del riesgo, así como de la revisión de las medidas de seguridad.

Así, la incidencia de la actualización del Documento de Seguridad en las medidas de seguridad es debido a que éste 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; y es por ello que, de actualizarse, se modificarían las medidas de seguridad dentro de las cuales se encuentra la presente Política que se constituye como una medida administrativa en sí misma.

Adicionalmente, podrán realizarse actualizaciones generadas por la propia actualización del SGSDP derivado de auditorías internas o externas en tanto que, con éste, se busca la mejora continua del propio sistema que tiene como fin la seguridad de los datos personales.

Por lo anterior, será indispensable que en todo momento las actualizaciones se reflejen tanto en el SGSDP como en el Documento de Seguridad que corresponda, para lo cual, cada Área deberá solicitarlo al Comité de Transparencia, a través de la Unidad de Transparencia.

6.6. Proceso general de atención de los derechos ARCO.

El ejercicio de los derechos ARCO deberá ser garantizado por todas las Áreas que integran a la UPN, atendiendo a lo dispuesto por los artículos 43 a 57 de la Ley General, así como en los artículos 73 a 107 de los Lineamientos Generales.

Para mayor referencia, a continuación se establecen las líneas generales del procedimiento para atender las solicitudes de derechos ARCO:

La persona titular podrá presentar su solicitud para el ejercicio de los derechos de acceso, rectificación, cancelación u oposición de sus datos personales (derechos ARCO) directamente ante la Unidad de Transparencia de la Universidad Pedagógica Nacional, cuyos datos de contacto son los siguientes:

- **Domicilio:** Carretera al Ajusco 24, Edificio de Gobierno, Primer Piso (Primer Nivel), Colonia Héroes de Padierna, Alcaldía Tlalpan, Ciudad de México, C.P. 14200.
- **Correo electrónico:** unidaddetransparencia@upn.mx
- **Teléfono:** 55 5630 9700, Ext. 1331

Asimismo, la persona Titular podrá presentar una solicitud de ejercicio de derechos ARCO a través de la Plataforma Nacional de Transparencia, disponible en http://www.plataformadetransparencia.org.mx y, a través de los siguientes medios:

Las solicitudes para el ejercicio de los derechos ARCO deberán presentarse ante la Unidad de Transparencia de esta Casa de Estudios, en el ámbito de su competencia, a través de escrito libre, formatos, medios electrónicos o cualquier otro medio que al efecto establezca el INAI.

Para ejercer los derechos ARCO, será necesario acreditar la identidad de la persona titular y, en su caso, la identidad y personalidad con la que actúe el representante. El ejercicio de los derechos ARCO por persona distinta a su titular o a su representante, será posible, excepcionalmente, en aquellos supuestos previstos por disposición legal, o en su caso, por mandato judicial. Para el caso de menores de edad o de personas que se encuentren en estado de interdicción o incapacidad, de conformidad con las leyes civiles, se estará a las reglas de representación dispuestas en la misma legislación. Tratándose de datos personales concernientes a personas fallecidas, la persona que acredite tener un interés jurídico, de conformidad con las leyes aplicables, podrá ejercer los derechos que le confiere la LGPDPPSO, siempre que el titular de los derechos hubiere expresado fehacientemente su voluntad en tal sentido o que exista un mandato judicial para dicho efecto. Lo anterior, de conformidad con lo establecido en el artículo 49 de la LGPDPPSO.

El **procedimiento para el ejercicio de los derechos ARCO** se resume a continuación:

En el ejercicio de los derechos ARCO, el plazo de respuesta no deberá exceder de veinte días contados a partir del día siguiente a la recepción de la solicitud. En caso de resultar procedente el ejercicio de los derechos ARCO, se deberá hacerlo efectivo en un plazo que no podrá exceder de quince días contados a partir del día siguiente en que se haya notificado la respuesta a la persona titular.

De conformidad con lo establecido en el artículo 52 de la LGPDPPSO, la solicitud para el ejercicio de los derechos ARCO deberá cumplir con los siguientes requisitos:

I. El nombre de la persona titular y su domicilio o cualquier otro medio para recibir notificaciones;
II. Los documentos que acrediten la identidad de la persona titular y, en su caso, la personalidad e identidad de su representante;
III. De ser posible, el área responsable que trata los datos personales y ante el cual se presenta la solicitud;
IV. La descripción clara y precisa de los datos personales respecto de los que se busca ejercer alguno de los derechos ARCO, salvo que se trate del derecho de acceso;
V. La descripción del derecho arco que se pretende ejercer, o bien, lo que solicita el titular, y
VI. Cualquier otro elemento o documento que facilite la localización de los datos personales, en su caso.

Tratándose de una **solicitud de acceso** a datos personales, la persona titular deberá señalar la modalidad en la que prefiere que éstos se reproduzcan. Las Áreas que resulten competentes deberán atender la solicitud en la modalidad requerida por la persona titular, salvo que exista una imposibilidad física o jurídica que lo limite a reproducir los datos personales en dicha modalidad, en este caso, deberá ofrecer otras modalidades de entrega de los datos personales fundando y motivando dicha actuación.

En caso de que la solicitud de datos no satisfaga alguno de los requisitos antes aludidos, y el Instituto o los organismos garantes no cuenten con elementos para subsanarla, se prevendrá a la persona titular de los datos dentro de los cinco días siguientes a la presentación de la solicitud de ejercicio de los derechos ARCO, por una sola ocasión, para que subsane las omisiones dentro de un plazo de diez días contados a partir del día siguiente al de la notificación. Transcurrido el plazo sin desahogar la prevención se tendrá por no presentada la solicitud de ejercicio de los derechos ARCO. La prevención tendrá el efecto de interrumpir el plazo que tiene el Instituto, o en su caso, los organismos garantes, para resolver la solicitud de ejercicio de los derechos ARCO.

Con relación a una **solicitud de cancelación**, el titular deberá señalar las causas que lo motiven a solicitar la supresión de sus datos personales en los archivos, registros o bases de datos de la Universidad Pedagógica Nacional.

En el caso de la **solicitud de oposición**, el titular deberá manifestar las causas legítimas o la situación específica que lo llevan a solicitar el cese en el tratamiento, así como el daño o perjuicio que le causaría la persistencia del tratamiento, o en su caso, las finalidades específicas respecto de las cuales requiere ejercer el derecho de oposición.

Esta Institución Educativa, por conducto de las Áreas que resulten competentes, deberán dar trámite a toda solicitud para el ejercicio de los derechos ARCO y entregar el acuse de recibo que corresponda.

Finalmente, para brindar más detalle del procedimiento interno para la atención a solicitudes de derechos ARCO, se podrá emitir una política complementaria o procedimiento interno donde se especifique a profundidad los plazos internos y actuaciones que dependen de este sujeto obligado.

6.7. Políticas Técnicas Complementarias de Protección de Datos Personales

Las políticas complementarias son aquellas que detallan procedimientos y medidas de seguridad para la protección de los datos personales de manera más específica y técnica. Éstas son importantes para operar un SGSDP y contribuyen a mejorar el deber de seguridad de los datos personales, ya que son consecuencia de los resultados obtenidos del análisis de riesgos y el análisis de brecha, particularmente éste último, de donde se deben elegir las medidas de seguridad a mejorar y a implementarse priorizando la atención de los riesgos más graves, y dentro de estas medidas de seguridad se encuentran las administrativas referentes a políticas de seguridad de los datos personales, las cuales son complementarias a la política rectora o general de gestión y tratamiento de datos personales.[19]

Así, derivado de que las políticas técnicas complementarias deben ser redactadas a detalle y, por ende, que en algunos casos serán más técnicas de acuerdo a la audiencia a la que se dirijan, para su elaboración deberá considerarse que también habrá personal que opere a nivel de usuario los sistemas de tratamiento y que no entienda tecnicismos, por lo que para estos últimos servirá una instrucción, manual o procedimiento de uso aceptable de los sistemas, en la que **se utilice un lenguaje más sencillo** donde se explique **qué está permitido, qué no lo está, cómo reportar una falla, etcétera**. Por ejemplo, si se trata de una política de

[19] *Recomendaciones para la elaboración de Políticas internas de gestión y tratamiento de datos personales (Sector Público)*. Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), Mayo 2022, página 34. Disponible para consulta en: https://home.inai.org.mx//wp-content/documentos/DocumentosSectorPublico/RecomendacionesPol%C3%ADticasPDP.pdf

control de acceso lógico, ésta será sumamente técnica en tanto que quienes operarán los controles de acceso lógicos podrían ser personas del Departamento de Informática.

Bajo este contexto, cada Área podrá implementar **políticas complementarias** conforme a sus necesidades, teniendo como objetivo principal regular de manera detallada procedimientos y medidas de seguridad para la protección de los datos personales que trate, de manera más específica y técnica.

De manera enunciativa, más no limitativa, a continuación se presentan algunos **ejemplos** de políticas complementarias son:

- Política control de accesos lógicos.
- Política de control de accesos físicos
- Política de seguridad física y ambiental
- Políticas, instrucciones, manuales o procedimientos orientados al usuario, tales como:
  - ✓ Manual de uso aceptable de activos
  - ✓ Política de escritorio y pantalla limpios
  - ✓ Política de gestión de contraseñas seguras
  - ✓ Política de comunicación de información que contiene datos personales
  - ✓ Política de restricciones a las instalaciones y uso del software
  - ✓ Política de copia de seguridad
  - ✓ Política de protección contra software malicioso
  - ✓ Protocolo o procedimiento para la atención de incidentes de seguridad
  - ✓ Política de controles criptográficos
  - ✓ Política de seguridad de las comunicaciones
  - ✓ Protocolo para cumplimiento del deber de confidencialidad con proveedores y personal externo.

En caso de que alguna Área pretenda implementar alguna política técnica complementaria, deberá hacerlo del conocimiento del Comité de Transparencia, por conducto de la Unidad de Transparencia para su respectiva aprobación.

6.8. Cumplimiento de la Política

Cada Área que trate datos personales deberá dar a conocer la presente Política a todo el personal que tenga adscrito, así como a personas externas a la UPN que intervengan por alguna razón justificada en el tratamiento, ya sea a la firma del contrato laboral o de servicios profesionales o contrato con proveedores correspondiente, o bien, durante el empleo, otorgando la política en físico o a través de medios electrónicos, y se deberá cerciorar que fue leída y comprendida, dejando constancia de ello a través de firma física o electrónica, o bien, mediante una casilla de confirmación de su lectura que otorgue constancia de la persona y el momento donde se ha leído y comprendido, a fin de que sirva como prueba de **cumplimiento del principio de responsabilidad y del deber de confidencialidad**.

6.9. Actualización de la Política

La aplicación de la Política es una actividad permanente y de mejora continua, por lo que deberán realizarse los reajustes que se consideren necesarios.

La presencia recurrente de la violación de la Política, el uso de nueva tecnología para el tratamiento de datos personales, vulneraciones o incidentes de seguridad son algunas de las razones por las cuales se deberá actualizar el presente documento, como se señala en el siguiente apartado.

6.10. Revisión, evaluación y mejora de la Política

Para efectos de revisión, evaluación y mejora, se deberá seguir el procedimiento general descrito en la presente Política en el numeral 6.5 "*Proceso general para el establecimiento, actualización, monitoreo y revisión de los mecanismos y medidas de seguridad*; *considerando además el análisis de riesgo realizado previamente al tratamiento de los datos personales*".

Asimismo, debe comprenderse que la Política como obligación legal y como medida de seguridad administrativa (además de ser parte del SGSDP), debe someterse a monitoreo, revisión y actualización constante para lograr una eficiente seguridad de los datos personales y de los sistemas de tratamiento con los que cuenta esta Casa de Estudios.

En ese sentido, es fundamental darle seguimiento a la Política, mantener su implementación a través del tiempo y actualizar o realizar ajustes a la misma cuando sea necesario, en particular conforme a lo establecido en los artículos 30 fracciones IV y V, 33 fracción VII, 34 y 35 fracción VI de la Ley General, los cuales debe ser interpretados de manera armónica y congruente, con lo establecido en los artículos 49 y 63 de los Lineamientos Generales.

"Educar para transformar"
Universidad Pedagógica Nacional