DOCUMENTO DE SEGURIDAD PARA LA PROTECCIÓN DE DATOS PERSONALES

INSTITUTO POLITÉCNICO NACIONAL

CONTENIDO

I. INTRODUCCIÓN

La información es un activo que debe protegerse mediante un conjunto de procesos y sistemas diseñados, administrados y mantenidos por una organización, por lo que resulta necesario establecer, implementar, operar, monitorear y mejorar los procesos y sistemas relativos a la gestión de la seguridad de dicha información obteniendo con esto la total confidencialidad, resguardo integridad y disponibilidad de la misma.

El presente Documento de Seguridad, se elabora en cumplimiento a lo dispuesto por el artículo 35 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO), señalando el control interno relacionado con la obtención, uso, registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de datos personales que aplica el Instituto Politécnico Nacional (IPN).

II. OBJETIVO

El principal objetivo de este documento de seguridad es describir y dar cuenta de manera general sobre las medidas de seguridad de carácter, administrativo, físico y técnico para la protección de datos personales, adoptadas, por el IPN, con el fin de protegerlos contra el daño, perdida, alteración, destrucción, uso acceso divulgación y/o tratamiento no autorizado, así como garantizar su confidencialidad, integridad y disponibilidad de la información de los sistemas manejados por esta Casa de Estudios.

III. MARCO JURÍDICO

- Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados
- Ley General de Archivo
- Ley Federal de Procedimiento Administrativo
- Reglamento Orgánico del Instituto Politécnico Nacional
- Reglamento Interno del Instituto Politécnico Nacional
- Lineamientos de Protección de Datos Personales para el Sector Público
- ACUERDO por el que se emiten las políticas y disposiciones para impulsar el uso y aprovechamiento de la informática, el

gobierno digital, las tecnologías de la información y comunicación, y la seguridad de la información en la Administración Pública Federal.
- Política Institucional de Seguridad de la Información

IV. TÉRMINOS Y DEFINICIONES

Para los efectos del presente Documento se Seguridad para la Protección de Datos Personales, además de las definiciones contenidas en el artículo 3° de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, se entenderá por:

I. **Áreas:** Instancias de los sujetos obligados previstas en los respectivos reglamentos interiores, estatutos orgánicos o instrumentos equivalentes que cuentan o puedan contar, dar tratamiento, y ser responsables o encargadas se los datos personales.

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

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

IV. **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;

V. **Derechos ARCOP:** Los derechos de acceso, rectificación, cancelación, oposición y portabilidad al tratamiento de datos

personales;

VI. **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 de los datos personales que posee;

VII. **Encargado:** La persona física o jurídica, pública o privada, ajena a la organización del responsable, que sola o conjuntamente con otras trate datos personales a nombre y por cuenta del responsable;

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

IX. **Lineamientos Generales:** Lineamientos Generales de Protección de Datos Personales para el Sector Público;

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

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

XII. **Medidas de seguridad físicas:** conjunto de acciones y mecanismos para proteger el entorno físico de los datos personales y de los recursos involucrados en su tratamiento;

XIII. **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 y los recursos involucrados en su tratamiento;

XIV. **Responsable:** Los sujetos obligados a que se refiere el

artículo 1 de la Ley General, que deciden sobre el tratamiento de datos personales;

XV. **Titular:** La persona física a quien corresponde los datos personales;

XVI. **Transferencia:** Toda comunicación de datos personales dentro o fuera del territorio mexicano, realizada a persona distinta del titular, del responsable o del encargado;

XVII. **Tratamiento:** Cualquier acción o conjunto de acciones efectuadas mediante procedimientos manuales o automatizados aplicados a los datos personales, relacionadas con la obtención, uso registro, organización conservación, elaboración utilización, comunicación, difusión almacenamiento o disposición de datos personales.

PARTE 1.- INVENTARIO DE DATOS PERSONALES Y DE LOS SISTEMAS DE TRATAMIENTO

De acuerdo con los artículos 58 y 59 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público, se presenta en este apartado el inventario de datos personales, así como de los sistemas de tratamientos implementados por esta Casa de Estudios. En relación con lo previsto en el artículo 33, fracción III de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, el responsable (IPN) deberá elaborar un inventario con la información básica de cada tratamiento de datos personales considerando al menos, los siguiente:

INFORMACIÓN EN EL IPN

Con relación al ciclo de vida de los datos personales en el inventario de éstos, el Artículo 59 de los Lineamientos Generales, informa que, aunado a lo dispuesto en el artículo anterior, en la elaboración del inventario de datos personales el responsable deberá considerar el ciclo de vida de los datos personales conforme a 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.

Bajo ese contexto el IPN, informa que en todos los procedimientos, trámites y servicios etc. tanto del personal adscrito a esta Casa de Estudios como son el Personal de Apoyo y Asistencia a la Educación como el Personal Docente, Investigadores y Servidores Públicos de estructura es decir personal de mando medios y superiores, así como los correspondientes que realiza el alumnado inscrito a esta Institución Educativa, en ese sentido los datos personales que se recaban son los siguientes:

- **Datos Personales**
- **Datos sensibles**

Catálogo de medios físicos y electrónicos a través de los cuales se obtienen los datos personales

Medios electrónicos: formularios web correos institucionales de las Dependencias Politécnicas.

Medios físicos: oficialía de partes, control escolar, mediante llenado de formatos.

Finalidad de cada tratamiento de datos personales

Se realiza el procedimiento conforme a las facultades y funciones de cada Dependencia Politécnica conforme al Reglamento Orgánico del IPN, Reglamento Interno del IPN y en su caso el Reglamento interno de casa Unidad académica o

administrativa que compone este Sujeto Obligado.

Formatos de almacenamiento:

De manera física: los expedientes que se generan conforme a la Ley General de Archivo y el Catálogo de Disposición Documental, por lo que se tienen expedientes resguardados en archiveros con llave que a su vez resguardan las diversas dependencias que componen el IPN.

De manera electrónica: en los sistemas, correos electrónicos institucionales y la nube que se encuentran bajo las más estrictas medidas de seguridad por parte de la Coordinación General del Centro Nacional de Calculo en concordancia con las Direcciones dependientes de la misma, en ese sentido, se enlistan el inventario de los sistemas informáticos que se encuentran en el Instituto Politécnico Nacional:

Inventario de sistemas informáticos:

SISTEMAS CON LOS QUE CUENTA EL INSTITUTO POLITÉCNICO NACIONAL

Transferencia mediante el traslado de soporte físicos:

LA QUE REALIZA EL INSTITUTO POLITÉCNICO NACIONAL

Transferencia mediante el traslado en soportes electrónicos:

LA QUE REALIZA EL INSTITUTO POLITÉCNICO NACIONAL

Resguardo de sistemas de datos personales con soportes físicos:

Medidas de seguridad que se implementan para el resguardo de los soportes físicos del sistema de manera que evite la alteración, perdida o acceso no autorizado a los mismos.

Nombre del sistema	**SISTEMAS CON LOS QUE CUENTA EL INSTITUTO POLITÉCNICO NACIONAL**
Cargo de la persona responsable	INSTITUTO POLITÉCNICO NACIONAL
Funciones	FUNCIONES DE LOS SISTEMAS CON LOS QUE CUENTA EL INSTITUTO POLITÉCNICO NACIONAL
Objetivo (funcionalidad)	OBJETO DE LOS SISTEMAS CON LOS QUE CUENTA EL INSTITUTO POLITÉCNICO NACIONAL
¿Incluye aviso de privacidad?	Si
Datos personales recabados	DE CONFORMIDAD CON LA NORMATIVA EN MATERIA DE DATOS PERSONALES
Uso de los datos	USO DE DATOS DE LOS SISTEMAS CON LOS QUE CUENTA EL INSTITUTO POLITÉCNICO NACIONAL
Formato de almacenamiento	Electrónico
Descripción general de la ubicación física y/o electrónica de los datos personales	SISTEMAS CON LOS QUE CUENTA EL INSTITUTO POLITÉCNICO NACIONAL
Área solicitante	ÁREA REQUIRENTE
Tipo de usuario final	A QUIEN SE DIRIGE

El análisis de riesgos

Para dar cumplimiento al artículo 33, fracción IV de la Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados, el responsable deberá realizar un análisis de riesgos de los datos personales tratados considerando lo siguiente:

1. Los requerimientos regulatorios, códigos de conducta o mejores prácticas de un sector específico;
2. El valor de los datos personales de acuerdo a su clasificación previamente definida y su ciclo de vida;
3. El valor y exposición de los activos involucrados en el tratamiento de los datos personales;
4. Las consecuencias negativas para los titulares que pudieran derivar de una vulneración de seguridad ocurrida, y

Además de los factores previstos en el artículo 32 de la Ley General

I. El riesgo inherente a los datos personales tratados;
II. La sensibilidad de los datos personales tratados;
III. El desarrollo tecnológico;
IV. Las posibles consecuencias de una vulneración para los titulares;
V. Las transferencias de datos personales que se realicen;
VI. El número de titulares;
VII. Las vulneraciones previas ocurridas en los sistemas de tratamiento, y
VIII. El riesgo por el valor potencial cuantitativo o cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada para su posesión.

De ahí que, la realización del análisis de riesgo es fundamental para la gestión de proyectos, dado que es una herramienta que ayuda a prever los riesgos y amenazas a los que está sometido un proyecto para que de esta manera se puedan realizar planes de contingencia y reducir el posible impacto en los procesos del sistema. El análisis de riesgo puede emplearse para estimar cómo un riesgo particular podría afectar la finalización de un proyecto.

Para el IPN es importante la implementación de medidas de seguridad para la

protección de datos personales en todos sus sistemas desarrollados.

Hay que tener medidas de seguridad física las cuales son un conjunto de acciones y mecanismos para proteger el entorno físico de los datos personales y de los recursos involucrados en su tratamiento, previniendo el acceso no autorizado al perímetro de la organización y recursos e información. También, hay que proteger los recursos móviles, portátiles y cualquier soporte físico o electrónico, proveer a los equipos que contienen o almacenan datos personales de un mantenimiento eficaz que asegure su disponibilidad, integridad y funcionalidad.

El Instituto trabaja constantemente para evitar que las vulnerabilidades puedan convertirse en violaciones de seguridad a gran escala que puedan generar pérdidas de datos importantes.

Tipos de vulnerabilidad informática

Algunos tipos de vulnerabilidades típicas de sistemas y aplicaciones son:

- **COMPROMETEN LA SEGURIDAD DE LOS SISTEMAS**

Es recomendable realizar una serie de acciones para no poner en peligro los sistemas y aplicaciones, como:

- **ACCIONES QUE SE IMPLEMENTAN**

El análisis de brecha

Con relación al artículo 33, fracción V de la Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados, para la realización del análisis de brecha el responsable deberá considerar lo siguiente:

1. Las medidas de seguridad existentes y efectivas;
2. Las medidas de seguridad faltantes, y
3. La existencia de nuevas medidas de seguridad que pudieran remplazar a uno o más controles implementados actualmente.

Por lo cual, se deberá en caso de detectar la existencia de nuevas medidas de

seguridad que pudieran remplazar a uno o más controles implementados actualmente.

El análisis de brecha es de naturaleza diagnóstica y contribuye a conocer las áreas de oportunidad por cada tratamiento. A su vez, esta información da sustento a las políticas y mecanismos institucionales en materia de protección de datos personales que se han aprobado por el Comité de Transparencia para atenderlas de manera paulatina y en coordinación con cada una de las áreas.

Debido a la naturaleza sensible de los datos personales, es imperativo que los responsables del tratamiento de los mismos cuenten con principios como lealtad, calidad, responsabilidad y licitud. Tal y como se menciona en el apartado 2 de este documento, el responsable tendrá la obligación de informar a los titulares de los datos, la información que se recaba de ellos y con qué fines, a través de un documento llamado "Aviso de privacidad".

Este documento se vuelve la primera medida de prevención, ya que evita que se brinden datos innecesarios, así como también se mencionan el/los proceso(s) por el/los cual(es) se limitarán el uso o la divulgación de la información.

Por otro lado, las medidas de seguridad pueden aplicarse en diversos ámbitos, ya sea físico, técnico o administrativo.

Plan de trabajo

Para el cumplimiento de lo previsto en el artículo 33, fracción VIII de la Ley General de Protección de Datos Personales en posesión de Sujetos Obligados, 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, 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.

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.

Los mecanismos de monitoreo y revisión de las medidas de seguridad

Monitoreo y supervisión periódica de las medidas de seguridad implementadas artículo 63. Con relación al artículo 33, fracción VII de la Ley General de Protección de Datos Personas en Posesión de los Sujetos Obligados, 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.

Aunado a lo previsto en las fracciones anteriores del presente artículo, 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.