POLÍTICAS DE SEGURIDAD EN LOS SISTEMAS DE DATOS PERSONALES DE LA ADMINISTRACIÓN DEL SISTEMA PORTUARIO NACIONAL TUXPAN, S.A DE C.V. 2022-2025

ÍNDICE

I. INTRODUCCIÓN.

En cumplimiento a lo que establecen los artículos 33 y 35, ambos de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, y con el objeto de establecer y mantener las medidas de seguridad para la protección de los Sistemas de Datos Personales, las Unidades Administrativas de la ASIPONA TUXPAN, deberán definir las funciones y obligaciones del personal involucrado en el tratamiento de datos personales; elaborar un inventario de los Sistemas de Datos Personales y de los sistemas de tratamiento; realizar un análisis de riesgos de los datos personales, considerando las amenazas y vulnerabilidades existentes para los datos personales y los recursos involucrados en su tratamiento; realizar un análisis de brecha; elaborar un plan de trabajo para la implementación de las medidas de seguridad faltantes; así como 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.

Es así que, se emite las presentes Políticas sobre el manejo de la Seguridad en los Sistemas de Datos Personales del Administración del Sistema Portuario Nacional Tuxpan, S.A de C.V., en apego a lo dispuesto por los artículos 33, 34, 35 y 36 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, cuya observancia es general y obligatoria para las Unidades Administrativas de la ASIPONA TUXPAN y los servidores públicos adscritos a las mismas, para establecer criterios, procedimientos institucionales y responsabilidades de los servidores públicos, a efecto de garantizar el derecho de acceso a la información pública que posee la ASIPONA TUXPAN, de conformidad con la Ley General de Transparencia y Acceso a la Información Pública, Ley Federal de Transparencia y Acceso a la Información Pública, Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, y demás disposiciones legales y normativas aplicables.

Las presentes Políticas y sus anexos, son un instrumento necesario para establecer y mantener las medidas de seguridad de carácter administrativo, físico y técnico para la protección de los Sistemas de datos personales, que permitan protegerlos contra daño, pérdida, alteración, destrucción o uso, acceso o tratamiento no autorizado, así como garantizar su confidencialidad, integridad y disponibilidad.

II. MARCO JURÍDICO.

a) Constitución Política de los Estados Unidos Mexicanos.

b) Leyes:

b.1. Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, y

b.2. Ley General de Transparencia y Acceso a la Información Pública.

III. OBJETO.

Las presentes Políticas tiene por objeto, acordar y divulgar los estándares, procedimientos, medidas de seguridad de carácter administrativos, físicos y técnicos, y los niveles de seguridad que se aplican para la seguridad de los Sistemas de Datos Personales en el ASIPONA TUXPAN; así como los mecanismos y medidas de control que deberá emplear el personal del ASIPONA TUXPAN responsable, los usuarios y encargados de la Administración de los Sistemas de Datos Personales, de conformidad con las presentes Políticas y las normas establecidas para el efecto.

IV. ÁMBITO DE APLICACIÓN.

El presente documento será de aplicación obligatoria a las y los servidores públicos de la ASIPONA TUXPAN responsables de la Administración de los Sistemas de Datos que contienen datos de carácter personal, así como a las personas externas cuyos servicios contratados por la ASIPONA TUXPAN, estén relacionados con el uso de dichos sistemas.

Todo el personal de la ASIPONA TUXPAN que tengan acceso a los datos personales, está obligado 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 datos personales, iniciando desde la obtención de los mismos y finalizando con su cancelación en los Sistemas.

V. DISPOSICIONES GENERALES.

5.1 NIVELES DE SEGURIDAD.

Los niveles de seguridad, se identificarán por cada responsable de la Administración de los Sistema de Datos que contienen datos de carácter personal.

Los niveles de seguridad responden a la mayor o menor necesidad de garantizar la integridad de los datos personales. Por lo tanto, las Unidades o Áreas Administrativas y sus Responsables aplicarán el nivel básico, medio o alto de medidas de seguridad.

Aunado a lo anterior, para determinar el nivel de riesgo se considera el criterio del riesgo inherente del dato personal, así como el nivel se seguridad requerido para éste, en adición a las vulnerabilidades y amenazas, de acuerdo con las categorías o tipos de datos personales que se detallan a continuación:

CRITERIOS DEL NIVEL DE RIESGO	
Riesgo Inherente Básico	**Nivel de Seguridad Básico**
Riesgo Inherente Medio	**Nivel de Seguridad Medio**
Riesgo Inherente Alto	**Nivel de Seguridad Alto**

A. NIVEL BÁSICO.

Las medidas de seguridad marcadas con nivel básico serán aplicables a todos los Sistemas de Datos Personales.

Se considerarán aplicables las medidas de seguridad de NIVEL BÁSICO a los Sistemas de Datos Personales que contengan algunos datos que enseguida se mencionan:

a.1. IDENTIFICACIÓN: Nombre, domicilio, correo electrónico, número de teléfono; RFC, CURP, cartilla militar, estado civil, firma, firma electrónica, lugar de nacimiento, fecha de nacimiento, nacionalidad, edad, nombres de familiares, dependientes, beneficiarios, fotografía, idioma o lengua, entre otros.

B. NIVEL MEDIO.

Los Sistemas de Datos Personales que contengan alguno de los datos que se enlistan a continuación, además de cumplir con las medidas de seguridad de nivel básico deberán observar las marcadas con nivel medio.

b.1. DATOS PATRIMONIALES: Bienes muebles e inmuebles, información fiscal, historial crediticio, ingresos y egresos, cuentas bancarias, seguros, afores, fianzas, servicios contratados, referencias personales, entre otros.

b.2 DATOS SOBRE PROCEDIMIENTOS ADMINISTRATIVOS SEGUIDOS EN FORMA DE JUICIO Y/O JURISDICCIONALES: Información relativa a una persona que se encuentre sujeta a un procedimiento administrativo seguido en forma de juicio o jurisdiccional en materia laboral, civil, penal o administrativa.

b.3 DATOS ACADÉMICOS: Trayectoria educativa, títulos, cédula profesional, certificados y reconocimientos, entre otros.

b.4 DATOS DE TRÁNSITO Y MOVIMIENTOS MIGRATORIOS: Información relativa al tránsito de las personas dentro y fuera del país e información migratoria de las personas, entre otros.

C. NIVEL ALTO.

Los Sistemas de Datos Personales que contengan alguno de los datos personales sensibles que se enlistan a continuación, además de cumplir con las medidas de seguridad de nivel básico y medio, deberán tomar las marcadas con nivel alto.

c.1 DATOS IDEOLÓGICOS: Creencia religiosa, ideológica, afiliación, política y/o sindical, pertenencia a organizaciones de la sociedad civil y/o asociaciones religiosas, entre otros.

c.2 DATOS DE SALUD: Estado de salud, historial clínico, alergias, enfermedades, información relacionada con cuestiones de carácter psicológico y/o psiquiátrico, incapacidades médicas, intervenciones quirúrgicas, vacunas, consumo de sustancias tóxicas, uso de aparatos oftalmológicos, ortopédicos, auditivos, prótesis, entre otros.

c.3 CARACTERÍSTICAS PERSONALES: Tipo de sangre, ADN, huella digital, u otros análogos.

c.4 CARACTERÍSTICAS FÍSICAS: Color de piel, color de iris, color de cabello, señas particulares, estatura, peso, complexión, discapacidades, entre otros.

c.5 VIDA SEXUAL: Preferencia sexual, hábitos sexuales, entre otros.

C.6 ORIGEN: Étnico o racial.

VI. ESPECIFICACIONES TÉCNICAS.

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

Para establecer y mantener las medidas de seguridad para la protección de los datos personales, las Unidades o Áreas Administrativas de la ASIPONA TUXPAN deberán elaborar un Inventario de los Sistemas de Datos Personales y de los Sistemas de Tratamiento.

INVENTARIO DE DATOS PERSONALES Y DE LOS SISTEMAS DE TRATAMIENTO art. 33 fracc. III y 35 de la LGPDP							
Unidad administrativa	**Nombre del Sistema**	**Responsable del Sistema**		**Tipo de datos Personales**	**Nivel de seguridad**	**Uso que se le da al sistema**	**Objeto del Sistema**
		Nombre	**Cargo**				

6.2 FUNCIONES Y OBLIGACIONES DE LAS PERSONAS QUE TRATEN DATOS PERSONALES.

Para establecer y mantener las medidas de seguridad para la protección de los Sistemas de Datos Personales, las Unidades o Áreas Administrativas de la ASIPONA TUXPAN deberán definir las funciones y obligaciones del personal involucrado en el tratamiento de datos personales.

LEY GENERAL DE ´PROTECCION DE DATOS PERSONALES EN POSESION DE SUJETOS OBLIGADOS art. 35, fracc. II					
Unidad administrativa	**Responsable del Sistema**	**Cargo**	**Nombre del Sistema de Tratamiento de Datos Personales**	**Funciones**	**Obligaciones**

6.3 MATRIZ DE RIESGOS Y ANÁLISIS DE BRECHA.

Con el objeto de establecer y mantener las medidas de seguridad para la protección de los Sistemas de Datos Personales, las Unidades o Áreas Administrativas de la ASIPONA TUXPAN deberán realizar un análisis de riesgo de los datos personales, y un análisis de brecha comparando las medidas de seguridad existentes contra las faltantes de cada uno de los Sistemas de 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.

Formato de Matriz de Riesgos y Análisis de Brecha que deberán requisitar todas las Unidades o Áreas Administrativas que mantienen y operan Sistemas de Datos Personales. (Anexo 3)

6.4 PLAN DE TRABAJO.

Formato del Plan de Trabajo que deberán requisitar todas las Unidades o Áreas Administrativas que mantienen y operan Sistemas de Datos Personales.

Conforme al análisis de brecha, existen algunas medidas de seguridad que se requieren y que aún no han sido definidas e implementadas, por lo que a continuación se presentan las actividades que se planean llevar a cabo para cada una de estas:

LEY GENERAL DE PROTECCION DE DATOS PERSONALES EN POSESION DE SUJETOS OBLIGADOS art. 33, fracc. IV y 35, fracc. V de la LGPDP	
PLAN DE TRABAJO	
Medias de seguridad Faltantes	**Actividad por desarrollar**

6.5 MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD.

En cumplimiento a lo que establecen los artículos 33, fracción VII y 35, fracción VI de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, y con el objeto de establecer y mantener las medidas de seguridad para la protección de los Sistemas de Datos Personales, las Unidades o Áreas Administrativas de la ASIPONA TUXPAN deberán 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 este contexto, es importante señalar la diferencia entre un soporte físico y un soporte electrónico, debido a que las medias de seguridad que el Titular de la Unidad Administrativa o Área responsable implemente para cada Sistema de Datos Personales, están estrechamente relacionadas con el tipo de soportes utilizados.

- **Soportes electrónicos:** Medios de almacenamiento inteligibles sólo mediante el uso de algún aparato con circuitos electrónicos que procese su contenido para examinar, modificar o almacenar los datos; es decir, cintas magnéticas de audio, video y datos, fichas de microfilm, discos ópticos (CDs y DVDs.), discos magnético-ópticos, discos magnéticos (flexibles y duros) y demás medios de almacenamiento masivo no volátil.
- **Soportes físicos**: Medios de almacenamiento inteligibles a simple vista, es decir, que no requieran de ningún aparato que procese su contenido para examinar, modificar o almacenar los datos; es decir, formularios impresos llenados "a mano" o "a máquina", fotografías y placas radiológicas, entre otros.

Con independencia del tipo de sistema en el que se encuentren los Datos Personales o el tipo de tratamiento que se efectúe, el personal titular de la Unidad Administrativa o Área responsable deberá establecer y mantener las medidas de seguridad de carácter administrativo, físico y técnico; en estas últimas, coadyuvando para tal efecto con área de Informática 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.

Las acciones relacionadas con las medidas de seguridad para el tratamiento de los datos personales que implementen las Unidades y Áreas Administrativas responsables de Sistemas de Datos Personales deberán estar documentadas y contenidas en el Sistema de que se trate, en términos de lo dispuesto por la Ley General de Protección de Datos en Posesión de Sujetos Obligados, y demás disposiciones administrativas aplicables.

6.6. DIVULGACIÓN DE INCIDENTES

En caso de que ocurra una vulneración de seguridad, el personal responsable deberá analizar las causas por las cuales se presentó e implementará en su plan de trabajo las acciones preventivas y correctivas para adecuar las medidas de seguridad y el tratamiento de los datos personales si fuese el caso a efecto de evitar que la vulneración se repita.

Se considerarán como vulneraciones de seguridad, en cualquier fase del tratamiento de datos, al menos, las siguientes:

I. La pérdida o destrucción no autorizada;
II. El robo, extravío o copia no autorizada;
III. El uso, acceso o tratamiento no autorizado, o
IV. El daño, la alteración o modificación no autorizada.

El personal responsable deberá llevar una bitácora de las vulneraciones de seguridad en la que se describa ésta, la fecha en la que ocurrió, el motivo de ésta y las acciones correctivas implementadas de forma inmediata y definitiva.

El personal responsable deberá informar por los medios de comunicación más inmediatos y sin dilación alguna al titular de los datos personales, y según corresponda, al INAI, las vulneraciones de seguridad que afecten de forma significativa los derechos patrimoniales o morales, en cuanto se confirme que ocurrió la vulneración y que el responsable haya empezado a tomar las acciones encaminadas a detonar un proceso de revisión exhaustiva de la magnitud de la afectación, a fin de que los titulares afectados puedan tomar las medidas correspondientes para la defensa de sus derechos.

El personal responsable deberá informar al titular de los datos personales al menos lo siguiente:

I. La naturaleza del incidente;
II. Los datos personales comprometidos;
III. Las recomendaciones al titular acerca de las medidas que éste pueda adoptar para proteger sus intereses;
IV. Las acciones correctivas realizadas de forma inmediata, y V. Los medios donde puede obtener más información al respecto.

En caso de robo o extravío de datos personales en soportes físicos y/o electrónicos, el personal responsable del o los Sistemas de Datos Personales que corresponda, al tener conocimiento del incidente, dará vista al Órgano Interno de Control para que en uso de facultades presenten en sus respectivas competencias, denuncia o querella en términos a los reglamentos administrativos y legales de acuerdo a sus atribuciones, o determinen lo conducente.

El personal responsable deberá establecer controles o mecanismos que tengan por objeto que todas aquellas personas que intervengan en cualquier fase del tratamiento de los datos personales, guarden confidencialidad respecto de éstos, obligación que subsistirá aún después de finalizar sus relaciones con el mismo.

6.6.2 SUPERVISIÓN.

De conformidad a lo establecido en el artículo 84, fracción V de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, el Comité de Transparencia supervisará periódicamente en coordinación con las unidades administrativas competentes, el cumplimiento a las medidas previstas en el presente documento.

6.6.3 CANCELACIÓN DE DATOS PERSONALES.

Para proceder a la baja o destrucción documental de soportes físicos que contienen datos personales, se observarán las disposiciones en materia de archivos que emita la Administración del Sistema Portuario Nacional Tuxpan.

El personal encargado llevará una bitácora donde registrará la baja de soportes electrónicos que contienen datos personales la cual deberá contener:

- Nombre y firma de la persona que realiza la acción;
- Fecha y hora en que se realiza;
- El destino que se le dará al soporte electrónico desechado;
- Nombre y firma del responsable y del titular del Área Administrativa correspondiente.