ACTA DE LA DÉCIMA PRIMERA SESIÓN ORDINARIA DEL AÑO 2024
DEL COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD PEDAGÓGICA NACIONAL

EN LA CIUDAD DE MÉXICO, SIENDO LAS **10:45 HORAS** DEL DÍA **VEINTINUEVE (29) DEL MES DE NOVIEMBRE DE DOS MIL VEINTICUATRO (2024)**, A TRAVÉS DE LA PLATAFORMA *TEAMS*, SE REUNIÓ DE FORMA VIRTUAL EL COMITÉ DE TRANSPARENCIA CON LA ASISTENCIA DE LAS SIGUIENTES PERSONAS: LA **LCDA. YISETH OSORIO OSORIO**, TITULAR DE LA UNIDAD DE TRANSPARENCIA; Y EL **LCDO. JUAN CARLOS NEGRETE ACOSTA**, RESPONSABLE DEL ÁREA COORDINADORA DE ARCHIVOS; CON EL OBJETO DE LLEVAR A CABO LA **DÉCIMA PRIMERA SESIÓN ORDINARIA DEL AÑO DOS MIL VEINTICUATRO (2024)**, DEL COMITÉ DE TRANSPARENCIA DE LA UPN.----------

LA TITULAR DE LA UNIDAD DE TRANSPARENCIA, **YISETH OSORIO OSORIO**, EN SU CARÁCTER DE PRESIDENTA DEL COMITÉ DE TRANSPARENCIA, DE CONFORMIDAD CON LO ESTABLECIDO EN LA FRACCIÓN I DEL ARTÍCULO 4 DE LOS *LINEAMIENTOS PARA EL FUNCIONAMIENTO INTERNO DEL COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD PEDAGÓGICA NACIONAL*, ENCABEZÓ LA SESIÓN DE LA QUE SE DA CUENTA. ----------

---------- **DESAHOGO DEL ORDEN DEL DÍA** ----------

COMO ACTO SEGUIDO, LA SESIÓN SE DESARROLLÓ BAJO LOS SIGUIENTES TÉRMINOS: ----------

PRIMER PUNTO.- LISTA DE ASISTENCIA Y DECLARACIÓN DEL QUÓRUM LEGAL. ----------

UNA VEZ QUE LOS PRESENTES CON USO DE LA VOZ AFIRMARON SU ASISTENCIA, SE DETERMINÓ LA EXISTENCIA DEL QUÓRUM PARA CELEBRAR LA **DÉCIMA PRIMERA SESIÓN ORDINARIA DEL AÑO DOS MIL VEINTICUATRO (2024)**, CONFORME A LO ESTABLECIDO EN EL ARTÍCULO 16 DE LOS *LINEAMIENTOS PARA EL FUNCIONAMIENTO INTERNO DEL COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD PEDAGÓGICA NACIONAL*, POR LO QUE SE PROSIGUIÓ CON EL SIGUIENTE PUNTO DEL ORDEN DEL DÍA. ----------

SEGUNDO PUNTO.- APROBACIÓN EL ORDEN DEL DÍA. ----------

EN APEGO A LO ESTABLECIDO EN EL ARTÍCULO 13 DE LOS *LINEAMIENTOS PARA EL FUNCIONAMIENTO INTERNO DEL COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD PEDAGÓGICA NACIONAL*, LA PRESIDENTA DEL COMITÉ DE TRANSPARENCIA DIO LECTURA AL SIGUIENTE **ORDEN DEL DÍA** QUE FUE SEÑALADO EN LA CONVOCATORIA A LA PRESENTE SESIÓN: ----------

1. LISTA DE ASISTENCIA Y DECLARACIÓN DEL QUÓRUM LEGAL. ----------
2. APROBACIÓN DEL ORDEN DEL DÍA.----------
3. PRESENTACIÓN Y, EN SU CASO, APROBACIÓN DEL ***DOCUMENTO DE SEGURIDAD DE LA UNIVERSIDAD PEDAGÓGICA NACIONAL***, EN EL MARCO DE LO ESTABLECIDO EN LOS ARTÍCULOS 35 Y 84, FRACCIÓN V, DE LA *LEY GENERAL DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE SUJETOS OBLIGADOS.* ----------
4. ASUNTOS GENERALES:----------

DATOS Y/O SISTEMAS EN LOS QUE SE TRATAN TALES DATOS, Y EL NIVEL INDIVIDUAL DE CUMPLIMIENTO DE LOS DEBERES, PRINCIPIOS Y OBLIGACIONES EN LA MATERIA DE PROTECCIÓN DE DATOS PERSONALES.

PARA TALES EFECTOS, EN EL MES DE JUNIO DEL EJERCICIO EN CURSO SE REQUIRIERON A TODAS LAS ÁREAS QUE INTEGRAN ESTA CASA DE ESTUDIOS PARA QUE LLEVARAN A CABO EL LLENADO DE LA ENCUESTA ANTES ALUDIDA. ----------

SUBSECUENTEMENTE, EL DÍA 27 DE JUNIO DE 2024, SE CELEBRÓ UNA REUNIÓN DE TRABAJO CON LAS PERSONAS SERVIDORAS PÚBLICAS DESIGNADAS COMO ENLACES DE TRANSPARENCIA, EN LA QUE SE BRINDÓ UNA ASESORÍA SOBRE EL LLENADO DE LA ENCUESTA, ----------

UNA VEZ HECHO LO ANTERIOR, A TRAVÉS DE LAS RESPUESTAS EMITIDAS POR LAS ÁREAS, SE IDENTIFICARON DIVERSOS TRATAMIENTOS DE DATOS PERSONALES.----------

- **SEGUNDA FASE.** A PARTIR DE LOS TRATAMIENTOS DE DATOS PERSONALES QUE FUERON REPORTADOS POR LAS ÁREAS EN LA ENCUESTA APLICADA EN LA PRIMERA FASE, DURANTE EL MES DE AGOSTO DE 2024, ÉSTAS FUERON REQUERIDAS CON LA FINALIDAD DE QUE INTEGRARAN SUS ***INVENTARIOS DE TRATAMIENTOS DE DATOS PERSONALES***, PARA LO CUAL, EN EL MES DE SEPTIEMBRE SE REALIZARON REUNIONES DE TRABAJO CON TODAS LAS ÁREA QUE TRATAN DATOS PERSONALES, CUYO PROPÓSITO FUE ASESORARLAS PARA QUE PUDIERAN INTEGRAR LOS INVENTARIOS EN COMENTO. ----------

  DE FORMA ULTERIOR, LA UNIDAD DE TRANSPARENCIA PROCEDIÓ A LA REVISIÓN DE LOS INVENTARIOS QUE FUERON PRESENTADOS POR LAS ÁREAS, IDENTIFICANDO LA NECESIDAD DE EMITIR OBSERVACIONES, LAS CUALES FUERON HECHAS DEL CONOCIMIENTO DE LAS PERSONAS TITULARES DE LAS ÁREAS Y ENLACES DE TRANSPARENCIA, A TRAVÉS DE REUNIONES DE TRABAJO CELEBRADAS EN SEPTIEMBRE Y OCTUBRE DE 2024.----------

  UNA VEZ HECHO LO ANTERIOR, LAS ÁREAS PRESENTARON SUS INVENTARIOS DE TRATAMIENTOS DE DATOS PERSONALES.----------

- **TERCERA FASE**. SE PROCEDIÓ A REALIZAR LOS ANÁLISIS DE RIESGOS Y DE BRECHA, LOS CUALES FUERON INTEGRADOS POR LAS ÁREAS EN REUNIONES CELEBRADAS ENTRE LOS MESES DE OCTUBRE Y NOVIEMBRE 2024.----------

- **CUARTA FASE.** CON BASE EN LOS CONTROLES ESTABLECIDOS EN LOS ANÁLISIS DE BRECHA, SE INTEGRÓ EL PLAN DE TRABAJO PARA LA GESTIÓN Y TRATAMIENTO DE RIESGOS. ----------

RESPECTO DE DICHAS ACTIVIDADES, LA SECRETARIA TÉCNICA SEÑALÓ QUE LA EVIDENCIA DOCUMENTAL QUE DA CUENTA DE DICHAS ACCIONES FUE INTEGRADA POR LA UNIDAD DE TRANSPARENCIA EN UN EXPEDIENTE. ----------

CONCLUIDA LA INTEGRACIÓN DEL DOCUMENTO DE SEGURIDAD SOMETIDO A CONSIDERACIÓN DE ESTE ÓRGANO COLEGIADO, Y DESPUÉS DE CONCLUIR CON EL ESTUDIO Y ANÁLISIS CORRESPONDIENTES, Y UNA VEZ EMITIDO EL

DATOS (INAI), LA SOLICITUD DEL **REFRENDO DEL *"RECONOCIMIENTO DE COMITÉ DE TRANSPARENCIA 100 % CAPACITADO"***, ASÍ COMO DEL **REFRENDO DEL *"RECONOCIMIENTO DE INSTITUCIÓN 100 % CAPACITADA"***, CORRESPONDIENTES AL EJERCICIO DOS MIL VEINTITRÉS (2023); MISMOS QUE, UNA VEZ QUE FUERON ACREDITADOS LOS REQUISITOS PARA LA OBTENCIÓN DE DICHOS REFRENDOS, A TRAVÉS DEL OFICIO NÚMERO **INAI/OC-BLIC/118/2024**, EL INAI NOTIFICÓ EL REFRENDO DE LOS MENCIONADOS RECONOCIMIENTOS. PARA MAYOR REFERENCIA, A CONTINUACIÓN SE INSERTA LA IMAGEN DEL OFICIO DE MÉRITO: ----------

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

2024, Año de Felipe Carrillo Puerto, Benemérito del Proletariado, Revolucionario y Defensor del Mayab

OFICINA DE LA COMISIONADA BLANCA LILIA IBARRA CADENA
OFICIO: INAI/OC-BLIC/118/2024
Ciudad de México, 15 de noviembre de 2024

Dra. Rosa María Torres Hernández
Rectora de la Universidad Pedagógica Nacional
P r e s e n t e

Con base en su solicitud y una vez validado el cumplimiento de lo estipulado en el Protocolo para la Expedición y Entrega del Oficio de Reconocimiento de Institución y Comité 100% Capacitado, por parte de la Dirección General de Capacitación del INAI, respecto al ejercicio 2023, nos es grato comunicarle que la Universidad Pedagógica Nacional se ha hecho acreedora a los reconocimientos:

Institución 100% capacitada
Comité de Transparencia 100% capacitado

Por ello, nos complace emitir el presente oficio por el cual el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, reconoce el trabajo personal e institucional que se ha desplegado para lograr el cien por ciento en materia de capacitación como sujeto obligado.

Lo anterior, constituye un testimonio del compromiso de la institución que usted representa, para impulsar el conocimiento adecuado de la normatividad vigente relacionada con los derechos humanos de acceso a la información, de protección de datos personales y temas conexos.

Aprovechamos la ocasión para enviarle un cordial saludo.

A t e n t a m e n t e,

Mtro. Adrián Alcalá Méndez
Comisionado Presidente

Mtra. Blanca Lilia Ibarra Cadena
Comisionada

Educación
Secretaría de Educación Pública

UNIVERSIDAD PEDAGÓGICA NACIONAL

DOCUMENTO DE SEGURIDAD DE LA UNIVERSIDAD PEDAGÓGICA NACIONAL

(UNIDADES UPN CIUDAD DE MÉXICO)

NOVIEMBRE 2024

CONTENIDO

PRESENTACIÓN

El 26 de enero de 2017 se expidió la *Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados* (en lo sucesivo LGPDPPSO), la cual tiene como objetivo establecer las bases, principios y procedimientos para garantizar el derecho que tiene toda persona a la protección de sus datos personales que estén en posesión de los sujetos obligados.

En su artículo primero, la LGPDPPSO señala que son sujetos obligados, en el ámbito federal, estatal y municipal, cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos.

En ese sentido, la Universidad Pedagógica Nacional (UPN), en su carácter de organismo desconcentrado de la Secretaría de Educación Pública, es sujeto obligado de la referida Ley y, por ello, debe observar lo dispuesto por dicho instrumento normativo en el tratamiento de datos personales que lleve a cabo.

De acuerdo con lo dispuesto por los artículos 29 y 30, fracciones I y VII de la LGPDPPSO, el responsable (sujeto obligado) deberá implementar mecanismos para acreditar el cumplimiento de los principios, deberes y obligaciones establecidos en dicha Ley.

Asimismo, la LGPDPPSO dispone que el tratamiento de datos personales que realicen los sujetos obligados estará regido por **ocho principios**: licitud, lealtad, información, consentimiento, finalidad, proporcionalidad, calidad y responsabilidad; y **dos deberes**: SEGURIDAD y confidencialidad.

Estos principios y deberes imponen una serie de obligaciones para los sujetos regulados por la LGPDPPSO, cuya finalidad es que el tratamiento se realice garantizando la protección de los datos personales, con el objeto de respetar el derecho a la autodeterminación informativa de las personas titulares.

Adicionalmente, la Ley General de la materia detalla el alcance y los procedimientos para el ejercicio de los cuatro derechos que el artículo 16 de la *Constitución Política de los Estados Unidos Mexicanos* reconoce a las personas titulares de los datos personales: acceso, rectificación, cancelación y oposición (derechos ARCO), y reconoce uno más, el de portabilidad.

Bajo este orden contexto, el 26 de enero de 2018 se publicó en el Diario Oficial de la Federación el Acuerdo mediante el cual se aprobaron los *Lineamientos Generales de Protección de Datos Personales para el Sector Público* (Lineamientos Generales) cuyo objetivo es desarrollar las disposiciones previstas en la LGPDPPSO y, con ello, hacer más comprensible el cumplimiento de los principios, deberes y obligaciones exigidos en materia de protección de datos personales.

En específico, respecto del **deber de seguridad**, el artículo 31 de la LGPDPPSO señala que el responsable del tratamiento deberá establecer y mantener medidas de seguridad de carácter administrativo, físico y técnico para la protección de los datos personales, que permitan protegerlos contra daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado, así como garantizar su confidencialidad, integridad y disponibilidad.

Por su parte, el artículo 35 de la LGPDPPSO establece como una obligación la elaboración de un **Documento de Seguridad**, que se define –de acuerdo con la fracción XIV del artículo 3 de la Ley General de la materia- como 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.

Así, de conformidad con el precepto legal antes invocado, el documento de seguridad deberá contener, al menos, la siguiente información:

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;
IV. El análisis de brecha;
V. El plan de trabajo;
VI. Los mecanismos de monitoreo y revisión de las medidas de seguridad, y
VII. El programa general de capacitación.

En este sentido, en cumplimiento de las obligaciones antes descritas, a continuación, se presenta el **Documento de Seguridad de la Universidad Pedagógica Nacional (UPN)**, en términos del artículo 35 de la Ley General, previamente citado.

GLOSARIO DE TÉRMINOS

Activo de Información (Activo): Es cualquier información o sistema relacionado con el tratamiento 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.[1]

Áreas: Instancias de la Universidad Pedagógica Nacional previstas en el Decreto de Creación, en el *Manual de Organización de la Universidad Pedagógica Nacional*, o bien, en los respectivos reglamentos interiores o instrumentos equivalentes, que traten datos personales, así como cualquier área u oficina que coadyuve a las unidades administrativas en el cumplimiento de sus funciones, aún y que no sean aludidas en el referido Manual de Organización.

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.[2]

Custodio. Aquella persona 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.[3]

---

[1] *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

[2] *Ibídem*, página 30.

[3] *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.[4]

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.[5]

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

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.[6]

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.[7]

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.

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

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.[8]

---

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

[5] Fracción X del artículo 3 de la LGPDPPSO.

[6] *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

[7] Fracción XIV del artículo 3 de la LGPDPPSO.

[8] *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

Integridad. 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.[9]

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

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.

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.

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

Riesgo. Combinación de la probabilidad de un evento y su consecuencia desfavorable.[10]

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

---

[9] *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

[10] *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 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.

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

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**).[11]

[11] *Ibídem*

COMPONENTES DEL DOCUMENTO DE SEGURIDAD

I. INVENTARIO DE DATOS PERSONALES Y DE LOS SISTEMAS DE TRATAMIENTO.

El artículo 33, fracción III de la LGPDPPSO, en relación con la fracción I del artículo 35 de esa misma Ley, establece como una de las actividades a realizar para implementar y mantener medidas de seguridad para la protección de datos personales, la elaboración de un **inventario de datos personales y de los sistemas de tratamiento**; el cual, debe formar parte del documento de seguridad.

Sobre el particular los artículos 58 y 59 de los Lineamientos Generales establecen lo siguiente:

> *"Artículo 58. Con relación a lo previsto en el artículo 33, fracción III de la Ley General, el responsable deberá elaborar un inventario con la información básica de cada tratamiento de datos personales, considerando, al menos, los siguientes elementos:*
>
> *I. El catálogo de medios físicos y electrónicos 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 servidores públicos 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 responsable, y*
> *VII. En su caso, los destinatarios o terceros receptores de las transferencias que se efectúen, así como las finalidades que justifican éstas.*
>
> *Artículo 59. Aunado a lo dispuesto en el artículo anterior de los presentes Lineamientos generales, en la elaboración del inventario de datos personales el responsable deberá considerar el ciclo de vida de los datos personales conforme lo siguiente:*
>
> *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 deberá identificar el riesgo inherente de los datos personales, contemplando su ciclo de vida y los activos involucrados en su tratamiento, como podrían ser hardware, software, personal, o cualquier otro recurso humano o material que resulte pertinente considerar.
[...]"

A partir de lo anterior, la Universidad Pedagógica Nacional integró los **Inventarios de Tratamientos de Datos Personales**, identificando los elementos informativos que señala el artículo 58 de los Lineamientos Generales y basados en el ciclo de vida de los datos personales como lo requiere el artículo 59 de los mismos Lineamientos Generales.

En este sentido, los INVENTARIOS antes referidos forman parte integral del presente documento de seguridad, los cuales fueron concentrados en el **ANEXO 1**.

Es oportuno señalar que diversas plazas presupuestales de la Universidad Pedagógica Nacional sufrieron de una renivelación, por lo que las diversas Subdirecciones que formaban parte de esta Casa de Estudios fueron re-niveladas a Jefaturas de Departamento, nivel O31; razón por la cual, actualmente se les nombra Áreas o Jefaturas de Departamento, lo que se considera importante mencionar ya que en algunos documentos se puede observar la denominación de una u otra forma en virtud de que se está en proceso de homologación de denominaciones de áreas en la normatividad y disposiciones internas de este sujeto obligado, como lo es el *Manual de Organización de la Universidad Pedagógica Nacional*, en donde se les observa como Subdirecciones.

Por otro lado, en el organigrama se advierte la existencia de dos Direcciones de Área (nivel M11) [Dirección de Docencia -con sus respectivas áreas adscritas- y la Dirección de Investigación], que corresponden a plazas que operativamente no son funcionales, es decir que no están en operación; empero, derivado de las necesidades de esta Institución Educativa, en el caso de la plaza presupuestal de la Dirección de Investigación actualmente está ocupada por la persona titular de la Unidad de Igualdad de Género e Inclusión, área que fue creada mediante Acuerdo RUPN-01-2022, emitido por la Rectora de esta Universidad y publicado en la Gaceta UPN número 154.

II. FUNCIONES Y OBLIGACIONES DE LAS PERSONAS QUE TRATAN LOS DATOS PERSONALES.

El artículo 33, fracción II de la LGPDPPSO, en relación con el artículo 35, fracción II, establece como una de las actividades a realizar para implementar y mantener medidas de seguridad para la protección de datos personales, la definición de las **funciones y obligaciones del personal** involucrado en el tratamiento de datos personales, elemento informativo que debe integrarse al documento de seguridad.

Sobre el particular, el artículo 57 de los Lineamientos Generales señala lo siguiente:

> *"Artículo 57. Con relación a lo dispuesto en el artículo 33, fracción II de la Ley General, el responsable deberá establecer y documentar los roles y responsabilidades, así como la cadena de rendición de cuentas de todas las personas que traten datos personales en su organización, conforme al sistema de gestión implementado.*
>
> *El responsable deberá establecer mecanismos para asegurar que todas las personas involucradas en el tratamiento de datos personales en su organización, conozcan sus funciones para el cumplimiento de los objetivos del sistema de gestión, así como las consecuencias de su incumplimiento."*

De conformidad con lo anterior, las funciones y obligaciones del personal de la Universidad Pedagógica Nacional se han identificado a nivel de personas servidoras públicas a través de los **Inventarios de Tratamientos de Datos Personales** que se desarrollaron por cada uno de los tratamientos de datos personales que lleva a cabo esta Casa de Estudios, mismos que están concentrados en el **ANEXO 1**, en los cuales se identificó el personal que realiza el tratamiento, el área al que está adscrito y la finalidad de dicho tratamiento.

Adicionalmente, conviene señalar que las funciones y obligaciones de las personas servidoras públicas que tratan datos personales se encuentran definidas en la legislación y normatividad que rige el actuar de la Universidad Pedagógica Nacional (UPN), como lo son, de manera enunciativa, más no limitativa, el *Decreto que crea la Universidad Pedagógica Nacional*, el *Manual de Organización de la Universidad Pedagógica Nacional*, así como los respectivos reglamentos interiores o instrumentos equivalentes.

III. Análisis de Riesgos, IV. Análisis de brecha y V. Plan de Trabajo.

El artículo 33, fracciones IV, V y VI de la LGPDPPSO, establece como una de las actividades a realizar para implementar y mantener medidas de seguridad para la protección de datos personales, la realización del análisis de riesgo, análisis de brecha y plan de trabajo, en los siguientes términos:

> *"Artículo 33. Para establecer y mantener las medidas de seguridad para la protección de los datos personales, el responsable deberá realizar, al menos, las siguientes actividades interrelacionadas:*
> *I. [...]*
> ***IV.*** *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 responsable, entre otros;*
> ***V.*** *Realizar un análisis de brecha, comparando las medidas de seguridad existentes contra las faltantes en la organización del responsable;*
> ***VI.*** *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;*

(...)"

Por su parte, los artículos 60, 61 y 62 de los Lineamientos Generales, establecen lo siguiente:

> *"Artículo 60. Para dar cumplimiento al artículo 33, fracción IV de la Ley General, el responsable deberá realizar un análisis de riesgos de los datos personales tratados 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 a 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 factores previstos en el artículo 32 de la Ley General."*
>
> *"Artículo 61. Con relación al artículo 33, fracción V de la Ley General, para la realización del análisis de brecha el responsable deberá considerar lo siguiente:*
>
> *I. Las medidas de seguridad existentes y efectivas;*
> *II. Las medidas de seguridad faltantes, y*
> *III. La existencia de nuevas medidas de seguridad que pudieran remplazar a uno o más controles implementados actualmente.*
> *(...)"*
>
> *"Artículo 62. De conformidad con lo dispuesto en el artículo 33, fracción VI de la Ley General, el responsable deberá elaborar un plan de trabajo que defina las acciones a implementar de acuerdo con el resultado del análisis de riesgos y del análisis de brecha, priorizando las medidas de seguridad más relevantes e inmediatas a establecer."*

En este tenor, la metodología y el procedimiento utilizados para evaluar y tratar los riesgos de los datos personales en la Universidad Pedagógica Nacional (UPN) consiste en la "*Metodología y Desarrollo del Análisis de Riesgos y Análisis de Brecha del Documento de Seguridad como base para el Sistema de Gestión de Protección Datos Personales (SGPDP) del INAI*", la cual a su vez tiene como referencias las siguientes normas y guías:

- Norma ISO/IEC 27001:2013, puntos 6.1.2, 6.1.3, 8.2, y 8.3
- Norma ISO/IEC 27000:2018
- Marco normativo aplicable a la seguridad y protección de datos personales
- Declaración de aplicabilidad
- Guía de Implementación de un Sistema de Gestión de Seguridad de Datos Personales (INAI)

A partir de lo anterior, se estableció lo siguiente:

- **Criterio de aceptación de riesgos.**

Para establecer los criterios de aceptación de riesgos se han considerado varios aspectos clave, incluyendo los elementos de la estrategia institucional, como la misión, visión y objetivos estratégicos; la normativa aplicable a la seguridad y tratamiento de datos personales; la operación de los procesos de tratamiento de datos; las tecnologías de la información, tanto en servicios como en infraestructura; y los recursos financieros y humanos disponibles para este fin.

Los criterios de aceptación se clasifican de la siguiente manera: un riesgo de nivel **bajo** es considerado **aceptable**, aunque debe ser monitoreado dentro de la gestión de riesgos; en cambio, si el nivel de riesgo es **medio** o **alto**, **no es aceptable** en ninguna circunstancia y debe ser gestionado adecuadamente.

❖ Criterio de impacto.

Los criterios de impacto se definen a partir de varios factores, entre los cuales se incluyen el valor de los activos de información y de apoyo afectados, la posible pérdida de los principios de seguridad de la información, como la confidencialidad, integridad y disponibilidad, así como el daño a la integridad de los titulares de datos personales.

También se consideran la degradación en la operación, ya sea interna o tercerizada, las vulneraciones de seguridad, la pérdida de valor financiero, el daño a la reputación institucional y el incumplimiento de requisitos legales y contractuales.

❖ Criterios para la evaluación de riesgos.

Los criterios para la evaluación de riesgos se basan en varios aspectos que incluyen el valor estratégico de los tratamientos de datos personales, la criticidad de los activos de información y de apoyo involucrados y el cumplimiento de los requisitos legales y obligaciones contractuales.

También se toma en cuenta la importancia operativa y de negocio de la disponibilidad, confidencialidad e integridad, así como las expectativas y percepciones de las partes interesadas, y las posibles consecuencias negativas para la reputación institucional.

❖ Identificación de riesgos.

a) Activos de información.

Un activo se define como cualquier elemento de valor involucrado en el tratamiento de datos personales, incluyendo bases de datos, conocimiento de procesos, personal, hardware, software, y documentos en papel.

Los activos críticos son aquellos considerados más valiosos por el responsable; su pérdida, destrucción, robo, extravío, uso no autorizado, o cualquier alteración podría causar una crisis y comprometer las operaciones o incluso la existencia del Instituto. Es necesario identificar todos los activos de información y de apoyo que puedan afectar

la confidencialidad, integridad y disponibilidad de los datos personales resguardados por la Universidad Pedagógica Nacional.

Estos activos pueden ser información en papel o en formato electrónico, aplicaciones, bases de datos, personal, hardware, software, infraestructura tecnológica, instalaciones, así como servicios o procesos externos.

Además, se debe determinar el valor del activo basándose en los tres principios fundamentales de seguridad de la información: confidencialidad, integridad y disponibilidad, utilizando una escala del 1 al 3, donde 1 representa el valor más bajo y 3 el más alto. El valor total del activo se calculará sumando los valores asignados a cada principio, empleando rangos para obtener un valor final tanto cualitativo como cuantitativo.

Rango	Valor Cualitativo	Valor Cuantitativo
1-3	Bajo	1
4-6	Medio	2
7-9	Alto	3

Para determinar adecuadamente la valoración de los activos y su asociación con cada principio de seguridad de la información, se establecen las siguientes preguntas:

Principio	Pregunta
Confidencialidad	¿Qué importancia tendría el activo si estuviera disponible o fuera conocido o revelado a personas, entidades o procesos no autorizados?
Integridad	¿Qué importancia tendría el activo si fuera alterado o modificado sin autorización o control?
Disponibilidad	¿Qué importancia tendría el activo si no estuviera accesible o utilizable a petición de una entidad autorizada?

Por cada activo se deberá identificar un propietario: persona o entidad (área que trata los datos personales) con la responsabilidad y la autoridad para gestionar un activo. El propietario del activo deberá determinar el valor de este. En su caso, también se deberá identificar el custodio de este.

b) Amenaza y vulnerabilidades.

Se deberá llevar a cabo la identificación de todas las amenazas y vulnerabilidades asociadas a cada activo. Este proceso de identificación será realizado por los propietarios de los activos.

c) Estimación del riesgo.

Se utilizará una escala cuantitativa y su equivalencia cualitativa con atributos calificativos para describir la magnitud de los impactos o consecuencias potenciales y la posibilidad de que ocurran. La estimación del impacto y probabilidad será realizada por los propietarios de los riesgos.

Los elementos para estimar el riesgo son:

- **Impacto.** Se refiere al grado del daño o costo que pudiera ser causado a partir de que un evento no deseado ocurriera. La estimación del grado de impacto o consecuencias debe ser determinado mediante la aplicación de criterios en función de los tres principios de seguridad de la información:

  - ✓ **Confidencialidad**: Propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.
  - ✓ **Integridad**: Propiedad de la información de completitud y exactitud.
  - ✓ **Disponibilidad**: propiedad de la información de ser y estar accesible y utilizable a petición de una entidad autorizada.

En este sentido:

Grado de Impacto		Criterio
Bajo	1	El daño o pérdida de confidencialidad, integridad y disponibilidad de activos de información, no afecta la operación (interna o tercerizada) de los procesos y servicios institucionales, sin embargo, podría provocar pérdidas financieras menores y tolerables.
Medio	2	El daño o pérdida de confidencialidad, integridad y disponibilidad de activos de información podría interrumpir parcialmente la operación (interna o tercerizada) de los procesos y servicios institucionales, provocar pérdidas financieras y/o patrimoniales exponenciales, consecuencias moderadas en la imagen y reputación institucional o en el cumplimento de los requisitos legales o contractuales.
Alto	3	El daño o pérdida de confidencialidad, integridad y disponibilidad de activos de información podría interrumpir totalmente la operación (interna o tercerizada) de los procesos y servicios institucionales, provocar pérdidas financieras y/o patrimoniales mayores, daños en la imagen y reputación institucional, incumplimiento de requisitos legales o contractuales.

- **Probabilidad.** Se refiere al grado del daño o costo que pudiera ser causado a partir de que un evento no deseado ocurriera:

Grado de Probabilidad		Criterio
Bajo	1	Si no ha habido ningún tipo de antecedente registrado y/o que por el entorno la posibilidad de que suceda sea mínima.
Medio	2	Si solo se ha tenido un antecedente registrado en un periodo anual y/o esporádicamente en intervalos de 3 a 5 años o que por el tipo de entorno y condiciones sea posible que ocurra.
Alto	3	Si ha habido más de dos eventos al término de un año o bien que por las condiciones actuales o el tipo de entorno sea sumamente posible que suceda.

❖ Determinación del nivel de riesgo.

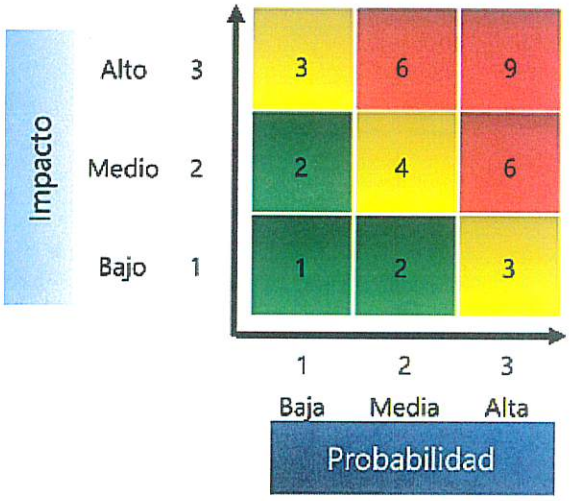
El nivel de riesgo debe ser representado en una escala cualitativa de 3 niveles, en orden creciente (bajo, medio y alto) y su equivalencia cuantitativa (1, 2 y 3) respectivamente.

La fórmula que se utilizará para determinar el nivel de riesgo será la siguiente:

Los valores del impacto y la probabilidad deberán ingresarse en el Cuadro de Evaluación de Riesgos para obtener el nivel de riesgo. El nivel de riesgo se calculará multiplicando los dos valores.

❖ Evaluación del riesgo.

La siguiente imagen muestra un mapa de calor con los resultados de las valoraciones señaladas con anterioridad.



La siguiente tabla muestra el nivel de riesgo en escala cuantitativa y cualitativa.

Impacto		Probabilidad		Nivel de riesgo	
Cuantitativo	Cualitativo	Cuantitativo	Cualitativo	Cuantitativo	Cualitativo
3	Alto	1	Baja	3	Medio
3	Alto	2	Media	6	Alto
3	Alto	3	Alta	9	Alto
2	Medio	1	Baja	2	Bajo
2	Medio	2	Media	4	Medio
2	Medio	3	Alta	6	Alto
1	Bajo	1	Baja	1	Bajo
1	Bajo	2	Media	2	Bajo
1	Bajo	3	Alta	3	Medio

Una vez realizadas las valoraciones, se procederá a evaluar el riesgo comparando el nivel de riesgo con los criterios de aceptación del riesgo establecidos previamente, en donde:

1. Los valores 1 y 2 (bajo) serán riesgos aceptables.
2. Los valores 3 y 4 (medio) serán riesgos no aceptables, por lo que deberán ser tratados.
3. Los valores 6 y 9 (alto) serán riesgos no aceptables por lo que deberán ser tratados.
4. Para los riesgos no aceptables, se deberá priorizar el tratamiento del riesgo para aquellos activos de mayor a menor valor; 3 (alto), 2 (medio) y 1 (bajo).

Con el fin de evitar retrabajo o costos innecesarios, en su caso, se deben identificar controles existentes que permitan reducir el nivel de riesgo; éstos tendrán que ser ingresados en el Cuadro de Evaluación de Riesgos, determinando su nivel de madurez:

- Si el nivel de madurez de los controles existentes es 1, el riesgo no tendrá que ser tratado.
- Si el nivel de madurez de los controles existentes es 2 el riesgo deberá ser tratado.

❖ Identificación de los propietarios de los riesgos.

Para cada riesgo se deberá identificar un propietario: persona o unidad administrativa con la responsabilidad y la autoridad para gestionar un riesgo, destacando que podrá o no ser el mismo que el propietario del activo.

❖ Tratamiento del riesgo.

El tratamiento de riesgos se implementará a través del Cuadro de tratamiento de riesgos, donde se copiarán todos los riesgos identificados como no aceptables desde el Cuadro de evaluación de riesgos. Esta tarea será realizada por el propietario del riesgo, y en los casos que lo requieran, de manera conjunta y coordinada con el custodio del activo.

Para los riesgos valorados en 3 y 4, así como 6 y 9, se deberá seleccionar una opción de tratamiento que puede ser: reducir el riesgo, lo que implica tomar acciones para disminuir la probabilidad o las consecuencias negativas asociadas; aceptar el riesgo, que se refiere a la aceptación de la posible pérdida o ganancia, permitida solo si otras opciones de tratamiento resultan más costosas que el impacto potencial; evitar el riesgo, que consiste en decidir no participar en una situación riesgosa; o transferir el riesgo, que implica compartir con un tercero la carga de la pérdida o ganancia, como a través de un seguro o un contrato.

En el caso de optar por la reducción del riesgo, será necesario evaluar el nuevo valor de impacto y probabilidad en el Cuadro de tratamiento de riesgos para medir la efectividad de los controles planificados.

- **Análisis de brecha.**

La Unidad de Transparencia con las áreas correspondientes deberán integrar el Plan de tratamiento de riesgos en el que se planificará la implementación de los controles.

- **Revisiones periódicas de la evaluación y el tratamiento de riesgos.**

Los propietarios de riesgos deberán revisar los riesgos vigentes y actualizar los Cuadros de evaluación de riesgos y tratamiento de riesgos, según los nuevos riesgos identificados. Esta revisión se llevará a cabo al menos una vez al año, y con mayor frecuencia si se producen cambios organizacionales significativos, importantes modificaciones en la tecnología, alteraciones en los objetivos estratégicos, o cambios en el entorno del marco normativo aplicable relacionado con la seguridad de la información y los datos personales.

- **Informes.**

La Unidad de Transparencia documentará los resultados de la evaluación y del tratamiento de riesgos y de todas las revisiones subsecuentes. La Unidad de Transparencia supervisará el progreso de la implementación del **Plan de Tratamiento de Riesgos** e informará periódicamente los resultados al Comité de Transparencia.

Conforme lo anterior, los análisis de riesgos y de brecha se llevaron a cabo a partir de las siguientes fuentes de información.

1. **Análisis de riesgos de la infraestructura tecnológica y recursos de software y hardware.** Este análisis abarca la evaluación de los sistemas, dispositivos y plataformas tecnológicas que la Universidad utiliza para llevar a cabo sus operaciones.

2. **Análisis de riesgos de hábitos de seguridad del personal de la Universidad Pedagógica Nacional.** Este análisis se enfoca en evaluar las prácticas y comportamientos de seguridad de las personas servidoras públicas, sin asociarlas directamente a un tratamiento específico.

3. **Análisis de riesgos a partir de los inventarios de tratamientos de datos personales**. Este análisis se realiza de manera específica para cada uno de los tratamientos reportados en los inventarios de datos personales de la Universidad, teniendo en cuenta sus particularidades, contextos y riesgos inherentes a cada proceso.

En el caso de los dos primeros análisis se realizan de manera general y aplican transversalmente, ya que el primero refiere a los distintos sistemas o medios en los que se llevan a cabo los diversos tratamientos que realiza la Universidad, por lo que los riesgos y controles que se determinen aplican de manera directa a estos medios o sistemas; mientras que el segundo, versa sobre los hábitos de seguridad del personal, de manera general y no asociados a un tratamiento en lo particular.

Por su parte, el análisis 3 se realiza de manera específica, asociado a cada uno de los tratamientos reportados en los inventarios de datos personales y tomando en cuenta sus particularidades.

En ese sentido, los **Análisis** antes enlistados se encuentran contenidos en el **ANEXO 2** del presente documento de seguridad.

Por su parte, el **Plan de Trabajo** al que se hace referencia en el artículo 33, fracción VI de la LGPDPPSO, se encuentra en el **ANEXO 3** como parte integral del documento de seguridad.

VI. Mecanismos de Monitoreo y Revisión de las Medidas de Seguridad.

El artículo 35, fracción VI, de la Ley General establece que el documento de seguridad deberá contener, entre otros aspectos, los mecanismos de monitoreo y revisión de las medidas de seguridad.

Para poder definir el mecanismo interno de monitoreo y revisión de medidas de seguridad, se debe tomar en consideración los dispuesto en el artículo 33, fracción VII de la LGPDPPSO y el artículo 63 de los Lineamientos Generales, que a la letra dicen:

> *"Artículo 33. Para establecer y mantener las medidas de seguridad para la protección de los datos personales, el responsable deberá realizar, al menos, las siguientes actividades interrelacionadas:*
> *(...)*
> *VII. 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, y*
> *(...)"*

> *"Artículo 63. Con relación al artículo 33, fracción VII de la Ley General, el responsable 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 cumplir con lo dispuesto en el párrafo anterior del presente artículo, el responsable deberá monitorear continuamente lo siguiente:

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

El artículo 63 de los Lineamientos Generales establece que el responsable 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 cumplir con lo anterior, el responsable deberá monitorear continuamente lo siguiente:

1. Los nuevos activos que se incluyan en la gestión de riesgos.

2. Las modificaciones necesarias a los activos, como podría ser el cambio o migración tecnológica, entre otras.

3. Las nuevas amenazas que podrían estar activas dentro y fuera del sujeto obligado y que no han sido valoradas.

4. La posibilidad de que vulnerabilidades nuevas o incrementadas sean explotadas por las amenazas correspondientes.

5. Las vulnerabilidades identificadas para determinar aquéllas expuestas a amenazas nuevas o pasadas que vuelvan a surgir.

6. El cambio en el impacto o consecuencias de amenazas valoradas, vulnerabilidades y riesgos en conjunto, que resulten en un nivel inaceptable de riesgo.

7. Los incidentes y vulneraciones de seguridad ocurridos.

Asimismo, el responsable deberá contar con un programa de auditoría, interno y/o externo, para monitorear y revisar la eficacia y eficiencia del sistema de gestión.

En ese sentido, la Universidad Pedagógica Nacional desarrollará el cumplimiento de dicha obligación a través de los siguientes mecanismos que forman parte integral del presente documento de seguridad:

A. Mecanismo de monitoreo y supervisión.

La Unidad de Transparencia será la encargada de ejecutar el mecanismo de monitoreo y supervisión de las medidas de seguridad implementadas en la protección de datos personales, a través de los siguientes ejes:

I. **Etapa de Monitoreo**. La Unidad de Transparencia requerirá a cada una de las áreas que reportaron tratamientos de datos personales, a través de sus inventarios, la elaboración de un reporte.

II. **Etapa de Supervisión.** La Unidad de Transparencia analizará los reportes de las áreas y emitirá recomendaciones o requerimientos que se consideren pertinentes en materia de seguridad, con la finalidad de que las áreas las atiendan y remitan las evidencias de su cumplimiento.

B. Mecanismos de actuación ante vulneraciones a la seguridad de los datos personales.

El artículo 33, fracción VII, de la Ley General, dispone que, para establecer y mantener las medidas de seguridad para la protección de los datos personales, el responsable deberá monitorear y revisar de manera periódica las medidas de seguridad implementadas, así como las amenazas y vulneraciones a las que están sujetos los datos personales.

En ese sentido, el artículo 63, fracción VII, de los Lineamientos Generales de Protección de Datos Personales para el Sector Público, entre otras disposiciones estipula que, para evaluar y medir los resultados de las políticas, planes, procesos y procedimientos implementados en materia de seguridad y tratamiento de los datos personales, se deberán monitorear las vulneraciones de seguridad ocurridas.

Por ello, la Unidad de Transparencia deberá monitorear y revisar de manera periódica las medidas de seguridad, así como las amenazas y vulneraciones a las que están sujetos los datos personales.

C. Mecanismos de auditoría en materia de datos personales.

Entre los mecanismos que se deben adoptar para cumplir con el principio de responsabilidad el artículo 30, fracción V, de la Ley General de Datos Personales en Posesión de Sujetos Obligados, establece que se deberá mantener un

sistema de supervisión y vigilancia, incluyendo auditorías, que permita comprobar el cumplimiento de las políticas de datos personales.

El artículo 63 de los Lineamientos Generales, dispone que además del monitoreo y supervisión periódica de las medidas de seguridad, se deberá contar con un programa de auditoría para revisar la eficacia y eficiencia del sistema de gestión.

Por tanto, resulta necesario establecer un mecanismo que permita dar cumplimiento a las disposiciones antes citadas. Las auditorías en materia de datos personales tendrán la finalidad de verificar la adaptación, adecuación y eficacia de los controles, medidas y mecanismos implementados para el cumplimiento de las disposiciones previstas en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y los Lineamientos Generales de Protección de Datos Personales para el Sector Público.

Lo anterior, permitirá identificar de forma ordenada las acciones y mejoras que habrán de implementarse para el adecuado manejo y protección de los datos personales.

VII. Programa General de Capacitación.

En cumplimiento a los artículos 30, fracción III; 33, fracción VIII y 35, fracción VIII de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y, 64 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público, debe elaborarse un programa de capacitación y actualización permanente de las personas servidoras públicas de la Universidad, sobre las obligaciones y cumplimiento de los principios y deberes en materia de protección de datos personales.

La fracción VIII del artículo 33 de la Ley General señala que, para establecer y mantener las medidas de seguridad para la protección de los datos personales, el responsable deberá 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.

De acuerdo con la fracción VII del artículo 35 de la Ley General, el programa de capacitación forma parte del documento de seguridad. Por su parte, el artículo 64 de los Lineamientos Generales señala lo siguiente:

> *Artículo 64. Para el cumplimiento de lo previsto en el artículo 33, fracción VIII de la Ley General, el responsable 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, 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, el responsable 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.

A partir de lo anterior, la Universidad Pedagógica Nacional desarrolló su **Programa General de Capacitación** con base en la detección de necesidades, mismo que integra el **ANEXO 4** de este documento de seguridad.

ACTUALIZACIÓN DEL DOCUMENTO DE SEGURIDAD.

El artículo 36 de la Ley General establece la obligación de la actualización del documento de seguridad cuando ocurran los siguientes eventos:

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. Implementación de acciones correctivas y preventivas ante una vulneración de seguridad.

En este sentido, las Áreas deberán informar al Comité de Transparencia, por conducto de la Unidad de Transparencia, cuando ocurra alguno de los supuestos antes citados para que, en su caso, se proceda a la actualización el presente documento de seguridad.

Educación
Secretaría de Educación Pública

UNIVERSIDAD PEDAGÓGICA NACIONAL

PLAN DE TRABAJO PARA LA GESTIÓN Y TRATAMIENTO DE RIESGOS

UNIVERSIDAD PEDAGÓGICA NACIONAL (UNIDADES UPN CIUDAD DE MÉXICO)

NOVIEMBRE 2024

PRESENTACIÓN

La *Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados* (en lo sucesivo LGPDPPSO) dispone que el tratamiento de datos personales que realicen los sujetos obligados estará regido por **ocho principios**: licitud, lealtad, información, consentimiento, finalidad, proporcionalidad, calidad y responsabilidad; y **dos deberes**: SEGURIDAD y confidencialidad.

Estos principios y deberes imponen una serie de obligaciones para los sujetos regulados por la LGPDPPSO, cuya finalidad es que el tratamiento se realice garantizando la protección de los datos personales, con el objeto de respetar el derecho a la autodeterminación informativa de las personas titulares.

Adicionalmente, los *Lineamientos Generales de Protección de Datos Personales para el Sector Público* (Lineamientos Generales) tienen por objetivo desarrollar las disposiciones previstas en la LGPDPPSO y, con ello, hacer más comprensible el cumplimiento de los principios, deberes y obligaciones exigidos en materia de protección de datos personales.

En específico, respecto del **deber de seguridad**, el artículo 31 de la LGPDPPSO señala que el responsable del tratamiento deberá establecer y mantener medidas de seguridad de carácter administrativo, físico y técnico para la protección de los datos personales, que permitan protegerlos contra daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado, así como garantizar su confidencialidad, integridad y disponibilidad.

Por su parte, el artículo 35 de la LGPDPPSO establece como una obligación la elaboración de un **Documento de Seguridad**, que se define –de acuerdo con la fracción XIV del artículo 3 de la Ley General de la materia- como 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.

Así, de conformidad con la fracción V del precepto legal antes invocado, el documento de seguridad deberá contener un **plan de trabajo** en el que se deben puntualizar las actividades a realizar, el responsable que las va a implementar y el tiempo y recursos destinados a su realización.

En este sentido, en cumplimiento a la fracción V del artículo 35 de la LGPDPPSO se integra el presente ***PLAN DE TRABAJO PARA LA GESTIÓN Y TRATAMIENTO DE RIESGOS*** **(Plan de Trabajo)**.

METODOLOGÍA PARA EL ANÁLISIS DE RIESGOS Y ANÁLISIS DE BRECHA.

Para estar en aptitud de integrar el **Plan de Trabajo**, es importante señalar que previamente se realizó el Análisis de Riesgos y Brecha por cada uno de los tratamientos de datos personales que se realizan en esta Casa de Estudios, mismos que se realizaron conforme a la metodología y el procedimiento utilizados para evaluar y tratar los riesgos de los datos personales en la Universidad Pedagógica Nacional (UPN) consiste en la "*Metodología y Desarrollo del Análisis de Riesgos y Análisis de Brecha del Documento de Seguridad como base para el Sistema de Gestión de Protección Datos Personales (SGPDP) del INAI*", la cual a su vez tiene como referencias las siguientes normas y guías:

- Norma ISO/IEC 27001:2013, puntos 6.1.2, 6.1.3, 8.2, y 8.3
- Norma ISO/IEC 27000:2018
- Marco normativo aplicable a la seguridad y protección de datos personales
- Declaración de aplicabilidad
- Guía de Implementación de un Sistema de Gestión de Seguridad de Datos Personales del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI).

A partir de lo anterior, se estableció lo siguiente:

❖ Criterio de aceptación de riesgos.

Para establecer los criterios de aceptación de riesgos se han considerado varios aspectos clave, incluyendo los elementos de la estrategia institucional, como la misión, visión y objetivos estratégicos; la normativa aplicable a la seguridad y tratamiento de datos personales; la operación de los procesos de tratamiento de datos; las tecnologías de la información, tanto en servicios como en infraestructura; y los recursos financieros y humanos disponibles para este fin.

Los criterios de aceptación se clasifican de la siguiente manera: un riesgo de nivel **bajo** es considerado **aceptable**, aunque debe ser monitoreado dentro de la gestión de riesgos; en cambio, si el nivel de riesgo es **medio** o **alto**, **no es aceptable** en ninguna circunstancia y debe ser gestionado adecuadamente.

❖ Criterio de impacto.

Los criterios de impacto se definen a partir de varios factores, entre los cuales se incluyen el valor de los activos de información y de apoyo afectados, la posible pérdida de los principios de seguridad de la información, como la confidencialidad, integridad y disponibilidad, así como el daño a la integridad de los titulares de datos personales.

También se consideran la degradación en la operación, ya sea interna o tercerizada, las vulneraciones de seguridad, la pérdida de valor financiero, el daño a la reputación institucional y el incumplimiento de requisitos legales y contractuales.

❖ Criterios para la evaluación de riesgos.

Los criterios para la evaluación de riesgos se basan en varios aspectos que incluyen el valor estratégico de los tratamientos de datos personales, la criticidad de los activos de información y de apoyo involucrados y el cumplimiento de los requisitos legales y obligaciones contractuales.

También se toma en cuenta la importancia operativa y de negocio de la disponibilidad, confidencialidad e integridad, así como las expectativas y percepciones de las partes interesadas, y las posibles consecuencias negativas para la reputación institucional.

❖ Identificación de riesgos.

a) Activos de información.

Un activo se define como cualquier elemento de valor involucrado en el tratamiento de datos personales, incluyendo bases de datos, conocimiento de procesos, personal, hardware, software, y documentos en papel.

Los activos críticos son aquellos considerados más valiosos por el responsable; su pérdida, destrucción, robo, extravío, uso no autorizado, o cualquier alteración podría causar una crisis y comprometer las operaciones o incluso la existencia del Instituto. Es necesario identificar todos los activos de información y de apoyo que puedan afectar la confidencialidad, integridad y disponibilidad de los datos personales resguardados por la Universidad Pedagógica Nacional.

Estos activos pueden ser información en papel o en formato electrónico, aplicaciones, bases de datos, personal, hardware, software, infraestructura tecnológica, instalaciones, así como servicios o procesos externos.

Además, se debe determinar el valor del activo basándose en los tres principios fundamentales de seguridad de la información: confidencialidad, integridad y disponibilidad, utilizando una escala del 1 al 3, donde 1 representa el valor más bajo y 3 el más alto. El valor total del activo se calculará sumando los valores asignados a cada principio, empleando rangos para obtener un valor final tanto cualitativo como cuantitativo.

Rango	Valor Cualitativo	Valor Cuantitativo
1-3	Bajo	1
4-6	Medio	2
7-9	Alto	3

Para determinar adecuadamente la valoración de los activos y su asociación con cada principio de seguridad de la información, se establecen las siguientes preguntas:

Principio	Pregunta
Confidencialidad	¿Qué importancia tendría el activo si estuviera disponible o fuera conocido o revelado a personas, entidades o procesos no autorizados?
Integridad	¿Qué importancia tendría el activo si fuera alterado o modificado sin autorización o control?

Disponibilidad	¿Qué importancia tendría el activo si no estuviera accesible o utilizable a petición de una entidad autorizada?

Por cada activo se deberá identificar un propietario: persona o entidad (área que trata los datos personales) con la responsabilidad y la autoridad para gestionar un activo. El propietario del activo deberá determinar el valor de este. En su caso, también se deberá identificar el custodio de este.

b) Amenaza y vulnerabilidades.

Se deberá llevar a cabo la identificación de todas las amenazas y vulnerabilidades asociadas a cada activo. Este proceso de identificación será realizado por los propietarios de los activos.

c) Estimación del riesgo.

Se utilizará una escala cuantitativa y su equivalencia cualitativa con atributos calificativos para describir la magnitud de los impactos o consecuencias potenciales y la posibilidad de que ocurran. La estimación del impacto y probabilidad será realizada por los propietarios de los riesgos.

Los elementos para estimar el riesgo son:

- **Impacto.** Se refiere al grado del daño o costo que pudiera ser causado a partir de que un evento no deseado ocurriera. La estimación del grado de impacto o consecuencias debe ser determinado mediante la aplicación de criterios en función de los tres principios de seguridad de la información:

  - ✓ **Confidencialidad**: Propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.
  - ✓ **Integridad**: Propiedad de la información de completitud y exactitud.
  - ✓ **Disponibilidad**: propiedad de la información de ser y estar accesible y utilizable a petición de una entidad autorizada.

  En este sentido:

Grado de Impacto		Criterio
Bajo	1	El daño o pérdida de confidencialidad, integridad y disponibilidad de activos de información, no afecta la operación (interna o tercerizada) de los procesos y servicios institucionales, sin embargo, podría provocar pérdidas financieras menores y tolerables.
Medio	2	El daño o pérdida de confidencialidad, integridad y disponibilidad de activos de información podría interrumpir parcialmente la operación (interna o tercerizada) de los procesos y servicios institucionales, provocar pérdidas financieras y/o patrimoniales exponenciales, consecuencias moderadas en la

Grado de Impacto		Criterio
		imagen y reputación institucional o en el cumplimento de los requisitos legales o contractuales.
Alto	3	El daño o pérdida de confidencialidad, integridad y disponibilidad de activos de información podría interrumpir totalmente la operación (interna o tercerizada) de los procesos y servicios institucionales, provocar pérdidas financieras y/o patrimoniales mayores, daños en la imagen y reputación institucional, incumplimiento de requisitos legales o contractuales.

- **Probabilidad.** Se refiere al grado del daño o costo que pudiera ser causado a partir de que un evento no deseado ocurriera:

Grado de Probabilidad		Criterio
Bajo	1	Si no ha habido ningún tipo de antecedente registrado y/o que por el entorno la posibilidad de que suceda sea mínima.
Medio	2	Si solo se ha tenido un antecedente registrado en un periodo anual y/o esporádicamente en intervalos de 3 a 5 años o que por el tipo de entorno y condiciones sea posible que ocurra.
Alto	3	Si ha habido más de dos eventos al término de un año o bien que por las condiciones actuales o el tipo de entorno sea sumamente posible que suceda.

❖ Determinación del nivel de riesgo.

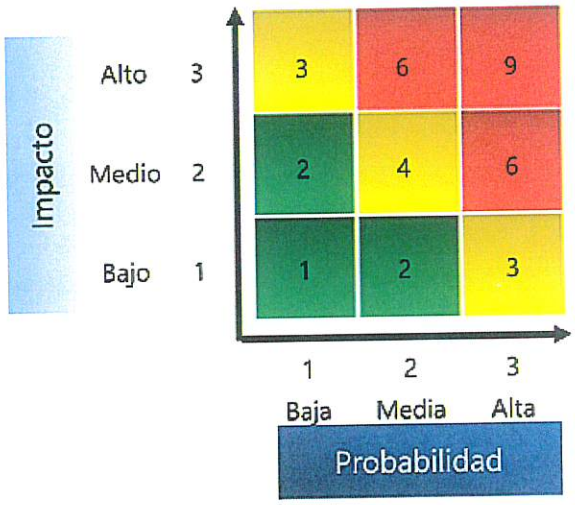
El nivel de riesgo debe ser representado en una escala cualitativa de 3 niveles, en orden creciente (bajo, medio y alto) y su equivalencia cuantitativa (1, 2 y 3) respectivamente.

La fórmula que se utilizará para determinar el nivel de riesgo será la siguiente:

Los valores del impacto y la probabilidad deberán ingresarse en el Cuadro de Evaluación de Riesgos para obtener el nivel de riesgo. El nivel de riesgo se calculará multiplicando los dos valores.

❖ Evaluación del riesgo.

La siguiente imagen muestra un mapa de calor con los resultados de las valoraciones señaladas con anterioridad.



La siguiente tabla muestra el nivel de riesgo en escala cuantitativa y cualitativa.

Impacto		Probabilidad		Nivel de riesgo	
Cuantitativo	**Cualitativo**	**Cuantitativo**	**Cualitativo**	**Cuantitativo**	**Cualitativo**
3	Alto	1	Baja	3	Medio
3	Alto	2	Media	6	Alto
3	Alto	3	Alta	9	Alto
2	Medio	1	Baja	2	Bajo
2	Medio	2	Media	4	Medio
2	Medio	3	Alta	6	Alto
1	Bajo	1	Baja	1	Bajo
1	Bajo	2	Media	2	Bajo
1	Bajo	3	Alta	3	Medio

Una vez realizadas las valoraciones, se procederá a evaluar el riesgo comparando el nivel de riesgo con los criterios de aceptación del riesgo establecidos previamente, en donde:

1. Los valores 1 y 2 (bajo) serán riesgos aceptables.
2. Los valores 3 y 4 (medio) serán riesgos no aceptables, por lo que deberán ser tratados.
3. Los valores 6 y 9 (alto) serán riesgos no aceptables por lo que deberán ser tratados.
4. Para los riesgos no aceptables, se deberá priorizar el tratamiento del riesgo para aquellos activos de mayor a menor valor; 3 (alto), 2 (medio) y 1 (bajo).

Con el fin de evitar retrabajo o costos innecesarios, en su caso, se deben identificar controles existentes que permitan reducir el nivel de riesgo; éstos tendrán que ser ingresados en el Cuadro de Evaluación de Riesgos, determinando su nivel de madurez:

- Si el nivel de madurez de los controles existentes es 1, el riesgo no tendrá que ser tratado.
- Si el nivel de madurez de los controles existentes es 2 el riesgo deberá ser tratado.

❖ Identificación de los propietarios de los riesgos.

Para cada riesgo se deberá identificar un propietario: persona o unidad administrativa con la responsabilidad y la autoridad para gestionar un riesgo, destacando que podrá o no ser el mismo que el propietario del activo.

❖ Tratamiento del riesgo.

El tratamiento de riesgos se implementará a través del Cuadro de tratamiento de riesgos, donde se copiarán todos los riesgos identificados como no aceptables desde el Cuadro de evaluación de riesgos. Esta tarea será realizada por el propietario del riesgo, y en los casos que lo requieran, de manera conjunta y coordinada con el custodio del activo.

Para los riesgos valorados en 3 y 4, así como 6 y 9, se deberá seleccionar una opción de tratamiento que puede ser: reducir el riesgo, lo que implica tomar acciones para disminuir la probabilidad o las consecuencias negativas asociadas; aceptar el riesgo, que se refiere a la aceptación de la posible pérdida o ganancia, permitida solo si otras opciones de tratamiento resultan más costosas que el impacto potencial; evitar el riesgo, que consiste en decidir no participar en una situación riesgosa; o transferir el riesgo, que implica compartir con un tercero la carga de la pérdida o ganancia, como a través de un seguro o un contrato.

En el caso de optar por la reducción del riesgo, será necesario evaluar el nuevo valor de impacto y probabilidad en el Cuadro de tratamiento de riesgos para medir la efectividad de los controles planificados.

❖ Análisis de brecha.

La Unidad de Transparencia con las áreas correspondientes deberán integrar el Plan de tratamiento de riesgos en el que se planificará la implementación de los controles.

❖ Revisiones periódicas de la evaluación y el tratamiento de riesgos.

Los propietarios de riesgos deberán revisar los riesgos vigentes y actualizar los Cuadros de evaluación de riesgos y tratamiento de riesgos, según los nuevos riesgos identificados. Esta revisión se llevará a cabo al menos una vez al año, y con mayor frecuencia si se producen cambios organizacionales significativos, importantes modificaciones en la tecnología, alteraciones en los objetivos estratégicos, o cambios en el entorno del marco normativo aplicable relacionado con la seguridad de la información y los datos personales.

❖ Informes.

La Unidad de Transparencia documentará los resultados de la evaluación y del tratamiento de riesgos y de todas las revisiones subsecuentes.

En este sentido, la Unidad de Transparencia supervisará el progreso de la implementación del presente **Plan de Trabajo** e informará periódicamente los resultados al Comité de Transparencia.

❖ Resultados.

Conforme a lo anterior, los análisis de riesgos y de brecha se llevaron a cabo a partir de tres fuentes de información clave:

1. **Análisis de riesgos de la infraestructura tecnológica y recursos de software y hardware**. Este análisis abarcó la evaluación de los sistemas, dispositivos y plataformas tecnológicas que la Universidad utiliza para llevar a cabo sus operaciones.

2. **Análisis de riesgos de hábitos de seguridad del personal de la Universidad Pedagógica Nacional**. Este análisis se enfocó en evaluar las prácticas y comportamientos de seguridad de las personas servidoras públicas, sin asociarlas directamente a un tratamiento específico.

3. **Análisis de riesgos a partir de los inventarios de tratamientos de datos personales**. Este análisis fue realizado de manera específica para cada uno de los tratamientos reportados en los inventarios de datos personales de la Universidad, teniendo en cuenta sus particularidades, contextos y riesgos inherentes a cada proceso.

DESARROLLO DEL PLAN DE TRABAJO PARA LA GESTIÓN Y TRATAMIENTO DE RIESGOS.

El presente ***Plan de Trabajo para la Gestión y Tratamiento de Riesgos*** ha sido elaborado como parte de los esfuerzos continuos de esta Universidad para garantizar la seguridad de la información y la protección de los datos personales en sus diversas actividades y procesos.

El objetivo principal de este plan es reducir los riesgos identificados, con el fin de alcanzar un nivel aceptable de seguridad que proteja tanto los recursos tecnológicos como los datos personales en posesión de la Universidad.

En este sentido, como resultado de los análisis de riesgos y de brechas realizados por cada uno de los tratamientos de datos personales que realizan todas las áreas de esta Casa de Estudios, se identificaron diversas áreas de riesgo que requieren la implementación de controles específicos para reducir el nivel de riesgo a un nivel aceptable.

Los controles propuestos en este Plan de Trabajo están alineados con las mejores prácticas y normas internacionales, específicamente con los **Anexos de la Norma ISO/IEC 27001:2013**, la cual establece los lineamientos para la gestión de la seguridad de la información.

Una vez expuesto lo anterior, a continuación se establece las actividades específicas a realizar, el responsable que las va a implementar, así como el tiempo y recursos destinados a su realización:

1. Dirección de Biblioteca y Apoyo Académico (DByAA).

Control Norma ISO 27001	Actividad	Responsable	Fecha programada
11.2.4 Mantenimiento de equipo	Los equipos de cómputo deberán mantenerse correctamente para asegurar su continua disponibilidad e integridad.	DByAA (Solicitarlo) Área de Informática (Ejecutarlo)	Enero a diciembre de 2025
9.1.1 Política de control de acceso	Se debe establecer, documentar y revisar una política de control de acceso basada en los requisitos de la unidad administrativa y de la seguridad de la información.	DByAA	Enero a diciembre de 2025
11.1.4 Protección contra amenazas externas y ambientales	Se debe diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.	DByAA	Enero a diciembre de 2025
11.2.7 Disposición o reutilización segura del equipo	Todos los elementos del equipo que contiene medios de almacenamiento deben ser verificados para garantizar que cualquier dato sensible y software licenciado ha sido eliminado o sobrescrito de manera segura previo a su disposición o reutilización.	DByAA	Enero a diciembre de 2025

2. Centro de Enseñanza y Aprendizaje de Lenguas (CEAL).

Control Norma ISO 27001	Actividad	Responsable	Fecha programada
11.2.4 Mantenimiento de equipo	Los equipos de cómputo deberán mantenerse correctamente para asegurar su continua disponibilidad e integridad.	CEAL (Solicitarlo) Área de Informática (Ejecutarlo)	Enero a diciembre de 2025
9.1.1 Política de control de acceso	Se debe establecer, documentar y revisar una política de control de acceso basada en los requisitos de la unidad administrativa y de la seguridad de la información.	CEAL	Enero a diciembre de 2025
11.2.7 Disposición o reutilización segura del equipo	Todos los elementos del equipo que contiene medios de almacenamiento deben ser verificados para garantizar que cualquier dato sensible y software licenciado ha sido eliminado o sobrescrito de manera segura previo a su disposición o reutilización.	CEAL	Enero a diciembre de 2025
9.2.1 Registro y cancelación de usuarios	Se debe implementar un proceso formal de registro y cancelación de usuarios para permitir la asignación de derechos de acceso.	CEAL	Enero a diciembre de 2025

3. Dirección de Comunicación Social (DCS).

Control Norma ISO 27001	Actividad	Responsable	Fecha programada
11.2.4 Mantenimiento de equipo	Los equipos de cómputo deberán mantenerse correctamente para asegurar su continua disponibilidad e integridad.	DCS (Solicitarlo) Área de Informática (Ejecutarlo)	Enero a diciembre de 2025
11.2.1 Ubicación y protección del equipo	El equipo debe estar situado y protegido para reducir los riesgos de amenazas ambientales y peligros, y las oportunidades para el acceso no autorizado.	DCS	Enero a diciembre de 2025
7.2.2 Concientización, educación y capacitación en seguridad de la información	Todas las personas servidoras públicas que participen en algún tratamiento de datos personales deben recibir concientización, educación y capacitación apropiada y actualizaciones regulares de políticas y procedimientos organizacionales, principalmente cuando sea relevante para la realización de sus funciones de trabajo.	DCS	Enero a diciembre de 2025

4. Comité de Ética.

Control Norma ISO 27001	Actividad	Responsable	Fecha programada
6.1.1 Roles y responsabilidades para la seguridad de la información	Todas las responsabilidades de la seguridad de la información deben definirse y asignarse.	Presidencia del Comité de Ética	Enero a diciembre de 2025

Control Norma ISO 27001	Actividad	Responsable	Fecha programada
13.2.4 Acuerdos de confidencialidad o de no divulgación	Se deben identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación reflejando las necesidades de la organización para la protección de la información.	Presidencia del Comité de Ética	Enero a diciembre de 2025
11.1.3 Aseguramiento de oficinas, salas e instalaciones	Se debe diseñar y aplicar seguridad física para oficinas, salas e instalaciones.	Presidencia del Comité de Ética	Enero a diciembre de 2025

5. Secretaría Administrativa (SA).

Control Norma ISO 27001	Actividad	Responsable	Fecha programada
11.2.4 Mantenimiento de equipo	Los equipos de cómputo deberán mantenerse correctamente para asegurar su continua disponibilidad e integridad.	SA (Solicitarlo) Área de Informática (Ejecutarlo)	Enero a diciembre de 2025
7.2.2 Concientización, educación y capacitación en seguridad de la información	Todas las personas servidoras públicas que participen en algún tratamiento de datos personales deben recibir concientización, educación y capacitación apropiada y actualizaciones regulares de políticas y procedimientos organizacionales, principalmente cuando sea relevante para la realización de sus funciones de trabajo.	SA	Enero a diciembre de 2025
9.1.1 Política de control de acceso	Se debe establecer, documentar y revisar una política de control de acceso basada en los requisitos de la unidad administrativa y de la seguridad de la información.	SA	Enero a diciembre de 2025

6. Área de Informática.

Control Norma ISO 27001	Actividad	Responsable	Fecha programada
11.2.4 Mantenimiento de equipo	Los equipos de cómputo deberán mantenerse correctamente para asegurar su continua disponibilidad e integridad.	Área de Informática	Enero a diciembre de 2025
11.2.1 Ubicación y protección del equipo	El equipo debe estar situado y protegido para reducir los riesgos de amenazas ambientales y peligros, y las oportunidades para el acceso no autorizado.	Área de Informática	Enero a diciembre de 2025
9.4 Control de acceso a sistemas y aplicaciones	Se deberá implementar un sistema integral de control de acceso a sistemas y aplicaciones, que incluya la restricción de acceso a la información y funciones según las políticas establecidas, el uso de procedimientos de inicio de sesión seguro, sistemas de administración de contraseñas de calidad y la	Área de Informática	Enero a diciembre de 2025

Control Norma ISO 27001	Actividad	Responsable	Fecha programada
	restricción del acceso al código fuente de los programas.		
5.1.1 Políticas de seguridad de la información	Se debe definir, aprobar, publicar y comunicar a todos los empleados y partes externas relevantes un conjunto de políticas para la seguridad de la información.	Área de Informática	Enero a diciembre de 2025

7. Área de Recursos Financieros (ÁRF).

Control Norma ISO 27001	Actividad	Responsable	Fecha programada
11.2.4 Mantenimiento de equipo	Los equipos de cómputo deberán mantenerse correctamente para asegurar su continua disponibilidad e integridad.	ÁRF (Solicitarlo) Área de Informática (Ejecutarlo)	Enero a diciembre de 2025
7.2.2 Concientización, educación y capacitación en seguridad de la información	Todas las personas servidoras públicas que participen en algún tratamiento de datos personales deben recibir concientización, educación y capacitación apropiada y actualizaciones regulares de políticas y procedimientos organizacionales, principalmente cuando sea relevante para la realización de sus funciones de trabajo.	ÁRF	Enero a diciembre de 2025
13.2.4 Acuerdos de confidencialidad o de no divulgación	Se deben identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación reflejando las necesidades de la organización para la protección de la información.	ÁRF	Enero a diciembre de 2025
6.1.3 Contacto con autoridades	Se deben mantener contactos apropiados con las autoridades para el uso de aplicativos.	ÁRF	Enero a diciembre de 2025
9.4 Control de acceso a sistemas y aplicaciones	Se deberá implementar un sistema integral de control de acceso a sistemas y aplicaciones, que incluya la restricción de acceso a la información y funciones según las políticas establecidas.	ÁRF	Enero a diciembre de 2025

8. Área de Recursos Materiales y Servicios (ÁRMS).

Control Norma ISO 27001	Actividad	Responsable	Fecha programada
11.2.4 Mantenimiento de equipo	Los equipos deberán mantenerse correctamente para asegurar su continua disponibilidad e integridad.	ÁRMS (Solicitarlo) Área de Informática (Ejecutarlo)	Enero a diciembre de 2025
7.2.2 Concientización, educación y capacitación en seguridad de la información	Todas las personas servidoras públicas que participen en algún tratamiento de datos personales deben recibir concientización, educación y capacitación apropiada y actualizaciones regulares de políticas y	ÁRMS	Enero a diciembre de 2025

Control Norma ISO 27001	Actividad	Responsable	Fecha programada
	procedimientos organizacionales, principalmente cuando sea relevante para la realización de sus funciones de trabajo.		
13.2.4 Acuerdos de confidencialidad o de no divulgación	Se deben identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación reflejando las necesidades de la organización para la protección de la información.	ÁRMS	Enero a diciembre de 2025

9. Unidad de Igualdad de Género e Inclusión (UIGI)

Control Norma ISO 27001	Actividad	Responsable	Fecha programada
11.2.4 Mantenimiento de equipo	Los equipos de cómputo deberán mantenerse correctamente para asegurar su continua disponibilidad e integridad.	UIGI (Solicitarlo) Área de Informática (Ejecutarlo)	Enero a diciembre de 2025
11.1.3 Aseguramiento de oficinas, salas e instalaciones	Se debe diseñar y aplicar seguridad física para oficinas, salas e instalaciones.	UIGI	Enero a diciembre de 2025
13.2.4 Acuerdos de confidencialidad o de no divulgación	Se deben identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación reflejando las necesidades de la organización para la protección de la información.	UIGI	Enero a diciembre de 2025
11.1.1 Perímetro de seguridad física	Se deben definir y utilizar perímetros de seguridad para proteger las áreas que contienen información ya sea sensible o crítica y las instalaciones de procesamiento de la información.	UIGI	Enero a diciembre de 2025
7.2.2 Concientización, educación y capacitación en seguridad de la información	Todas las personas servidoras públicas que participen en algún tratamiento de datos personales deben recibir concientización, educación y capacitación apropiada y actualizaciones regulares de políticas y procedimientos organizacionales, principalmente cuando sea relevante para la realización de sus funciones de trabajo.	UIGI	Enero a diciembre de 2025

10. Área de Personal (ÁP).

Control Norma ISO 27001	Actividad	Responsable	Fecha programada
11.2.4 Mantenimiento de equipo	Los equipos de cómputo deberán mantenerse correctamente para asegurar su continua disponibilidad e integridad.	ÁP (Solicitarlo) Área de Informática (Ejecutarlo)	Enero a diciembre de 2025
Validación de datos de entrada.	Cuando se proporcionen datos a un sistema o formato, se debe validar que estos sean ingresados de forma correcta, tal que no	Área de Personal	Enero a diciembre de 2025

Control Norma ISO 27001	Actividad	Responsable	Fecha programada
	produzcan conflictos de tratamiento posteriores.		
12.3.1 Respaldos de la información	Copias de respaldos de la información, software e imágenes de sistemas deben realizarse y probarse.	Área de personal.	Enero a diciembre de 2025
7.2.2 Concientización, educación y capacitación en seguridad de la información	Todas las personas servidoras públicas que participen en algún tratamiento de datos personales deben recibir concientización, educación y capacitación apropiada y actualizaciones regulares de políticas y procedimientos organizacionales, principalmente cuando sea relevante para la realización de sus funciones de trabajo.	Área de personal	Enero a diciembre de 2025
13.2.4 Acuerdos de confidencialidad o de no divulgación	Se deben identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación reflejando las necesidades de la organización para la protección de la información.	Área de personal	Enero a diciembre de 2025
9.4 Control de acceso a sistemas y aplicaciones	Se deberá implementar un sistema integral de control de acceso a sistemas y aplicaciones, que incluya la restricción de acceso a la información y funciones según las políticas establecidas.	Área de personal	Enero a diciembre de 2025
11.1.3 Aseguramiento de oficinas, salas e instalaciones	Se debe diseñar y aplicar seguridad física para oficinas, salas e instalaciones.	Área de personal	Enero a diciembre de 2025

11. Dirección de Planeación.

Control Norma ISO 27001	Actividad	Responsable	Fecha programada
11.2.4 Mantenimiento de equipo	Los equipos de cómputo deberán mantenerse correctamente para asegurar su continua disponibilidad e integridad.	DP (Solicitarlo) Área de Informática (Ejecutarlo)	Enero a diciembre de 2025
13.2.4 Acuerdos de confidencialidad o de no divulgación	Se deben identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación reflejando las necesidades de la organización para la protección de la información.	Dirección de Planeación	Enero a diciembre de 2025

12. Dirección de la Coordinación de Unidades (DCU).

Control Norma ISO 27001	Actividad	Responsable	Fecha programada
11.2.4 Mantenimiento de equipo	Los equipos de cómputo deberán mantenerse correctamente para asegurar su continua disponibilidad e integridad.	DCU (Solicitarlo) Área de Informática (Ejecutarlo)	Enero a diciembre de 2025

Control Norma ISO 27001	Actividad	Responsable	Fecha programada
7.2.2 Concientización, educación y capacitación en seguridad de la información	Todas las personas servidoras públicas que participen en algún tratamiento de datos personales deben recibir concientización, educación y capacitación apropiada y actualizaciones regulares de políticas y procedimientos organizacionales, principalmente cuando sea relevante para la realización de sus funciones de trabajo.	DCU	Enero a diciembre de 2025

13. Dirección de Difusión y Extensión Universitaria (DDyEU).

Control Norma ISO 27001	Actividad	Responsable	Fecha programada
11.2.4 Mantenimiento de equipo	Los equipos de cómputo deberán mantenerse correctamente para asegurar su continua disponibilidad e integridad.	DDyEU (Solicitarlo) Área de Informática (Ejecutarlo)	Enero a diciembre de 2025
13.2.4 Acuerdos de confidencialidad o de no divulgación	Se deben identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación reflejando las necesidades de la organización para la protección de la información.	DDyEU.	Enero a diciembre de 2025
12.3 Respaldos (copias de seguridad)	Copias de respaldos de la información, software e imágenes de sistemas deben realizarse y probarse.	DDyEU.	Enero a diciembre de 2025

14. Comisión Académica Dictaminadora (CAD).

Control Norma ISO 27001	Actividad	Responsable	Fecha programada
11.2.4 Mantenimiento de equipo	Los equipos de cómputo deberán mantenerse correctamente para asegurar su continua disponibilidad e integridad.	CAD (Solicitarlo) Área de Informática (Ejecutarlo)	Enero a diciembre de 2025
12.3 Respaldos (copias de seguridad)	Copias de respaldos de la información.		Enero a diciembre de 2025

15. Área de Servicios Escolares (ÁSE).

Control Norma ISO 27001	Actividad	Responsable	Fecha programada
11.2.4 Mantenimiento de equipo	Los equipos de cómputo deberán mantenerse correctamente para asegurar su continua disponibilidad e integridad.	ÁSE (Solicitarlo) Área de Informática (Ejecutarlo)	Enero a diciembre de 2025

16. Dirección de Servicios Jurídicos (DSJ).

Control Norma ISO 27001	Actividad	Responsable	Fecha programada
11.2.4 Mantenimiento de equipo	Los equipos de cómputo deberán mantenerse correctamente para asegurar su continua disponibilidad e integridad.	DSJ (Solicitarlo) Área de Informática (Ejecutarlo)	Enero a diciembre de 2025
11.1.3 Aseguramiento de oficinas, salas e instalaciones	Se debe diseñar y aplicar seguridad física para oficinas, salas e instalaciones.	DSJ	Enero a diciembre de 2025
13.2.4 Acuerdos de confidencialidad o de no divulgación	Se deben identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación reflejando las necesidades de la organización para la protección de la información.	DSJ	Enero a diciembre de 2025
7.2.2 Concientización, educación y capacitación en seguridad de la información	Todas las personas servidoras públicas que participen en algún tratamiento de datos personales deben recibir concientización, educación y capacitación apropiada y actualizaciones regulares de políticas y procedimientos organizacionales, principalmente cuando sea relevante para la realización de sus funciones de trabajo.	DSJ	Enero a diciembre de 2025

17. Oficina de la Rectoría.

Control Norma ISO 27001	Actividad	Responsable	Fecha programada
11.2.4 Mantenimiento de equipo	Los equipos de cómputo deberán mantenerse correctamente para asegurar su continua disponibilidad e integridad.	Oficina de la Rectoría (Solicitarlo) Área de Informática (Ejecutarlo)	Enero a diciembre de 2025

18. Secretaría Académica.

Control Norma ISO 27001	Actividad	Responsable	Fecha programada
11.2.4 Mantenimiento de equipo	Los equipos de cómputo deberán mantenerse correctamente para asegurar su continua disponibilidad e integridad.	Secretaría Académica (Solicitarlo) Área de Informática (Ejecutarlo)	Enero a diciembre de 2025
7.2.2 Concientización, educación y capacitación en seguridad de la información	Todas las personas servidoras públicas que participen en algún tratamiento de datos personales deben recibir concientización, educación y capacitación apropiada y actualizaciones regulares de políticas y procedimientos organizacionales,	Secretaría Académica	Enero a diciembre de 2025

Control Norma ISO 27001	Actividad	Responsable	Fecha programada
	principalmente cuando sea relevante para la realización de sus funciones de trabajo.		
11.1.3 Aseguramiento de oficinas, salas e instalaciones	Se debe diseñar y aplicar seguridad física para oficinas, salas e instalaciones.	Secretaría Académica	Enero a diciembre de 2025
14.1 Requisitos de seguridad de sistemas de información.	Los requisitos relacionados con la seguridad de la información deben estar incluidos en los requisitos para los nuevos sistemas de información o mejoras a los sistemas de información existentes.	Secretaría Académica	Enero a diciembre de 2025

19. Centro de Atención a Estudiantes (CAE).

Control Norma ISO 27001	Actividad	Responsable	Fecha programada
9.4.3 Sistema de administración de contraseñas	Los sistemas de administración de contraseñas deben ser interactivos y deben asegurar contraseñas de calidad.	CAE	Enero a diciembre de 2025

20. Unidad de Transparencia.

Control Norma ISO 27001	Actividad	Responsable	Fecha programada
11.2.4 Mantenimiento de equipo	Los equipos de cómputo deberán mantenerse correctamente para asegurar su continua disponibilidad e integridad.	UT (Solicitarlo) Área de Informática (Ejecutarlo)	Enero a diciembre de 2025

21. Infraestructura tecnológica y recursos de software y hardware de la Universidad Pedagógica Nacional.

Control Norma ISO 27001	Actividad	Responsable	Fecha programada
11.2.4 Mantenimiento de equipo	Los equipos de cómputo deberán mantenerse correctamente para asegurar su continua disponibilidad e integridad.	Área de Informática	Enero a diciembre de 2025
6.1.5 Seguridad de la información en la gestión de proyectos	La seguridad de la información debe incluirse en la administración de todos los proyectos, independientemente del tipo de proyecto.	Área de Informática	Enero a diciembre de 2025

Finalmente, el **SEGUIMIENTO** a la ejecución del presente Plan de Trabajo se realizará de conformidad con los Mecanismos de Monitoreo y Revisión de las Medidas de Seguridad contenidos en el Documento de Seguridad de la Universidad Pedagógica Nacional (UPN).

EDUCACIÓN
SECRETARÍA DE EDUCACIÓN PÚBLICA

UNIVERSIDAD PEDAGÓGICA NACIONAL

PROGRAMA DE CAPACITACIÓN EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES

UNIVERSIDAD PEDAGÓGICA NACIONAL

PROGRAMA DE CAPACITACIÓN EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES

En cumplimiento a los artículos 30, fracción III; 33, fracción VIII y 35, fracción VIII de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y, 64 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público, debe elaborarse un programa de capacitación y actualización permanente de las personas servidoras públicas de la Universidad, sobre las obligaciones y cumplimiento de los principios y deberes en materia de protección de datos personales.

En este sentido, en la 5a Sesión Ordinaria 2024, el Comité de Transparencia de la Universidad Pedagógica Nacional, mediante Acuerdo **CT-UPN/2023/ORD-05/01,** a efectos de atender lo establecido en el artículo 30 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, aprobó el **PROGRAMA DE CAPACITACIÓN Y ACTUALIZACIÓN DEL PERSONAL SOBRE LAS OBLIGACIONES Y DEMÁS DEBERES EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES DE LA UNIVERSIDAD PEDAGÓGICA NACIONAL PARA EL AÑO 2024** , mismo que se adjunta al presente documento.

De esta manera, en el citado programa se considera un programa de capacitación en dos vertientes: Capacitación Básica y Capacitación Especializada.

Capacitación Básica

El objeto de esta capacitación es que las personas conozcan aspectos teóricos, conceptuales y normativos fundamentales en materia de protección de datos personales.

En este rubro se consideran un curso de introducción a la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, enfocado en conocer los aspectos relevantes sobre la normatividad de en la materia, con la siguiente temática:

- Introducción a la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

  - Objetivos y ámbitos de aplicación.
  - Principios y deberes de protección de datos personales.
  - Derechos ARCO.
  - Medios de impugnación.
  - Casos prácticos.

Capacitación Especializada.

Esta capacitación se dirige a atender las necesidades o problemáticas sobre aspectos particulares de la normatividad en materia de protección de datos personales.

En este sentido, se consideran cursos con las siguientes temáticas:

- Clasificación de información.

- Fundamentos del Documento de Seguridad en Materia de Protección de Datos Personales.

- Elaboración del Documento de Seguridad en Materia de Protección de Datos Personales.

- Aviso de Privacidad - Sector Público.

- Temas Especializados en Protección de Datos Personales.

- Esquemas de Mejores Prácticas en Materia de Protección de Datos Personales en el Sector Público.

PROGRAMA DE CAPACITACIÓN EN PROTECCIÓN DE DATOS PERSONALES 2024

Nombre del Sujeto Obligado:	UNIVERSIDAD PEDAGÓGICA NACIONAL (UPN)
Objetivo del Programa de Capacitación:	A partir de la capacitación de las personas servidoras públicas en la materia de protección de datos personales, se pretende lograr que la Universidad Pedagógica Nacional cumpla con los deberes y principios establecidos en la *Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados*, de tal forma que este responsable garantice el derecho humano de protección de datos personales de las personas titulares de quienes estén en posesión de esta Casa de Estudios.

Sector:	Educación y Cultura
Fecha de Elaboración:	27/05/2024

TOTAL DE PERSONAS SERVIDORAS PÚBLICAS O INTEGRANTES DEL SUJETO OBLIGADO	SUBTOTAL
Mandos Superiores (Secretarios(as), Subsecretarios(as), Directores(as) Generales, o puestos del 1o, 2do y 3er nivel de mando)	3
Mandos Medios (Directores(as) de Área, Subdirectores(as) de Área, Jefes(as) de Departamento, Enlaces)	49
Técnicos Operativos (Analistas, Personal Técnico, Personal Operativo, o puestos similares)	671
TOTAL DE SERVIDORES PÚBLICOS O INTEGRANTES DEL SUJETO OBLIGADO (Suma del total de personas servidoras públicas / integrantes del Sujeto Obligado)	723

UNIVERSO A CAPACITAR EN 2024	SUBTOTAL
Mandos Superiores (Secretarios(as), Subsecretarios(as), Directores(as) Generales, o puestos del 1o, 2do y 3er nivel de mando)	3
Mandos Medios (Directores(as) de Área, Subdirectores(as) de Área, Jefes(as) de Departamento, Enlaces)	70
Técnicos Operativos (Analistas, Personal Técnico, Personal Operativo, o puestos similares)	69
Total	142

	Nombre de la Acción de Capacitación	Personas Servidoras Públicas o Integrantes del Sujeto Obligado Programados a Capacitar en 2024 (Anotar el total de personas a capacitar en cada acción de acción de capacitación y modalidad)														TOTALES			
		COMITÉ DE TRANSPARENCIA			UNIDAD DE TRANSPARENCIA			MANDOS SUPERIORES			MANDOS MEDIOS			TÉCNICOS OPERATIVOS			TOTAL PROGRAMADOS: PRESENCIAL / PRESENCIAL A DISTANCIA	TOTAL PROGRAMADOS EM LÍNEA (CEVINAI)	TOTAL PROGRAMADOS CON RECURSOS PROPIOS	TOTAL DE PARTICIPANTES PROGRAMADOS
		PRESENCIAL / PRESENCIAL A DISTANCIA	LÍNEA (CEVINAI)	RECURSOS PROPIOS	PRESENCIAL / PRESENCIAL A DISTANCIA	LÍNEA (CEVINAI)	RECURSOS PROPIOS	PRESENCIAL / PRESENCIAL A DISTANCIA	LÍNEA (CEVINAI)	RECURSOS PROPIOS	PRESENCIAL / PRESENCIAL A DISTANCIA	LÍNEA (CEVINAI)	RECURSOS PROPIOS	PRESENCIAL / PRESENCIAL A DISTANCIA	LÍNEA (CEVINAI)	RECURSOS PROPIOS				
Capacitación Básica	Introducción a la LFTAIP	0	ND	0	0	ND	0	1	ND	0	16	ND	0	2	ND	0	19	ND	0	19
	Introducción a la LGPDPPSO	0	ND	0	0	ND	0	1	ND	0	16	ND	0	16	ND	0	33	ND	0	33
	Ética Pública	0	ND	0	0	ND	0	0	ND	0	0	ND	0	1	ND	0	1	ND	0	1
	Introducción a la Ley General de Archivos	0	ND	0	0	ND	0	1	ND	0	16	ND	0	19	ND	0	36	ND	0	36

	Nombre de la Acción de Capacitación	Personas Servidoras Públicas o Integrantes del Sujeto Obligado Programados a Capacitar en 2024 (Anotar el total de personas a capacitar en cada modalidad)														TOTALES			
		COMITÉ DE TRANSPARENCIA			UNIDAD DE TRANSPARENCIA			MANDOS SUPERIORES			MANDOS MEDIOS			TÉCNICOS OPERATIVOS			TOTAL PROGRAMADOS PRESENCIAL / PRESENCIAL A DISTANCIA	TOTAL PROGRAMADOS E.M. LÍNEA (CEVINAI)	TOTAL PROGRAMADOS CON RECURSOS PROPIOS	TOTAL DE PARTICIPANTES PROGRAMADOS
		PRESENCIAL / PRESENCIAL A DISTANCIA	LÍNEA (CEVINAI)	RECURSOS PROPIOS	PRESENCIAL / PRESENCIAL A DISTANCIA	LÍNEA (CEVINAI)	RECURSOS PROPIOS	PRESENCIAL / PRESENCIAL A DISTANCIA	LÍNEA (CEVINAI)	RECURSOS PROPIOS	PRESENCIAL / PRESENCIAL A DISTANCIA	LÍNEA (CEVINAI)	RECURSOS PROPIOS	PRESENCIAL / PRESENCIAL A DISTANCIA	LÍNEA (CEVINAI)	RECURSOS PROPIOS				
Capacitación Especializada	Clasificación de la Información y Prueba de Daño / Clasificación de la Información	0	ND	0	0	ND	0	0	ND	0	1	ND	0	5	ND	0	6	ND	0	6
	Fundamentos del Documento de Seguridad en Materia de Protección de Datos Personales	0	ND	0	0	ND	0	0	ND	0	1	ND	0	1	ND	0	2	ND	0	2
	Elaboración del Documento de Seguridad en Materia de Protección de Datos Personales	0	ND	0	0	ND	0	0	ND	0	1	ND	0	1	ND	0	2	ND	0	2
	Aviso de Privacidad - Sector Público	0	ND	0	0	ND	0	0	ND	0	3	ND	0	7	ND	0	10	ND	0	10
	Temas Especializados en AIP y PDP	0	ND	0	2	ND	0	0	ND	0	2	ND	0	1	ND	0	5	ND	0	5
	Esquemas de Mejores Prácticas en Materia de Protección de Datos Personales en el Sector Público	0	ND	0	0	ND	0	0	ND	0	1	ND	0	0	ND	0	1	ND	0	1
	Obligaciones de Transparencia y Carga de Información en el SIPOT / Guía Instructiva para el Uso del SIPOT	1	ND	0	0	ND	0	0	ND	0	1	ND	0	8	ND	0	10	ND	0	10
	Gobierno Abierto	0	ND	0	0	ND	0	0	ND	0	1	ND	0	1	ND	0	2	ND	0	2
	Transparencia Proactiva	0	ND	0	0	ND	0	0	ND	0	3	ND	0	0	ND	0	3	ND	0	3
	Datos Abiertos	0	ND	0	2	ND	0	0	ND	0	0	ND	0	0	ND	0	2	ND	0	2
	Obligaciones de Transparencia en Materia de Archivos y Gestión Documental	2	ND	0	2	ND	0	0	ND	0	0	ND	0	2	ND	0	6	ND	0	6
	Políticas de Acceso a la Información	0	ND	0	0	ND	0	0	ND	0	1	ND	0	3	ND	0	4	ND	0	4

Ciudad de México, 26 de noviembre, 2024

INFORME DE CUMPLIMIENTO AL *PROGRAMA DE CAPACITACIÓN EN TRANSPARENCIA, ACCESO A LA INFORMACIÓN, PROTECCIÓN DE DATOS PERSONALES Y TEMAS RELACIONADOS 2024 DE LA UNIVERSIDAD PEDAGÓGICA NACIONAL* (PCTAIPDPTR 2024)

❖ METAS ESTABLECIDAS EN EL PCTAIPDPTR 2024

a) Metas establecidas conforme el universo a capacitar y el nivel de mando:

UNIVERSO A CAPACITAR EN 2024	SUBTOTAL DE PARTICIPACIONES
Mandos Superiores *(Secretarios(as), Subsecretarios(as), Directores(as) Generales, o puestos del 1o, 2do y 3er nivel de mando)*	3
Mandos Medios *(Directores (as) de Área, Subdirectores(as) de Área, Jefes(as) de Departamento, Enlaces)*	81
Técnicos Operativos *(Analistas, Personal Técnico, Personal Operativo, o puestos similares)*	72
Total	156

b) Metas establecidas conforme a la oferta de cursos*:

CURSOS 2024	SUBTOTAL DE PARTICIPACIONES
Aviso de Privacidad / 4to. Taller Nacional del Aviso de Privacidad	14
Clasificación de la Información y prueba de daño	6
Datos Abiertos	2
Documento de Seguridad en materia de Protección de Datos Personales	2
Elaboración del Documento de Seguridad	5

CURSOS 2024	SUBTOTAL DE PARTICIPACIONES
Esquemas de Mejores Prácticas en materia de Protección de Datos Personales	1
Ética Pública	1
Gobierno Abierto	2
Introducción a la Ley Federal de Transparencia y Acceso a la Información Pública	23
Introducción a la Ley General de Archivos	39
Introducción a la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados	35
Obligaciones de Transparencia en Materia de Archivos y Gestión Documental	6
Obligaciones de Transparencia y carga de Información en el SIPOT	8
Políticas de Acceso a la Información	4
Sistema de Gestión de Seguridad de Datos Personales Sector Público	2
Temas especializados en Acceso a la Información y Protección de Datos Personales (Recurso de Revisión)	3
Transparencia Proactiva (4 horas) (Presencial)	3
Aviso de Privacidad / 4to. Taller Nacional del Aviso de Privacidad	14
Total	**156**

* Para el año 2024, el INAI únicamente ofertó cursos en la modalidad presencial.

❖ COMPARATIVO ENTRE METAS ESTABLECIDAS EN EL PCTAIPDPTR 2024 Y LAS PARTICIPACIONES ACREDITADAS.

a) Comparativo por universo a capacitar y nivel de mando:

UNIVERSO A CAPACITAR EN 2024	PARTICIPACIONES COMPROMETIDAS	PARTICIPACIONES ACREDITADAS
Mandos Superiores *(Secretarios(as), Subsecretarios(as), Directores(as) Generales, o puestos del 1o, 2do y 3er nivel de mando)*	3	3
Mandos Medios	81	86

(Directores (as) de Área, Subdirectores(as) de Área, Jefes(as) de Departamento, Enlaces)		
Técnicos Operativos *(Analistas, Personal Técnico, Personal Operativo, o puestos similares)*	72	72
Total	159	161

b) Comparativo por cursos:

CURSOS 2024	PARTICIPACIONES COMPROMETIDAS	PARTICIPACIONES ACREDITADAS
Aviso de Privacidad / 4to. Taller Nacional del Aviso de Privacidad	14	14
Clasificación de la Información y prueba de daño	6	6
Datos Abiertos	2	2
Documento de Seguridad en materia de Protección de Datos Personales	2	2
Elaboración del Documento de Seguridad	5	5
Esquemas de Mejores Prácticas en materia de Protección de Datos Personales	1	1
Ética Pública	1	2
Gobierno Abierto	2	2
Introducción a la Ley Federal de Transparencia y Acceso a la Información Pública	23	24
Introducción a la Ley General de Archivos	39	39
Introducción a la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados	35	35
Obligaciones de Transparencia en Materia de Archivos y Gestión Documental	6	6
Obligaciones de Transparencia y carga de Información en el SIPOT	8	8
Políticas de Acceso a la Información	4	4
Sistema de Gestión de Seguridad de Datos Personales Sector Público	2	2

CURSOS 2024	PARTICIPACIONES COMPROMETIDAS	PARTICIPACIONES ACREDITADAS
Temas especializados en Acceso a la Información y Protección de Datos Personales (Recurso de Revisión)	3	3
Transparencia Proactiva (4 horas) (Presencial)	3	3
Foro internacional: Gestión de Riesgos para el cumplimiento del deber de seguridad	---	3
Total	**156**	**161**

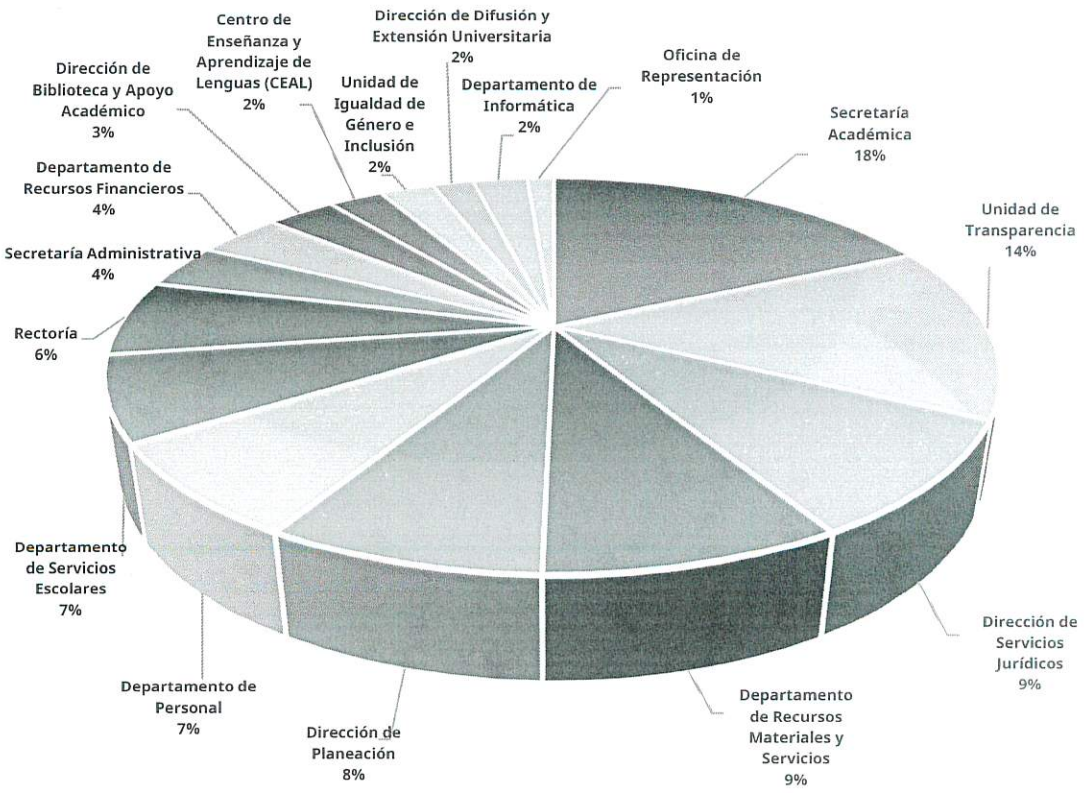
* Foro realizado fuera de la oferta ordinaria del INAI.

❖ PARTICIPACIONES POR ÁREA:

ÁREA DE ADSCRIPCIÓN	NÚMERO DE PARTICIPACIONES
Secretaría Académica	29
Unidad de Transparencia	23
Dirección de Servicios Jurídicos	15
Departamento de Recursos Materiales y Servicios	14
Dirección de Planeación	13
Departamento de Personal	12
Departamento de Servicios Escolares	11
Rectoría	10
Secretaría Administrativa	6
Departamento de Recursos Financieros	6
Dirección de Biblioteca y Apoyo Académico	5
Centro de Enseñanza y Aprendizaje de Lenguas (CEAL)	4
Unidad de Igualdad de Género e Inclusión	4

ÁREA DE ADSCRIPCIÓN	NÚMERO DE PARTICIPACIONES
Dirección de Difusión y Extensión Universitaria	3
Departamento de Informática	4
Oficina de Representación	2
TOTAL	**161**

CAPACITACIÓN POR ÁREA



❖ CAPACITACIÓN POR GÉNERO:

PARTICIPACIONES POR GÉNERO	
FEMENINO	**94 (58%)**
MASCULINO	**67 (42%)**

CAPACITACIÓN POR GÉNERO