TLAXCALA
UNA NUEVA HISTORIA

UPTx

DOCUMENTO DE SEGURIDAD DE DATOS PERSONALES DE LA UNIVERSIDAD POLITÉCNICA DE TLAXCALA

ÍNDICE

- GLOSARIO

I. INTRODUCCIÓN

II. MARCO NORMATIVO

III. ÁMBITO DE APLICACIÓN Y OBSERVACIONES GENERALES

IV. INVENTARIO DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES DE LA UPTx, ASÍ COMO LA DESCRIPCIÓN DE FUNCIONES Y OBLIGACIONES DE LAS PERSONAS QUE TRATAN DATOS PERSONALES

V. MEDIDAS DE SEGURIDAD

VI. ANÁLISIS DE RIESGOS

VII. ANÁLISIS DE BRECHA

VIII. PLAN DE TRABAJO

IX. MEACANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD DE PROTECCIÓN DE DATOS PERSONALES

X. PROGRAMA GENERAL DE CAPACITACIÓN

GLOSARIO:

Área administrativa: son las unidades que conforman la estructura orgánica de la Universidad Politécnica de Tlaxcala, cuyos titulares fungen como responsables del tratamiento de los datos personales que se encuentran en posesión de dichas áreas.

Bases de datos: Conjunto de datos personales relativos a personas físicas identificadas e identificables, condicionado a criterios determinados con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización.

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

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

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.

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.

Medidas de seguridad: Conjunto de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permiten garantizar la protección, confidencialidad, disponibilidad e integridad de los datos personales.

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.

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.

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.

Nube: Modelo de provisión externa de servicios de cómputo bajo demanda que implica el suministro de infraestructura, plataforma o programa informático, distribuido de modo flexible, mediante procedimientos virtuales en recursos compartidos dinámicamente.

Respaldo de la información: Se refiere a la copia de la información que se genera, utiliza y actualiza a lo largo del tiempo, dicho término se emplea para referirse a las copias de seguridad que se llevan a cabo en los sistemas de información, bases de datos software de aplicación, sistemas operativos, entre otros. El respaldo tiene como objetivo garantizar la recuperación de la información en caso de que ésta haya sido eliminada, dañada o alterada.

Responsable: Sujetos obligados a que se refiere el artículo 1 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, que deciden sobre el tratamiento de datos personales.

Titular: Persona física a quien pertenecen los datos personales.

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

Usuarios: Persona autorizada por el responsable, y parte de la organización del sujeto obligado, que da tratamiento y/o tiene acceso a los datos y/o a los sistemas de datos personales.

I. INTRODUCCIÓN:

El artículo 6, apartado A, fracción II de la Constitución Política de los Estados Unidos Mexicanos prevé que toda la información que se refiere a la vida privada y los datos personales será protegida en los términos y con las excepciones que fijen las leyes.

El artículo 16, párrafo segundo dispone que toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley, la cual establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros.

En ese tenor, la Universidad Politécnica de Tlaxcala, tiene bajo su resguardo diversa información de carácter personal, tanto de alumnos, trabajadores, así como de personas externas, por lo que tiene el deber de salvaguardar dicha información y protegerla en los términos de la normatividad aplicables vigente en la materia.

A fin de dar cumplimiento a la obligación establecida en el artículo 35 de la Ley General de Protección de Datos Personales, se crea el presente documento de seguridad, el cual contiene las medidas de seguridad administrativa, física y técnica aplicables a los sistemas de tratamiento de datos personales de la Universidad Politécnica de Tlaxcala, con la finalidad de asegurar la integridad, confidencialidad y disponibilidad personal en estos contenidos.

El objetivo del presente documento es identificar los diversos sistemas de tratamientos de datos personales que posee esta Universidad, el tipo de datos personales que contiene cada uno, los responsables, encargados, usuarios de cada sistema y las medidas de seguridad implementadas.

II. MARCO NORMATIVO:

El presente documento de seguridad tiene fundamento en lo previsto en los artículos 6, inciso A, fracción II y 16, párrafo segundo de la Constitución Política de los Estados Unidos Mexicanos, 3, fracción XIV, 33, 34 y 35 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y 55 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público.

III. ÁMBITO DE APLICACIÓN Y OBSERVACIONES GENERALES:

Con fundamento en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, el presente documento es aplicable para todas las áreas administrativas de la Universidad Politécnica de Tlaxcala, que, en el ejercicio de sus atribuciones, facultades y funciones, administren bases de datos en sistemas de tratamiento de datos personales, ya sea que administren sistemas completos o el tramo de información que le corresponda.

Asimismo, serán aplicables al tratamiento de datos personales que obren en soportes físicos y/o electrónicos, con independencia de la forma o modalidad de su creación, procesamiento, almacenamiento y organización. Los datos personales pueden obrar en forma numérica, alfabética, gráfica, alfanumérica, fotográfica o en cualquier otro formato.

Los servidores públicos de la UPTx, que tengan acceso a los datos personales están obligados a conocer y aplicar las medidas de seguridad propias de cada sistema en el que se concentren los datos y es aplicable en todas y cada una de las fases del tratamiento de los mismo, partiendo desde la obtención y concluyendo con su eliminación. Cabe señalar que, la obligación de confidencialidad debe subsistir aún después de que los involucrados hayan finalizado su participación en el tratamiento de los datos personales, porque hayan cambiado de funciones e inclusive cuando la relación laboral con la Universidad haya concluido.

Además de las funciones y obligaciones de los servidores públicos adscritos a la UPTx involucrados, establecidas en el análisis de cada uno de los sistemas, de manera general, deberán observar lo siguiente:

- Tratar los datos personales con responsabilidad y las medidas de seguridad que haya establecido para tal fin;
- Observar el deber de confidencialidad sobre la información que conozcan en el desarrollo de sus actividades;
- Dar aviso al superior jerárquico inmediato de cualquier acción que pueda vulnerar o poner en riesgo la seguridad de los datos personales.

El incumplimiento a lo establecido en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, los Lineamientos Generales de Protección de Datos Personales para el Sector Público, así como en el presente documento de deguridad, será causa de la aplicación de medias de apremio y/o sanciones correspondientes en los términos de dicha normatividad.

IV. INVENTARIO DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES DE LA UNIVERSIDAD POLITÉCNICA DE TLAXCALA, ASÍ COMO LA DESCRIPCIÓN DE FUNCIONES Y OBLIGACIONES DE LAS PERSONAS QUE TRATAN DATOS PERSONALES:

En la Universidad Politécnica de Tlaxcala, el manejo y tratamiento de la información se considera por áreas específicas donde se proporciona cada servicio. Existe personal designado como responsable de la administración de los datos y los sistemas que se manejan; este personal se encarga de realizar el inventario de los datos personales y de los sistemas para su tratamiento.

El tipo de información que recaba la Universidad Politécnica de Tlaxcala, engloba tres categorías de datos personales tratados, considerados como de identificación, patrimoniales y sensibles, a continuación, se enlistan de manera enunciativa, mas no limitativa:

- **Identificación**: Nombre, domicilio, C.U.R.P., fotografía, huella digital, firma autógrafa y electrónica, edad, estado civil, R.F.C., sexo, correo electrónico personal, teléfono, información académica y escolar, número de cuenta escolar, fecha y lugar de nacimiento, cédula profesional, nacionalidad, numero de seguridad social.

- **Patrimoniales**: Cuentas bancarias, estado de cuentas bancarias, número de tarjeta bancaria, CLABE interbancaria, institución bancaria, estados financieros, saldos, propiedades, primas de seguro.

- **Sensibles:** Datos relativos al estado de salud física y mental, tipo de sangre, orientación sexual, religión, datos socioeconómicos.

Los sistemas de datos personales que se mencionan en el presente documento son el conjunto organizado de archivos, registros, ficheros, bases o banco de datos personales en posesión de la UPTx, cualquiera sea la forma o modalidad de su creación, almacenamiento, organización y acceso.

V. MEDIDAS DE SEGURIDAD

De conformidad con lo dispuesto en el artículo 31 de la Ley General, los responsables del tratamiento de datos personales deben adoptar y mantener medidas de seguridad de carácter administrativo, físico y técnico que los protejan en contra de daños, pérdida, alteración, destrucción o que sean usados, tratados o divulgados a terceros sin la autorización correspondiente, como se aprecia de la siguiente lectura:

> Artículo 31. Con independencia del tipo de sistema en el que se encuentren los datos personales o el tipo de tratamiento que se efectúe, el responsable deberá establecer y mantener las 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.

Esto se complementa con lo previsto en los artículos 32, 33 y 34 de la Ley General; por tanto, se deben establecer medidas de carácter administrativo, físico y técnico.

Se entiende por **medidas de seguridad administrativas** las acciones realizadas por el responsable encaminadas a proteger los datos personales. Es decir, son las políticas o los procedimientos establecidos para la adecuada obtención, tratamiento, bloqueo y supresión de datos personales. Entre estas medidas se encuentra la confidencialidad obligatoria por parte de los responsables del tratamiento de datos personales, inclusive después de haber concluido la relación laboral, institucional o jurídica con la UPTx.

Las **medidas de seguridad físicas** son las destinadas a resguardar el área o perímetro que delimita la ubicación de las bases de datos; es decir, los instrumentos utilizados para proteger el lugar donde se ubican los datos personales.

Las **medidas de seguridad técnicas** son los instrumentos electrónicos utilizados para el tratamiento de datos personales. Se componen de hardware y software. Son medidas de seguridad técnicas la tecnología utilizada para proteger el entorno digital de los datos personales y los recursos físicos (computadoras, laptops, etc.) empleados para su desarrollo y tratamiento.

Medidas de seguridad administrativas

En la Universidad Politécnica de Tlaxcala, se han implementado las siguientes medidas de seguridad administrativas:

Por conducto de la persona titular de la Dirección de Transparencia, se han creado los Lineamientos Internos para la Protección de Datos Personales.

De igual manera, es responsable de la elaboración de Avisos de Privacidad y apoya a las áreas en las dudas que surgen en el tratamiento de los datos personales.

Se cuenta con convenio de confidencialidad con las personas responsables del tratamiento de datos personales, con el objetivo de garantizar el derecho a que los mismos sean tratados con estricto apego a la Ley de Protección de Datos Personales, es decir, a que éstos no se difundan o compartan con terceros, salvo que exista consentimiento para ello o alguna disposición normativa requiera su difusión.

Medidas de seguridad físicas

Para prevenir el acceso no autorizado a las instalaciones de la UPTx, a sus áreas físicas y las bases de datos en ellas contenidas.

El acceso a la institución es restringido al personal, y en caso de personas externas, se cuenta con un riguroso registro de entradas y salidas encomendado mediante servicios de seguridad y vigilancia ajenos al personal de la UPTx, para acreditar criterios de imparcialidad.

Los servicios de seguridad, tienen por objeto la vigilancia y la protección de los bienes y las personas que ingresan a las instalaciones o inmuebles de la Universidad. Tienen capacidad de respuesta a cuestiones de prevención, contención y, de ser el caso, de auxilio a las unidades administrativas que lo soliciten. Sus elementos resguardan las áreas donde se encuentran las bases de datos electrónicas y físicas; resguardan las instalaciones 24 horas al día los 365 días al año.

Prevención de daños a equipos electrónicos

La atención de equipos electrónicos de la UPTX, está a cargo de personal especializado del área de informática. De este modo, se protege de daño o menoscabo la información que se resguarda en las computadoras. Además, existe un programa de mantenimiento de los equipos electrónicos para preservarlos y asegurar que sigan funcionando correctamente, lo que permite lograr también otros objetivos, como la portabilidad de los datos personales.

Medidas de seguridad técnicas

Para prevenir el acceso no autorizado y privilegios de terceros a los equipos de cómputo de la UPTx.

Todos los equipos de cómputo de la UPTx cuentan con contraseñas: para utilizar o ingresar a ellos es necesario registrar al usuario y su contraseña personalísima. Cada servidor público debe generar su contraseña y resguardarla debidamente, con la finalidad de evitar que terceros ingresen a su equipo de cómputo y realicen un tratamiento inadecuado de datos personales.

Para prevenir el acceso de terceros externos a los equipos de cómputo o a las redes electrónicas de la UPTx.

A cargo del departamento de Informática, se cuenta con equipo de seguridad perimetral (Firewall) que controla el tráfico entrante y saliente.

Además, se tiene equipo de prevención de intrusos (IPS) que inspecciona el tráfico para detectar y bloquear patrones de ataque y trafico sospechoso. Cuenta con equipo de filtrado de contenidos web para evitar que los usuarios visiten sitios que puedan comprometer la información de la UPTx.

En todos los equipos se bloquea el acceso a sitios de suplantación de identidad y opera un mecanismo antivirus que los protege de correos potencialmente peligrosos.

VI. ANÁLISIS DE RIESGOS

Riesgo: Es la exposición a diferentes amenazas y la probabilidad de que se materialice en una de ellas. Las amenazas consisten en eventos, acciones u omisiones que puedan materializarse en una vulneración a la privacidad del titular, en un impacto al tratamiento de datos personales y en un incumplimiento a las disposiciones legales en la materia.

De conformidad con el artículo 33, fracción IV, de la Ley General, el análisis de riesgo debe ser elaborado considerando las amenazas y vulnerabilidades existentes para los datos personales que son recabados y los recursos involucrados en su tratamiento, como pueden ser, de manera enunciativa más no limitativa, el tipo de hardware, software, o las características del responsable, entre otros.

De acuerdo con lo estipulado en el artículo 60 de los Lineamientos Generales, en la realización del análisis de riesgo se deberá considerar lo siguiente:

- La existencia de requerimientos regulatorios, códigos de conducta o mejores prácticas de un sector específico para proteger los datos personales.
- El valor de los datos personales de acuerdo con su clasificación previamente definida, y su ciclo de vida, de conformidad con la normatividad aplicable.
- El valor y exposición de los activos involucrados en su tratamiento.
- Las consecuencias negativas para las personas titulares que pudieran derivar de una vulneración de seguridad ocurrida.
- El riesgo inherente a los datos personales tratados, su sensibilidad (datos personales sensibles), el desarrollo tecnológico, las posibles consecuencias de una vulneración para las personas titulares, las transferencias de datos personales que se realicen, el número de personas titulares, las vulneraciones previas ocurridas en los sistemas de tratamiento, y 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; siempre en función y estricto apego a la normatividad aplicable.

En consecuencia, las áreas responsables del tratamiento de datos personales, deben analizar el riego existente en cada uno de éstos, describiendo sus conclusiones a través de la justificación de los aspectos siguientes:

❖ Información general

a. La identificación de los datos personales que se obtienen o reciben.
b. Motivo por el cual se recaban o reciben los datos personales.

❖ **Finalidades del tratamiento**

a. La denominación del tratamiento de datos personales que realiza y la forma en que se opera, detallando el fundamento legal y normativo aplicable al tratamiento.
b. La categoría correspondiente a los datos personales tratados, es decir, si se ejerce sobre datos de carácter identificativo, de características personales, circunstancias sociales, datos académicos y profesionales, detalles del empleo, de información comercial, datos económicos o financieros y de seguro.
c. La duración del tratamiento que realiza, es decir, si es instantáneo, o si tiene un periodo de duración.
d. Si la obtención de los datos tiene como finalidad la supervisión o evaluación sistemática y exhaustiva de aspectos personales, como son, aquellos a través de los cuales se pueden determinar hábitos, comportamientos, preferencias, gustos, intereses, etc., de personas identificadas o identificables.
e. Si la obtención de los datos tiene como finalidad el tratamiento de datos personales sensibles.
f. Si la finalidad del tratamiento pudiera cumplirse recabando un menor número de datos personales.
g. Si la finalidad del tratamiento implica el uso específico de datos de personas con discapacidad o cualquier otro colectivo en situación de especial vulnerabilidad.
h. Si el tratamiento de los datos personales tiene la finalidad de elaborar documentos, perfiles o es utilizado para la toma de decisiones.
i. Si el número de personas servidoras públicas involucradas en el tratamiento de datos personales resulta insuficiente, suficiente o excesivo.
j. Identificar si personas servidoras públicas adscritas a otras áreas se encuentran involucradas en el tratamiento de datos personales.

❖ **Tecnologías empleadas para el tratamiento**

a. La tecnología implementada en el tratamiento de datos personales, describiendo el nombre y el modo de empleo.

❖ **Transferencia de datos personales**

a. Si en el tratamiento de datos personales se realiza una transferencia de datos, destacando la normatividad correspondiente y el instrumento legal en el que se convino dicha transferencia.

b. Si en el tratamiento de datos personales se realiza una transferencia de datos a entidades internacionales, señalando la normatividad correspondiente, el nombre y país de la entidad internacional y describiendo el instrumento legal en el que se convino dicha transferencia.

❖ **Esquema de niveles de riesgo**

- Los datos personales tratados por las áreas, se consideran de un alto valor social, debido a que su uso deriva de la función constitucional que es otorgada a la UPTx y del cumplimiento de las atribuciones que le son concedidas por la ley.
- Las etapas del ciclo de vida de los datos personales se encuentran definidas en Ley de Archivo y de más normatividad aplicable en la materia.
- Los activos involucrados resultan ser aquellos indispensables para que las áreas cumplan con la finalidad del tratamiento, misma que en todo momento estará fundada y motivada por un marco legal y normativo; entre los que se encuentran:

  ✓ El soporte documental o electrónico mediante el cual se evidencia el tratamiento.
  ✓ Los procesos internos llevados a cabo para la realización del tratamiento.
  ✓ Las personas servidoras públicas asignadas para efectuar el tratamiento.
  ✓ El soporte técnico implementado para el funcionamiento de los elementos de hardware y software asignados para el tratamiento.

VII. ANÁLISIS DE BRECHA

¿Qué controles y medidas deben ser implementadas para la protección de los datos personales?

El artículo 33, fracción V, de la Ley General, estipula que para establecer y mantener las medidas de seguridad para la protección de los datos personales es necesaria la elaboración de un análisis de brecha en el que se comparen las medidas de seguridad existentes contra las faltantes.

EL artículo 61 de los Lineamientos Generales, dispone que en la realización del análisis de brecha se debe considerar lo siguiente:

✓ Las medidas de seguridad existentes y efectivas.
✓ Las medidas de seguridad faltantes.
✓ La existencia de nuevas medidas de seguridad que pudieran remplazar a uno o más controles implementados actualmente.

Una vez identificados los riesgos y medidas de seguridad, es procedente el análisis de brecha, en el que se identifiquen los controles que deben ser implementados.

En síntesis, ante la percepción de la existencia de un riesgo, las áreas competentes deben analizar las brechas atendibles justificando los aspectos siguientes:

- Si los controles de seguridad implementados han resultado efectivos para garantizar la seguridad de los datos personales.

- Si después del análisis de los controles de seguridad, se considera que el tratamiento de datos personales puede conllevar una pérdida o alteración de la información.
- Si los controles y medidas de seguridad existentes para la obtención, tratamiento, resguardo y archivo de los datos personales cumplen su objetivo de manera efectiva.
- Los riesgos que se consideran pueden afectar los controles y medidas de seguridad implementadas en el tratamiento de datos personales.
- La forma en la que se estima que los riesgos señalados pueden reducirse a futuro.

VIII. PLAN DE TRABAJO

OBJETIVO: implementar las medidas de seguridad recomendadas para los tratamientos de datos personales

La Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados en sus artículos 33 fracción VI, establece la obligación para los responsables del tratamiento de elaborar un plan de trabajo, para la implementación de las medidas de seguridad y tratamiento de datos personales.

Acciones:

1. Eliminar las brechas a través de la implementación de medidas de seguridad en cada uno de los tratamientos de datos personales identificados; y,

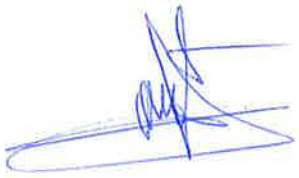
2. Consolidar y preservar los niveles de protección de los datos personales a través de mecanismos de monitoreo y revisión.

IX. MEACANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD DE PROTECCIÓN DE DATOS PERSONALES

Para establecer y mantener la seguridad de los datos personales, el artículo 33 fracción VII de la Ley General, establece que se deben monitorear de manera periódica las medidas de seguridad implementadas, así como las amenazas y vulneraciones a las que están sujetos los datos personales.

X. PROGRAMA GENERAL DE CAPACITACIÓN

El artículo 33, fracción VIII, de la Ley General dispone que, para establecer y mantener las medidas de seguridad para la protección de los datos personales, se deberá promover la de capacitación del personal que maneja tratamiento de datos personales.

Responsable del Desarrollo	Mtra. Silvia Salome Hernández Loaiza Titular de la Dirección de Transparencia Silviasalome.hernandez@uptx.edu.mx	
Revisó	C.P. Hilario Nicéforo Pérez García Secretario Administrativo hilarioniceforo.perez@uptlax.edu.mx	
Autorizó	Mtra. y Dra.H.C. Rosalía Nalleli Pérez Estrada Rectora de la Universidad Politécnica de Tlaxcala rectoria@uptlax.edu.mx	
Fecha de aprobación: 11/03/2024		