ALTAMIRA

ADMINISTRACIÓN DEL SISTEMA PORTUARIO NACIONAL

MARINA

DOCUMENTO DE SEGURIDAD

Para el Tratamiento de Datos Personales.

CONTROL DE CAMBIOS

Aprobación	Versión	Descripción del Cambio
2025	01	Emisión inicial

COMITÉ DE TRANSPARENCIA

L.C.P. Claudia Judith Martínez Padrón

Titular de la Unidad de Transparencia

Lic. Valeria Navarrete Muñoz

Suplente del Órgano Interno de Control.

Ing. Jesús Ernesto Lajas Aguilar.

Responsable del Área Coordinadora de Archivo.

ÍNDICE

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.

VII. El programa general de capacitación.

VIII. Glosario

INTRODUCCIÓN

La Administración del Sistema Portuario Nacional Altamira, S.A. de C.V. (ASIPONA ALTAMIRA), con fundamento en lo que dispone la **Ley General de Protección de Datos Personales en posesión de los sujetos Obligados,** en su carácter de **sujeto obligado**, cumple y observa los principios de **licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad** en el tratamiento de los datos personales, establecidos en el artículo 10 de dicho ordenamiento legal.

Los principios rectores constituyen **criterios fundamentales y obligatorios** que guían la actuación del personal responsable del tratamiento de datos personales, asegurando que dicho tratamiento se realice con estricto apego a la normatividad aplicable, protegiendo los derechos de las personas titulares.

1. PRINCIPIO DE LICITUD.
El tratamiento de los datos personales debe realizarse únicamente cuando se encuentre **fundado en atribuciones o facultades previstas en la normativa aplicable le confiera**, garantizando que las operaciones de recolección, registro, uso, almacenamiento, transferencia o supresión se ejecuten conforme a derecho.

El personal responsable debe verificar que toda actividad de tratamiento tenga un **fundamento jurídico claro, válido y vigente**.

2. PRINCIPIO DE FINALIDAD.
Los datos personales deben recabarse y tratarse **exclusivamente para finalidades concretas, lícitas, explícitas y legítimas**, las cuales deberán estar directamente relacionados con las atribuciones y obligaciones de la Entidad.

Esta finalidad debe hacerse del conocimiento de la persona titular mediante el **aviso de privacidad**, y todo tratamiento debe responder a un propósito institucional claramente determinado.

3. PRINCIPIO DE LEALTAD.
El tratamiento debe realizarse **de manera honesta, transparente y respetuosa**, absteniéndose de obtener datos personales mediante **engaños, fraudes o prácticas desleales**.

El responsable debe garantizar que las personas titulares conserven una **expectativa razonable de privacidad** y que la información sea tratada con integridad.

4. PRINCIPIO DE CONSENTIMIENTO
Como regla general, el tratamiento de los datos personales requiere el **consentimiento previo** de la persona titular, el cual debe ser:

- **Libre:** sin presiones, engaños o dolo.
- **Específico:** referido a finalidades determinadas.
- **Informado:** otorgado con pleno conocimiento del aviso de privacidad.

El consentimiento podrá ser **expreso o tácito**, conforme a la Ley, para datos personales sensibles se requiere consentimiento **expreso y por escrito**, se entenderá que es expreso, cuando la persona titular se manifieste verbalmente, por escrito, o por medios electrónicos, ópticos, signos inequívocos o por cualquier otra tecnología, mientras que el consentimiento será tácito cuando, habiéndose puesto a disposición de la persona titular el aviso de privacidad, ésta no manifieste su voluntad en sentido contrario.

La Entidad o Institución deberá verificar si el tratamiento encuadra en alguno de los **supuestos de excepción** establecidos por la Ley.

5. PRINCIPIO DE CALIDAD.
Los datos personales deben ser **exactos, completos, pertinentes, correctos y actualizados**, de modo que reflejen la veracidad necesaria para cumplir la finalidad del tratamiento.

Los datos deben suprimirse cuando dejen de ser necesarios, conforme a los plazos de conservación establecidos en la normativa aplicable y la gestión institucional.

6. PRINCIPIO DE PROPORCIONALIDAD.
El responsable solo debe recabar y tratar aquellos datos personales que sean **estrictamente indispensables, adecuados y relevantes** para cumplir la finalidad prevista.

Se debe evitar solicitar o conservar datos que resulten excesivos o innecesarios.

7. PRINCIPIO DE INFORMACIÓN.
El responsable está obligado a informar a las personas titulares sobre la **existencia, características y finalidades del tratamiento de sus datos personales** a través del aviso de privacidad.

Este aviso deberá ser **claro, accesible y comprensible**, y difundirse por los medios físicos y electrónicos institucionales. Cuando no sea posible proporcionarlo directamente, se deberán implementar **medidas compensatorias de comunicación masiva**, conforme a los lineamientos aplicables.

8. PRINCIPIO DE RESPONSABILIDAD ("RENDICIÓN DE CUENTAS")
El responsable deberá **demostrar** que cumple con todos los principios, deberes y obligaciones en materia de protección de datos personales, mediante la instrumentación de:

- políticas y programas de protección de datos,
- capacitación permanente del personal,
- revisión periódica de medidas de seguridad,
- auditorías internas o externas,
- mecanismos de supervisión,
- sistemas y tecnologías diseñados conforme a los estándares de protección de datos (*privacidad por diseño y por defecto*).

Este principio impone la obligación de establecer **controles internos documentados**, así como de rendir cuentas ante las instancias competentes.

El presente Documento de Seguridad se elabora para:

- Establecer medidas administrativas, técnicas y físicas que aseguren la protección de los datos personales tratados en procedimientos, plataformas, sistemas, trámites, programas, servicios y actividades administrativas de la Entidad.

- Garantizar que el tratamiento de datos personales en cada fase de su ciclo de vida (obtención, almacenamiento, uso, transferencia, bloqueo y supresión) se realice bajo un **estricto deber de seguridad**.

- Informar a los titulares de los datos personales, que la ASIPONA Altamira realiza un tratamiento responsable, seguro y lícito de la información que le es confiada.

Este documento se constituye en cumplimiento de los artículos 31 a 38 de la LGPDPPSO, los Lineamientos Generales.

Este documento tiene carácter vinculante para todas las unidades administrativas, dependencias, entidades, servidores públicos y terceros que bajo cualquier figura tengan acceso, almacenen, procesen o transmitan datos personales en nombre o por cuenta de la ASIPONA Altamira.

ÁMBITO DE APLICACIÓN Y OBSERVANCIA

El presente documento es obligatorio para:

- Todo el personal adscrito a la ASIPONA Altamira.
- Personal eventual y prestadores de servicios profesionales que, en virtud del vínculo jurídico con la Entidad, tengan acceso a datos personales.
- Personas Físicas, Morales, Dependencias y Entidades, presten servicios a la ASIPONA Altamira y accedan a sistemas o bases de datos.

Las medidas de seguridad se aplican a datos contenidos en soportes:

- Físicos.
- Electrónicos (*Tokens, usuarios y contraseñas claves electrónicas, certificados digitales*).
- Videograbaciones.
- Sistemas biométricos.
- Registros de acceso.
- Sistemas de reconocimientos y registro ópticos (*Reconocimiento de iris y retina*).
- Sistemas internos de gestión.
- Huellas Dactilares.
- Reconocimiento facial.
- Reconocimiento de voz.
- Geometría de la mano.
- Firma electrónica avanzada.
- Patrones de pulsaciones en teclado.
- Videograbaciones contenidas por cámara de drones.
- Las contenidas en cualquier otra tecnología.

MARCO LEGAL Y PRINCIPIOS APLICABLES

1. **Constitución Política de los Estados Unidos Mexicanos**, artículos 6°, Base A y 16, segundo párrafo, que contiene la Garantía y/o Derecho Humano de las personas físicas y morales a la Protección de sus Datos Personales.

2. **Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO),** en particular los artículos relativos a las obligaciones de seguridad (capítulo correspondiente), los derechos de los titulares (acceso, rectificación, cancelación, oposición) y los principios para el tratamiento.

3. **Ley General de Transparencia y Acceso a la Información Pública (LGTAIP),** en lo referente a la protección de datos personales como parte de las obligaciones de los sujetos obligados.

4. **Ley General de Archivos**, que regula la obligación de conservación de documentos que contienen datos personales, por el periodo de tiempo que la propia ley establece, además de que exige medidas de preservación, seguridad y baja documental.

5. **Ley Federal de Derechos**, Relativo a la certificación electrónica y firma digital en actos de comercio en su interacción con datos.

6. **Ley de Firma Electrónica Avanzada**, En lo referente a que define datos y elementos biométricos usados para validar identidades digitales.

7. **Lineamientos Generales de Protección de Datos Personales para el Sector Público,** que establecen estándares mínimos para la seguridad de los datos, categorización, mecanismos de monitoreo, políticas de respaldo y de gestión de brechas.

8. **Otros instrumentos normativos relevantes:** normativas internas de ASIPONA Altamira, políticas de seguridad de tecnologías de la información, planes institucionales de continuidad del negocio, protocolos de seguridad informática, etc.

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

En cumplimiento de lo establecido por los artículos **27, fracción I** y **29, fracción I** de la *Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO)*, la Administración del Sistema Portuario Nacional **ASIPONA Altamira**, como responsable del tratamiento de datos personales, elaboró el Inventario de Datos Personales y de los Sistemas de Tratamiento que integran el presente Documento de Seguridad.

Asimismo, se da cumplimiento a lo dispuesto en los artículos **58 y 59** de los *Lineamientos Generales de Protección de Datos Personales para el Sector Público*, los cuales establecen los elementos mínimos que debe contener dicho inventario, así como la consideración del ciclo de vida de los datos personales.

1. *Elementos mínimos del Inventario (Artículo 58 de los Lineamientos Generales)*

Para cada uno de los tratamientos de datos personales identificados, se consideraron los siguientes elementos:

a) **Catálogo de medios físicos y electrónicos** mediante los cuales se obtienen los datos personales.
b) **Finalidades** del tratamiento correspondiente.
c) **Tipos de datos personales tratados**, indicando si se consideran sensibles.
d) **Formatos y ubicaciones de almacenamiento**, tanto físicos como electrónicos.
e) **Lista de servidores públicos** que tienen acceso a los sistemas de tratamiento.
f) En su caso, **identificación del encargado** que participa en el tratamiento y el instrumento jurídico aplicable.
g) En su caso, **destinatarios de transferencias** y las finalidades que las justifican.
Ser establecen los **Riesgos y/o Vulnerabilidad Identificados**, así como las **Medidas de Seguridad Implementadas** para su Resguardo.
h) En su caso **Lista e identificación de los Servidores Públicos** con acceso al Sistema.
i) Plataforma Tecnológica e Infraestructura donde se alojan.
j) Tiempo de Conservación y Criterios de eliminación.

2. Ciclo de vida de los datos personales (Artículo 59 de los Lineamientos Generales)

En la integración del inventario se valoró el ciclo de vida completo de los datos personales, considerando:

- **Obtención** de los datos personales.
- **Almacenamiento** físico y/o electrónico.
- **Uso**, manejo, aprovechamiento, monitoreo y procesamiento.
- **Divulgación**, incluyendo remisiones y transferencias.
- **Bloqueo**, en los casos que proceda.
- **Cancelación o supresión** de los datos personales.

La ASIPONA Altamira identificó los riesgos inherentes asociados al tratamiento, considerando los activos involucrados: hardware, software, personal, infraestructura y cualquier otro recurso pertinente.

3. Inventarios elaborados por ASIPONA ALTAMIRA

Con base en lo anterior, se integraron los inventarios correspondientes a cada unidad administrativa que trata datos personales. ASIPONA Altamira identifica los siguientes conjuntos de datos personales que trata como parte de sus funciones:

No.	Conjunto de Datos	Medios de Obtención	Finalidades del Tratamiento	Tipos de Datos, Sensibles	Formatos y Ubicación	Servidores Públicos con Acceso	Encargado e Instrumento Jurídico	Destinatarios y Finalidad
1	Datos de identificación	Formularios físicos, correos institucionales, ventanilla, identificaciones oficiales	Identificación plena de usuarios y servidores públicos	Identificación (no sensibles y algunos sensibles como fotografía)	Expedientes físicos en archivo; sistemas electrónicos internos	Unidad de Transparencia, RH, Jurídico	No aplica o contratos de servicios informáticos	Autoridades competentes; verificación y control
2	Datos de contacto	Formularios físicos, correos institucionales, solicitudes web	Establecer comunicación institucional	Contacto (no sensibles)	Sistemas de correo, archivos digitales; archivo físico	Personal autorizado del área correspondiente	No aplica	No se realizan transferencias
3	Datos relativos a la función pública/laboral	Sistemas internos RH, expedientes laborales, correos institucionales	Gestión de personal y administración de la relación laboral	Laborales (no sensibles, algunos sensibles en expedientes)	Expedientes laborales; sistema RH; archivo general	RH, Jurídico, Órgano Interno de Control	Encargados RH; contratos de prestación de servicios	STPS, SHCP cuando proceda; cumplimiento normativo
4	Datos de prestadores de servicios/proveedores/contratistas	Propuestas físicas y electrónicas, Compras MX , contratos	Formalizar relaciones contractuales y administrativas	Administrativos y financieros (algunos sensibles: cuentas bancarias)	Archivo físico; sistema de proveedores; plataformas electrónicas	Comercialización, Jurídico, Adquisiciones	Contratos con proveedores y terceros	SAT, SHCP; cumplimiento contractual
5	Datos relacionados con licitaciones y servicios portuarios	Plataformas de contratación, expedientes físicos y electrónicos	Administrar procedimientos de contratación y servicios portuarios	Administrativos, económicos (no sensibles en general)	Sistemas de contratación; archivo físico; servidores institucionales	Comercialización, Operaciones, Jurídico	Contratos y bases de licitación	Órganos de fiscalización; verificación

No.	Conjunto de Datos	Medios de Obtención	Finalidades del Tratamiento	Tipos de Datos, Sensibles	Formatos y Ubicación	Servidores Públicos con Acceso	Encargado e Instrumento Jurídico	Destinatarios y Finalidad
6	Datos de visitantes y usuarios de instalaciones portuarias	Bitácoras de acceso, credenciales, registros en caseta	Control de acceso y seguridad en instalaciones	Identificación (no sensibles)	Bitácoras en caseta; base digital de acceso	Seguridad física y control de acceso	No aplica	Autoridades de seguridad; control y trazabilidad
7	Datos de videovigilancia y control de acceso	Cámaras CCTV, controles electrónicos de acceso	Seguridad, monitoreo y control de accesos	Imágenes y registros (no sensibles)	Servidores del CCTV; respaldo institucional	Seguridad física, TI	Contratos con proveedores de CCTV	Autoridades de seguridad; prevención de incidentes
8	Datos sensibles	Dispositivos biométricos autorizados	Control de acceso reforzado y verificación de identidad	Datos biométricos (sensibles)	Base biométrica institucional, servidores de seguridad	Seguridad física, TI	Contratos de tecnología y seguridad	Autoridades competentes; identificación
9	Datos para envío de comunicaciones electrónicas y alertas	Listas de distribución, sistemas de comunicación institucional	Enviar notificaciones, avisos y alertas institucionales	Datos contacto (no sensibles)	Servidores institucionales; listas de distribución	Comunicación social, TI, áreas emisoras	No aplica	No se realizan transferencias

2. Sistemas de Tratamiento

Se identifican los siguientes sistemas de tratamiento de datos personales al interior de ASIPONA Altamira:

- Sistema de Recursos Humanos: gestión de expedientes de personal, altas, bajas, control de nómina y archivo electrónico.
- Sistema de Contrataciones y Adquisiciones: plataforma de licitaciones, adjudicaciones, gestión documental de proveedores, pagos.
- Sistema de Control de Acceso y Videovigilancia: hardware y software de reconocimiento de identidad, dispositivos de registro de entradas y salidas, cámaras de vigilancia.
- Sistema de Correo Electrónico Institucional y Mensajería: para el envío de avisos, comunicaciones internas y externas que pueden contener datos personales.
- Sistema de Gestión Documental Electrónica: repositorio de archivos electrónicos y expedientes que contienen datos personales.
- Sistema de Atención al Público y Registro de Visitas: módulo de recepción y acreditación de visitantes, registro y seguimiento.
- Sistema de Administración del Puerto / Logística: registros de operaciones, usuarios de servicios portuarios, datos de operadores, empresas.
- Copias de seguridad y almacenamiento en la nube o centro de datos alterno: respaldos y duplicación de los sistemas antes descritos.
- Sistema de Recepción y/o Ingreso Documental (*física y en dispositivos digitales*) al Público en General denominada Ventanilla Única.

3. Responsables del Inventario

La Unidad de Transparencia y Protección de Datos Personales de ASIPONA Altamira – junto con la Dirección de Tecnologías de la Información y la Unidad de Recursos Humanos – será responsable de mantener actualizado este inventario, revisándolo por lo menos cada doce meses o cuando se implemente un nuevo sistema de tratamiento.

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

En términos de lo dispuesto en el artículo 27 de **la LGPDPPSO** y los artículos correspondientes de los **LGPDPSP**, las personas (servidores públicos, contratistas, usuarios internos) que intervengan en el tratamiento de datos personales deberán observar las siguientes funciones y obligaciones:

1. Funciones

a) Conocer y aplicar la Política de Protección de Datos Personales de ASIPONA Altamira y el presente Documento de Seguridad.

b) Realizar las actividades de tratamiento únicamente conforme a las finalidades autorizadas, documentadas y comunicadas a los titulares.

c) Identificar, en su ámbito, los riesgos potenciales del tratamiento de datos personales y reportar incidentes de seguridad a la Unidad de Transparencia y Protección de Datos Personales.

d) Participar en los programas de capacitación, auditoría y revisión relacionados con protección de datos personales.

e) Guardar confidencialidad respecto de los datos personales a los que tengan acceso, durante el tiempo que estén bajo su responsabilidad, así como después de concluida la relación laboral o de prestación de servicios.

f) Facilitar el ejercicio de los derechos de los titulares de los datos personales (acceso, rectificación, cancelación u oposición —ARCO—) y colaborar con la Unidad de Transparencia en los trámites correspondientes.

g) Contribuir al cumplimiento de las medidas técnicas y organizativas establecidas para salvaguardar los datos personales.

2. Obligaciones

a) Tratar los datos personales conforme a los principios de licitud, lealtad, finalidad, proporcionalidad, calidad, transparencia, responsabilidad y rendición de cuentas, conforme a lo previsto en la LGPDPPSO, constituyendo una obligación de guardar secreto de cualquier dato personal al que en virtud de su puesto tenga acceso, en el entendido de que la obligación no termina aun cuando dejen el cargo, contrato o comisión.

b) Abstenerse de utilizar los datos personales para fines distintos de los señalados y/o previstos en la Ley, sus funciones, las facultades, actividades y atribuciones legales inherentes a su puesto o comisión, ya que el incumplimiento a esta obligación, es decir usarlos para fines distintos, sin contar con los mecanismos legales o comunicados al titular, constituye una infracción a la Ley.

c) Mantener actualizados los datos cuando corresponda, conforme al principio de calidad.

d) Adoptar las medidas de seguridad físicas, técnicas y administrativas que le correspondan según la categoría de los datos y los sistemas de tratamiento.

e) Comunicar de inmediato cualquier evento de vulneración de la seguridad (brecha de datos, acceso no autorizado, pérdida, robo o alteración) a la Unidad de Transparencia y Protección de Datos Personales.

f) Garantizar que los accesos a los sistemas de tratamiento sean únicamente los estrictamente necesarios para el cumplimiento de sus funciones (control de privilegios).

g) Conservar y proteger los registros de tratamiento, es decir asegurarse de que los datos se conserven de manera segura asegurándose que se dé cumpliendo con las medidas de seguridad físicas, técnicas y administrativas correspondientes, previniendo que se produzcan accesos, usos o modificaciones no autorizadas, así como apoyar en la elaboración de auditorías, monitoreos e informes de cumplimiento.

h) Al término de la relación laboral o contractual, devolver los soportes que contengan datos personales y proceder a su disposición documental conforme a lo señalado en el Catálogo de Disposición Documental de ASIPONA Altamira,

i) Abstenerse de recolectar datos que no sean necesarios, no guardar datos por un tiempo superior a la que establece la normatividad aplicable, y por ende debe de aplicar los plazos de conservación y los procedimientos de eliminación.

3. Responsabilidad

Las personas que incumplan las obligaciones previstas estarán sujetas a las sanciones administrativas, disciplinarias o penales que correspondan, de conformidad con la **LGPDPPSO,** la **LGTAI**, la **LFTAIG** y demás normativa aplicable.

III. ANÁLISIS DE RIESGOS

1. Identificación de riesgos

En el marco del tratamiento de datos personales, ASIPONA Altamira ha identificado los siguientes riesgos inherentes:

- Acceso no autorizado por personal interno o externo al sistema de tratamiento de datos personales.

- Pérdida o robo de soportes físicos o electrónicos que contengan datos personales (por ejemplo: unidades extraíbles, discos duros, laptops, servidores).
- Alteración o destrucción accidental o intencionada de los datos personales sin capacidad de recuperación.
- Filtración o divulgación no autorizada de datos personales al público o terceros no autorizados.
- Vulneración de la autenticidad e integridad de los datos personales (modificación no adecuada).
- Inadecuada gestión de privilegios de acceso, permitiendo que personas no autorizadas accedan a datos sensibles.
- Falla en los sistemas de respaldo o recuperación ante desastres, generando indisponibilidad de datos críticos.
- Fallas en la actualización o mantenimiento de software de tratamiento, exponiendo vulnerabilidades explotables.
- Transferencias de datos personales a terceros sin la debida salvaguarda contractual o técnica.
- Incumplimiento de los derechos ARCO de los titulares: acceso, rectificación, cancelación u oposición.
- Uso de datos personales con fines no previstos o sin consentimiento cuando sea requerido.

2. Evaluación del riesgo (probabilidad × impacto)

Riesgo	Probabilidad	Impacto	Nivel de riesgo
Acceso no autorizado	Media	Alto	Alto
Pérdida o robo de soporte físico	Media	Alto	Alto
Filtración de datos personales	Baja-Media	Muy Alto	Alto
Alteración de datos sin recuperación	Baja	Alto	Medio
Fallas en respaldo y recuperación	Media	Medio	Medio
Gestión inadecuada de privilegios	Media	Alto	Alto
Transferencias sin salvaguarda	Baja	Medio	Medio
Incumplimiento de derechos ARCO	Media	Medio	Medio

3. Valoración

Con base en la tabla anterior, se considera que los riesgos de mayor prioridad para atención inmediata son: acceso no autorizado, pérdida o robo de soportes, filtración de datos personales y gestión inadecuada de privilegios. Los demás riesgos deberán ser gestionados conforme al Plan de Trabajo.

IV. Análisis de Brecha

1. Identificación de brechas existentes

Tras la revisión de los sistemas y procesos de tratamiento, ASIPONA Altamira, con fundamento en lo que dispone la normatividad aplicable en materia de datos personales, los lineamientos generales, el aviso de privacidad, las medidas de seguridad exigidas y las buenas prácticas de tratamiento de datos personales, se detecta las siguientes brechas de seguridad y cumplimiento, estableciéndose que constituye un proceso obligatorio que forma parte de las medidas de seguridad, evaluación de riesgos y gestión del tratamiento de datos personales que deben realizar los sujetos obligados, establecidos en la Ley, de manera específica en: Artículo 31 (**medidas de seguridad**); artículo 32 (**análisis de riesgos y gestión**); y Artículos 58 y 59 (**inventario y documentación**):

- Falta de control de registro de accesos y auditoría detallada en el sistema de recursos humanos que capture acceso, modificación y baja de datos personales.
- Insuficiente capacitación formal y periódica para todo el personal en materia de protección de datos personales.
- Presencia de soportes extraíbles (USB, discos duros externos) sin cifrado ni política clara de uso y custodia.
- No existencia de un procedimiento formal para la destrucción segura de soportes que contienen datos personales cuando ya no son necesarios.
- Acuerdos o contratos con terceros que no contemplan cláusulas específicas de tratamiento de datos personales (encargados) conforme a la **LGPDPPSO.** Se exceptúan aquellos instrumentos emitidos por la SHCP o por cualquier otro órgano que los proporcione de manera oficial, respecto de los cuales será necesario solicitar una opinión jurídica a fin de determinar la viabilidad de su modificación o, en su caso, la procedencia de realizar ajustes complementarios.
- Ausencia de pruebas periódicas de recuperación ante desastres para los sistemas que contienen datos personales.
- Falta de un mecanismo de monitoreo permanente y revisión de los registros de incidentes de seguridad de los datos personales, de conformidad con lo que establece el artículo 32 de la LGPDPPSO, responsable deberá llevar una bitácora de las vulneraciones a la seguridad en la que se describa, la fecha en la que ocurrió, el motivo de ésta y las acciones correctivas implementadas de forma inmediata y definitiva.
- Falta de un registro eficaz y controles adecuados de los servidores públicos que acceden a los datos.
- Archivos físicos sin un control ni manejo adecuado.

2. Evaluación de la brecha

Existe la necesidad de realizar la evaluación de la brecha conforme lo dispone el artículo 31 de la LGPDPPSO, que señala que, en caso de que ocurra una vulneración a la seguridad, el responsable deberá analizar las causas por las cuales se

presentó e implementar 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 repite

El conjunto de brechas identificadas se considera de impacto medio-alto, dado el carácter sensible de algunos datos personales (por ejemplo, biométricos, datos de proveedores) y la obligación legal de protección que recae sobre ASIPONA Altamira en su calidad de sujeto obligado. Se estima que sin la corrección de estas brechas podría presentarse un incidente grave de seguridad que derive en sanciones, pérdida de confianza y vulneración de derechos de los titulares.

V. PLAN DE TRABAJO

1. Objetivo general

Garantizar que el tratamiento de los datos personales en posesión de ASIPONA Altamira se realice bajo estándares de seguridad adecuados, mitigando los riesgos identificados y subsanando las brechas existentes, con sujeción plena a la LGPDPPSO, la LGTAI y los LGPDPSP.

2. Acciones, responsables y cronograma

Acción	Responsable	Fecha de inicio	Fecha de término	Indicador de cumplimiento
Actualización del inventario de datos y sistemas de tratamiento	Unidad de Transparencia y TI	01 julio 2026	30 septiembre 2026	Inventario actualizado suscrito
Implantación de registro y auditoría de accesos al sistema de RRHH	Departamento de TI	01 agosto 2026	31 octubre 2026	Registro automático operativo
Implementación de política de cifrado para soportes extraíbles	Departamento de TI	15 agosto 2026	15 noviembre 2026	100 % de soportes cifrados
Revisión y firma de cláusulas de tratamiento de datos personales en contratos con terceros	Unidad de Transparencia /Gerencia Jurídica	01 julio 2026	31 diciembre 2026	100 % de contratos actualizados
Programa de destrucción segura de soportes con datos personales	Departamento de TI / Unidad de Archivo	01 septiembre 2026	30 noviembre 2026	Procedimiento implementado y primeros informes generados
Ejercicio de recuperación ante desastres (test) para sistemas críticos que contienen datos personales	Departamento de TI	01 octubre 2026	31 diciembre 2026	Informe de prueba con 0 % de fallos críticos
Capacitación inicial en protección de datos personales para todo el personal	Unidad de Transparencia / Departamento de RRHH	15 julio 2026	31 agosto 2026	100 % del personal capacitado y evaluación aprobada

Acción	Responsable	Fecha de inicio	Fecha de término	Indicador de cumplimiento
Establecimiento de mecanismos de reporte e incidente de datos personales	Unidad de Transparencia	01 septiembre 2026	30 noviembre 2026	Manual operativo y sistema de reporte activo
Revisión y actualización anual del Documento de Seguridad	Unidad de Transparencia	01 enero 2027	31 enero 2027 (posterior)	Documento revisado y aprobado por la dirección general

3. Recursos asignados

ASIPONA Altamira deberá asignar los recursos humanos, técnicos y presupuestales pertinentes para la implementación de cada acción. Se asume la participación del personal de **TI**, personales adscritos a las gerencias que reciben información dirigida a la Entidad, transparencia, archivo, recursos humanos, así como la contratación de servicios externos especializados, en su caso.

4. Supervisión y reporte

La Unidad de Transparencia presentará semestralmente a la dirección general un informe de avance del Plan de Trabajo, con indicadores de cumplimiento, incidencias y propuestas de mejora.

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

1. Monitoreo continuo

- Registro automático en bitácoras electrónicas de accesos, modificaciones y bajas de los datos personales, así como auditorías internas de logs., que emitan alertas de accesos no autorizados.
- Revisión mensual de incidentes reportados relacionados con datos personales, con análisis de causa raíz y medidas correctivas, que permitan identificar las vulnerabilidades y probabilidad de ocurrencia.
- Verificación trimestral del estado de cifrado de soportes, actualización de parches de software, control de privilegios de acceso, que permitan realizar un correcto análisis de amenazas internas y externas.
- Evaluación anual de cumplimiento de derechos ARCO y reporte de incidencias en trámites de acceso, rectificación, cancelación u oposición.

2. Revisión y evaluación periódica

- Auditoría interna anual del tratamiento de datos personales, incluyendo revisión de contratos con terceros, políticas de seguridad, recuperación ante desastres, destrucción de soportes.
- Revisión del Documento de Seguridad cada doce meses o cuando se detecten cambios significativos en la tecnología, estructura organizacional o normativa aplicable.

- Informe anual a la dirección general sobre el estado de la protección de datos personales e inclusión de plan de mejora continua.

3. Indicadores de cumplimiento mediante auditorías internas que permitan establecer:

- Porcentaje de personal que ha recibido capacitación y aprobado evaluación interna.
- Número de incidentes de datos personales reportados vs resueltos.
- Porcentaje de soportes cifrados respecto del total de soportes que contienen datos personales.
- Tiempo promedio de respuesta de trámites ARCO.
- Tiempo medio de restauración en ejercicios de recuperación ante desastres.
- El uso correcto de los equipos, el cumplimiento de políticas y el tratamiento adecuado de datos sensibles.

4. Mejora continua

- Las deficiencias detectadas en las auditorías y monitoreos se incorporarán al plan de mejora anual, en donde se actualizarán los análisis de riesgos, incorporando nuevos escenarios, de acuerdo con el avance de la ciencia, tales como ciberataques, accesos remotos, el uso de la Inteligencia Artificial, así como actualizar y ajustar los controles cuando cambien los sistemas o procesos.
- Actualizar los permisos cada vez que se cambie de personal y deshabilitar cuantes cuentas inactivas o sin justificación.
- Se actualizarán las políticas, procedimientos y protocolos conforme a las mejores prácticas, estándares internacionales y la normativa nacional aplicable.
- La dirección general de ASIPONA Altamira promoverá una cultura institucional de protección de datos personales, en la cual el cumplimiento sea visto como valor estratégico.
- La capacitación permanente y especializada del personal, en el ámbito normativo, de recursos humanos, simulación de incidentes y ciberataques, y en otras áreas, que la Entidad crea conveniente.

VII. PROGRAMA GENERAL DE CAPACITACIÓN

1. Objetivo

Fortalecer las competencias y conocimientos de todos los servidores públicos, contratistas y terceros que tratan datos personales en ASIPONA Altamira, para asegurar el cumplimiento de sus obligaciones legales, la prevención de riesgos y la correcta aplicación de las medidas de seguridad.

2. Contenido mínimo de capacitación

- Fundamento jurídico de la protección de datos personales en México: Constitución, LGPDPPSO, LGTAI, LFTAIG, LGPDPSP. CENACE+1
- Principios de protección de datos personales (licitud, finalidad, proporcionalidad, etc.).
- Derechos de los titulares: acceso, rectificación, cancelación, oposición y demás.

- Obligaciones del responsable y encargado del tratamiento.
- Medidas de seguridad físicas, técnicas y administrativas: cifrado, control de accesos, respaldo, destrucción segura, registro de incidentes.
- Gestión de riesgos y brechas de seguridad de datos personales.
- Procedimiento interno de reporte de incidentes y respuesta a brechas.
- Buenas prácticas para el manejo seguro de datos personales, uso adecuado de dispositivos electrónicos, políticas de contraseñas.
- Contratación de terceros, cláusulas de protección de datos y supervisión de encargados.
- Evaluación de sensibilización y cultura de protección de datos personales.

3. Cronograma y periodicidad

- Capacitación inicial obligatoria: dentro de los primeros sesenta días posteriores a la aprobación del presente documento.
- Refuerzo anual: mínimo una vez al año para todo el personal.
- Capacitación específica ad hoc: cuando se implante un nuevo sistema de tratamiento, cuando se modifique sustancialmente un proceso o tras una brecha significativa.
- Registro de asistencia, evaluación de conocimientos y seguimiento de acciones correctivas.

4. Evaluación y seguimiento

- Cada curso incluirá una prueba de conocimiento que deberá aprobarse con al menos 80 %.
- Los resultados se integrarán al expediente individual del servidor público o contratista.
- La Unidad de Transparencia en colaboración con Recursos Humanos elaborará un reporte anual de cumplimiento del programa y propondrá mejoras.

VIII. GLOSARIO

ASIPONA Altamira. -Administración del Sistema Portuario Nacional Altamira, S.A de C.V

SABG. – secretaria de Anticorrupción y Buen Gobierno.

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

LGTAIP. - Ley General de Transparencia y Acceso a la Información Pública

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

TI.- Tecnologías de la información (departamento de informática).

TRÁMITES ARCO. - Son un mecanismo legal que te permite ejercer control sobre tus datos personales. El acrónimo significa:

- Acceso
- Rectificación
- Cancelación
- Oposición