

DOCUMENTO DE SEGURIDAD

**Administración Portuaria Integral de
Tamaulipas, S.A de C.V.**

ÍNDICE

INTRODUCCIÓN	3
OBJETIVO	4
GLOSARIO	4
I. INVENTARIO DE DATOS PERSONALES.....	7
II. FUNCIONES Y OBLIGACIONES DE LAS PERSONAS QUE TRATEN LOS DATOS PERSONALES ...	10
III. ANÁLISIS DE RIESGOS	14
IV. ANÁLISIS DE BRECHA.....	15
V. PLAN DE TRABAJO	18
VI. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD	19
VII. PROGRAMA GENERAL DE CAPACITACIÓN EN DATOS PERSONALES	20

INTRODUCCIÓN

El presente documento se elaboró en apego a lo previsto por el artículo 17, fracción V, segundo párrafo de la Constitución Política del Estado de Tamaulipas, la cual se encuentra armonizada con las disposiciones de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, reglamentaria del artículo 16, párrafo segundo, de la Constitución Política de los Estados Unidos Mexicanos.

La Ley de Protección de Datos Personales en Posesión de Sujetos Obligados para el Estado de Tamaulipas establece, en lo particular un conjunto de bases, principios y procedimientos para garantizar el derecho a la protección de datos con carácter personal y que se encuentren en posesión de los sujetos obligados, entre los que figura la Administración Portuaria Integral del Puerto de Matamoros -**Administración Portuaria Integral de Tamaulipas, S. A. de C.V. (APITAM)**-

Para ello, en términos de lo previsto en el artículo 31 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados para el Estado de Tamaulipas, el cual establece que el responsable deberá mantener actualizado su documento de seguridad como resultado del proceso de mejora continua, la **APITAM**, emite el documento de seguridad con base en los requisitos establecidos en el artículo 29 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados para el Estado de Tamaulipas, a saber:

- I. El inventario de datos personales y de los sistemas de tratamiento;
- II. Las funciones y obligaciones de las personas que tratan datos personales;
- III. El análisis de riesgos;
- IV. El análisis de brecha;
- V. El plan de trabajo;
- VI. Los mecanismos de monitoreo y revisión de las medidas de seguridad; y
- VII. El programa general de capacitación.

OBJETIVO

Fomentar el derecho a la protección de datos personales en posesión de sujetos obligados y establecer los principales elementos que integran las medidas de seguridad administrativas, físicas y técnicas que ha adoptado esta **Administración Portuaria Integral del Puerto de Matamoros APITAM**, para garantizar la confidencialidad, integridad y disponibilidad de los datos personales.

Y que, en todo momento la persona titular de los datos personales pueda acceder a ellos, a través de los derechos **ARCO**, tales como: el acceso, rectificación, cancelación y oposición en los términos que determina la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Tamaulipas.

GLOSARIO

APITAM: Administración Portuaria Integral de Tamaulipas, S.A de C.V.

Ley: Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Tamaulipas.

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 de los datos personales.

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

Bases de datos: Conjunto ordenado de datos personales referentes a una persona identificada o identificable, condicionados 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 identificada o identificable. Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información.

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

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 permitan proteger 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.

Persona responsable: Persona física que sola o conjuntamente con otras trate datos personales a nombre del sujeto obligado.

Titular: Persona a quien corresponden los datos personales.

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

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.

Software: Es el conjunto de programas o aplicaciones, instrucciones y reglas informáticas que hacen posible el funcionamiento del equipo.

I. INVENTARIO DE DATOS PERSONALES

El Inventario de Tratamientos de Datos Personales (Inventario) es el control documentado que se lleva a cabo de los tratamientos de datos personales que realizan las áreas/órganos, contemplado en los artículos 27 y 29, fracción I, de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Tamaulipas.

Para cumplir con los objetivos y obligaciones que prevé la Ley, particularmente en materia de seguridad y de protección de datos personales que se manejan en **APITAM**, se realizó una revisión dentro de las unidades administrativas que conforman su estructura orgánica, para identificar los procesos prioritarios en los que actualmente se lleva a cabo el tratamiento de datos personales; obteniendo con ello el denominado Inventario de datos Personales de la **APITAM**.

Los elementos que actualmente se identifican en el Inventario de cada uno de los tratamientos son los siguientes:

- Nombre de la unidad administrativa.
- Datos que recaban.
- Finalidad.
- Fundamento normativo.
- Datos personales que se recaban.
- Forma de obtención de los datos personales.
- Cargos de las personas que tienen acceso a la base de datos.
- Tipo de soporte en el que se almacena la base de datos personales.
- Información sobre transferencias de datos personales.
- Plazo de conservación.

ESTRUCTURA ÓRGANICA

Dirección General

- **Secretario Ejecutivo de Cumplimiento Normativo y Operación del buen Gobierno**
- **Gerencia para el Desarrollo Sostenible e Internacional**
- **Gerencia Intersectorial para Gestiones Prospectivas**
- **Gerencia Interinstitucional de Proyectos Productivos para Mejoras Continuas**
- **Gerencia de Planeación, desarrollo y seguimiento**
 - Subgerencia de Planeación y Presupuesto
 - Departamento de Presupuesto
 - Departamento de Planeación
 - Departamento de Proyectos
 - Subgerencia de Gestión y Tramitología Interinstitucional
 - Departamento de Oficialía de Partes
 - Departamento de Tramitología
 - Subgerencia Técnica de Proyectos y Licitaciones
 - Departamento de Licitaciones
 - Departamento Técnico y Proyectos
 - Subgerencia de Integración de Expedientes Técnicos y Unitarios y Atención a Auditorías
 - Departamento de Presupuesto Público y Privado
 - Departamento de Presupuesto Propio
- **Gerencia Jurídica**
 - Subgerencia jurídica de Procedimientos Legales
 - Departamento de Estructura Corporativa y Contratos
 - Departamento de lo Contencioso
 - Subgerencia de Normatividad y Acceso a la Información
 - Departamento de Normatividad, Transparencia y Manejo de Datos Personales
- **Gerencia de Administración y Finanzas**
 - Subgerencia de Informática

- Departamento de Sistemas
- Subgerencia de Administración, Finanzas y Materiales
- Departamento de Recursos Financieros
- Departamento de Contabilidad
- Departamento de Recursos Humanos
- Departamento de Tesorería
- Departamento de Recursos Materiales

- **Gerencia de Ingeniería**
 - Subgerencia de Ecología y Gestión Ambiental
 - Departamento de Programas y Proyectos Ambientales
 - Departamento de Supervisión y Vigilancia Ambiental
 - Departamento de Análisis, Monitoreo y Protección Ambiental
 - Subgerencia de Construcción y Mantenimiento
 - Departamento de Construcción y Mantenimiento
 - Departamento de Supervisión y Control de Obra

- **Gerencia de Operaciones**
 - Subgerencia de Operaciones y Verificaciones Portuaria
 - Departamento de Operaciones
 - Departamento de Terminales y Recintos Fiscales
 - Departamento de Verificación y Estadística
 - Subgerencia de Protección Portuaria
 - Departamento de Seguridad
 - Departamento de Radalización y Meteorología
 - Centro de Control de Tráfico Marítimo

- **Gerencia de Comercialización**
 - Subgerencia de Desarrollo de Negocios
 - Departamento de Comercio Exterior

- Departamento de Estrategia, Estadística y Rentabilidad
- Subgerencia Comercial
- Departamento de Ventas y Marketing
- Departamento de inversiones y alianzas comerciales sectores fluidos (Hidrocarburos)
- Departamento de inversiones y alianzas comerciales de almacenaje
- Departamento de inversiones y alianzas de carga general no contenerizado
- Departamento de inversiones y alianzas comerciales de gráneles de construcción
- Departamento de inversiones y alianzas comerciales de gráneles minerales
- Departamento de inversiones y alianzas comerciales de gráneles agrícolas
- Departamento de Relaciones Públicas

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

- **Secretariado Ejecutivo de Cumplimiento Normativo y Operación del Buen Gobierno:** coordinar acciones con el director General en las comisiones que le encomiende, someter a su aprobación los estudios, proyectos, vigilar que se cumpla estrictamente con las disposiciones legales y administrativas en todos los asuntos asignados, a través de planear, programar, gestionar y evaluar una agenda estratégica interinstitucional normativa, para proyectar un plan de acción que asegure los máximos beneficios para la sociedad, garantizando el desarrollo humano, social y económico.
- **Auxiliar Administrativo:** actualizar el registro de información institucional, en coordinación con las diferentes áreas de la entidad, para mejorar el funcionamiento interno de la entidad.
- **Gerencia de Administración y Finanzas:** coordinar acciones con el Director General y con áreas adscritas a la Entidad en el establecimiento de normas, actualizaciones de registros contables, presupuestales, financieros, materiales, recursos humanos y

servicios generales, a través del Sistema Contable Gubernamental, con la finalidad de dar cumplimiento a las bases de legislación aplicable en la materia.

- **Subgerencia de Informática:** controlar, coordinar, evaluar e implementar las tecnologías de información y comunicación que opera la API Tamaulipas, bajo una difusión controlada, con la finalidad de dar atención a los nuevos requerimientos en esa materia.
- **Departamento de sistemas:** asegurar que las funciones, procesos y servicios a cargo de la Entidad se optimicen, a través del uso y aprovechamiento de tecnologías de la información e impulsando la implementación de soluciones tecnológicas innovadoras, con la finalidad de que contribuyan al logro de los objetivos estratégicos de la Entidad y se cumplan con las necesidades de los usuarios.
- **Auxiliar Técnico:** coadyuvar con el departamento de sistemas en todas las actividades con el fin de asegurar la eficiencia en el uso de las tecnologías de información que contribuyan al logro de los objetivos estratégicos de la Entidad.
- **Subgerencia de Administración, Finanzas y Materiales:** impulsar el desarrollo del capital humano, a través de la generación de competencias relacionadas con las responsabilidades del puesto y detectando necesidades de la empresa, así como obtener, administrar, aprovechar y supervisar los recursos financieros, estableciendo estrategias para la optimización de los mismos y elaborando y validando estados financieros, con la finalidad de contribuir al incremento de la efectividad de la Entidad y la competitividad del puerto.
- **Departamento de Contabilidad:** fomentar el cumplimiento de las políticas y procedimientos necesarios en apego a la normatividad aplicable, mediante la actualización diaria de la información en el sistema contable y elaborar estados financieros, para proporcionar información contable y presupuestal acorde a la norma.

- **Auxiliar Contable:** coadyuvar con el departamento de contabilidad, estableciendo directrices para el cumplimiento de obligaciones contables y fiscales aplicables a la entidad.
- **Departamento de Tesorería:** elaborar el proceso de gestión y pago de viáticos al personal de la empresa, realizando conciliaciones bancarias y acciones relativas al pago de contribuciones, validar comprobantes fiscales, y recursos financieros, controlar la disposición de efectivo, a fin de hacer eficiente la facturación y cobro de los servicios portuarios.
- **Departamento de Recursos Financieros:** manejar y controlar los recursos financieros, en apego a las Leyes y normas reglamentarias específicas; con base en el sistema contable gubernamental, banca de gobierno digital y herramientas presupuestales específicas; a fin de generar información ejecutiva para toma de decisiones.
- **Departamento de Recursos Humanos:** ejecutar el proceso de reclutamiento, selección y contratación de personal, establecer controles de asistencia, vacaciones, permisos, incapacidades, planificando, dirigiendo y coordinando las actividades del personal y las relaciones laborales, estableciendo y dando seguimiento a los asuntos laborales, a fin de garantizar que cada puesto esta operado por personal con el perfil idóneo.
- **Gerencia Jurídica:** asesorar al director General y a las unidades administrativas que conforman la Entidad, coordinar la adjudicación de contratos regulados por la Ley de Puertos, así como el registro y control de las obligaciones contractuales; recabando y difundiendo la información relativa a las obligaciones de transparencia y de cumplimiento normativo, con la finalidad de cumplir con la legislación aplicable y dotar de certidumbre jurídica todos los actos en que intervenga la API Tamaulipas.

- **Subgerencia Jurídica de Procedimiento Legales:** revisar los proyectos de demandas y contestación de demandas en los asuntos contenciosos, laborales, civiles, mercantiles, y en cualquier asunto en donde los intereses de la Entidad se vean afectados, mediante la elaboración de modelos de contratos y convenios, así como la revisión de los mismos y demás instrumentos jurídicos a través de los cuales la Entidad formalizan sus relaciones contractuales con terceros y en su caso la revisión de las garantías cuando por la complejidad de las mismas así lo ameriten, con la finalidad de dar cumplimiento a las acciones encomendadas.
- **Departamento de Estructura Corporativa y Contratos:** fijar y revisar las bases legales de las concesiones, permisos y autorizaciones relativos a contratos, convenios, coordinando acciones con las diferentes áreas de la Entidad, con la finalidad de vigilar el estricto cumplimiento a la normatividad y dictaminar su interpretación y efectos jurídicos.
- **Departamento de lo Contencioso:** desempeñar la defensa oportuna y adecuada en todos los asuntos contenciosos de la Entidad, a través de la aplicación de conocimientos lógicos jurídicos, con la finalidad de dar certeza legal a los actos en los que intervenga.
- **Subgerencia de Normatividad y Acceso a la Información:** instruir, coordinar y supervisar las acciones y procedimientos para asegurar la mayor eficacia en materia de acceso a la información, promoviendo la capacitación y actualización del personal de la entidad, con el fin de dar cumplimiento a las obligaciones de transparencia y rendición de cuentas.
- **Departamento de Normatividad, Transparencia y Manejo de Datos Personales:** brindar seguridad jurídica, para todos aquellos actos que deban realizar las unidades administrativas de la entidad, recabando y difundiendo obligaciones de transparencia, con la finalidad de servir como vínculo al recibir y tramitar las solicitudes de acceso a la información y de protección de los datos personales.

- **Subgerencia de Integración de Expedientes Técnicos y Unitarios y Atención a Auditorías:** revisar el cumplimiento normativo y la eficaz integración de expedientes técnicos y unitarios, detectar errores y desviaciones en el cumplimiento de las obligaciones, lo anterior; mediante un seguimiento continuo, permanente y sistemático de las operaciones y actuaciones de la Entidad, para una mejor cultura de transparencia y de evaluación de resultados de la gestión financiera.

III. ANÁLISIS DE RIESGOS

El presente análisis identifica el riesgo inherente a los datos personales en el tratamiento que reciben por la **APITAM** al ejercer sus atribuciones, de manera que pueda ser controlado por la institución para satisfacer el derecho humano a la autodeterminación informativa.

La Ley en sus artículos 27 fracciones IV y V, 29 fracciones III y IV considera que el determinar el riesgo inherente a los datos personales tratados es un deber de los sujetos obligados en la adopción de medidas de seguridad, para lo que deben realizar un análisis que considere las amenazas y vulnerabilidades para los datos, así como los recursos involucrados en el tratamiento.

Con base en la Ley, la valoración de los riesgos de los datos personales forma parte de los elementos mínimos que debe contener el instrumento que describe y da cuenta, en lo general, sobre las medidas de seguridad técnicas, físicas y administrativas adoptadas (Documento de seguridad), en este caso, por **APITAM**, con el propósito de garantizar la confidencialidad, integridad y disponibilidad de ese tipo de datos bajo su posesión.

La seguridad de los datos personales que se tratan en la **APITAM** demanda conocer y entender los riesgos a los que se encuentran expuestos en los distintos procesos que realizan

las unidades administrativas, lo que permitiría afrontarlos de manera adecuada y oportuna.

Para analizar los riesgos de los datos personales que son objeto de tratamiento por **APITAM**, se elaboró un instrumento que, a partir de considerar su objeto y atribuciones constitucionales, clasifica los datos en tres tipos, tal y como ha sido referenciado con antelación.

- 1) De **identificación o contacto**, que se refieren a información por la que se identifica a una persona y/o permiten su contacto como, por ejemplo, el nombre, el domicilio, el correo electrónico, la firma, los usuarios, el Registro Federal de Contribuyentes, la Clave Única de Registro de Población o la edad.
- 2) **Patrimoniales**, que comprenden la información que se encuentran vinculados al patrimonio de una persona como, por ejemplo, el salario, los créditos, las tarjetas de débito, los cheques o las inversiones.
- 3) **Sensibles**, que consideran la información concerniente a la esfera más íntima de su titular o que su uso puede dar origen a discriminación o conlleva un riesgo grave para éste como, por ejemplo, el origen étnico, el estado de salud presente o futuro, las creencias religiosas, la opinión política o la orientación sexual.

IV. ANÁLISIS DE BRECHA

El análisis de brecha permite identificar la distancia que existe entre las medidas recomendadas y las medidas implementadas por cada uno de los tratamientos reportados. Por ejemplo, si se recomienda implementar al tratamiento un conjunto de medidas y el área responsable informa que hacen falta implementar algunas, la identificación de lo que hace falta se conoce como brecha

MEDIDAS DE SEGURIDAD GENERALES

Las medidas generales de seguridad administrativas, físicas y técnicas con las que actualmente cuenta **APITAM** para mantener la confidencialidad e integralidad de la información, así como para proteger los datos personales contra daño, pérdida, destrucción o alteración, así como evitar el uso, acceso o tratamiento no autorizado, e impedir la divulgación no autorizada, son las siguientes:

MEDIDAS ADMINISTRATIVAS

1. Implementación de formatos de entrada y salida de préstamo de documentos por parte del área encargada del archivo.
2. Resguardo de los expedientes bajo los criterios, directrices y lineamientos para la atención de los expedientes técnicos.
3. Suscripción de una carta responsiva por parte de los usuarios o personal con acceso a sistemas de datos personales, acerca del deber de confidencialidad.
4. Reportar al superior jerárquico los incidentes detectados respecto de pérdida o alteración de cualquier documento que contenga datos personales.
5. Reportar a la autoridad competente acerca de la vulneración de datos personales.

MEDIDAS FÍSICAS

1. Resguardo de documentos e información en archivos físicos de trámite y concentración.
2. Disponer de la instalación de chapas con llave para mantener control de acceso de personas a espacios de resguardo de información.
3. Limitar el número de personas con acceso a archivos físicos.
4. Realizar el registro de personas con acceso a espacios físicos en los que se resguarda información con datos personales.
5. Suscribir cartas responsivas de confidencialidad con el personal que trata datos personales.
6. Designación de personal con acceso controlado a espacios de resguardo físico de expedientes y documentos con datos personales.

7. Resguardo de llaves en oficinas de acceso restringido.

MEDIDAS TÉCNICAS

1. Utilizar claves de usuario y contraseñas de manera personal, y evitar compartirlas, prestarlas o registrarlas a la vista de otras personas.
2. Establecer y utilizar contraseñas robustas, es decir, de al menos seis caracteres alfanuméricos y especiales, evitando que sean iguales al nombre del usuario, o cualquier otro nombre de personas, considerando que éstas sean fáciles de recordar y difíciles de adivinar o descifrar por un tercero, a fin de salvaguardar la información y datos personales a los que se tenga acceso.
3. Notificar de manera inmediata al Departamento de Informática los casos en los que los usuarios identifiquen o consideren que sus claves de usuario y/o contraseñas han sido utilizadas por un tercero.
4. Utilizar el correo electrónico para fines relacionados con las actividades laborales, evitando remitir datos personales.
5. Mantener los documentos electrónicos y físicos en lugares seguros, bajo llave, dentro de cajones cerrados, o bajo la protección de alguna contraseña, a fin de promover la restricción a los datos personales que pudieran contener.
6. No difundir, transmitir o compartir documentos electrónicos ni físico que contengan datos personales, a fin de garantizar que estos no sean divulgados de manera no autorizada.
7. Evitar dejar u olvidar los documentos físicos que contengan datos personales en los equipos de impresión, así como evitar su impresión, escaneo y fotocopiado si no es realmente requerido para las actividades laborales.
8. Evitar el acceso a los sistemas de información de tratamiento de datos personales, bajo el precepto del mínimo privilegio; es decir, únicamente al personal que por sus funciones y facultades laborales los requiera, a fin de mantener una adecuada segregación de funciones, restricción de acceso y tratamiento de esos datos.

9. Borrar o eliminar de la papelera de reciclaje del escritorio de los equipos de cómputo los documentos o archivos electrónicos que nos son necesarios para el desarrollo de funciones.
10. Notificar las bajas de accesos a los sistemas de información o de tratamiento de datos personales, con oportunidad, para restringir el acceso a dichos datos por personal no autorizado.

V. PLAN DE TRABAJO

El plan de trabajo para la protección de los datos personales que la Administración Portuaria Integral de Tamaulipas, S.A de C.V. será: cumplir con los principios y deberes de la Ley General de Datos Personales en Posesión de Sujetos Obligados proyecto que se llevará a cabo a través del Comité de Transparencia y Acceso a la Información Pública y que a continuación se enlistan:

1. Se mantendrá actualizado el inventario de datos personales y de los sistemas de tratamiento.
2. Capacitar al personal de la Administración Portuaria Integral de Tamaulipas, S.A de C.V. en materia de datos personales.
3. Implementar medidas de seguridad físicas, administrativas y técnicas para la debida protección de los datos personales.
4. Conformar el documento de seguridad como lo requiere la Ley.
5. Llevar a cabo visitas de seguimiento y de verificación, esto con el objetivo de corroborar el cumplimiento de las obligaciones que marca la Ley General de Datos Personales en Posesión de Sujetos Obligados.
6. Conformar la carpeta de evidencia del cumplimiento de las obligaciones según marca la Ley para que ésta sea revisada y aprobada por Comité de Transparencia y Acceso a la Información Pública.

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

Los Mecanismos de Monitoreo y Revisión (Mecanismos) tienen como objetivo fundamental preservar el nivel de cumplimiento y protección conseguido en la implementación de las medidas de seguridad, además de la mejora de los procesos en el tratamiento de los datos personales (artículo 29, fracción VI de la Ley General). Al respecto, la Ley menciona que, para establecer y mantener las medidas de seguridad para la protección de los datos personales, el responsable deberá monitorear y revisar de manera periódica las medidas de seguridad implementadas, así como las amenazas y vulneraciones a las que están sujetos los datos personales (artículo 27, fracción VII). Por lo anterior, se proponen diversas acciones relacionadas con el monitoreo y la revisión del cumplimiento de los principios y deberes en materia de protección de datos personales, que a continuación se desarrollan.

ACCIÓN 1. AUDITORÍAS Y PROCESOS CON PERSPECTIVA DE DATOS PERSONALES

Es importante una colaboración conjunta entre la **APITAM** y las áreas, con el propósito de dotar de esa perspectiva los procesos de las áreas a través de los cuales se tratan datos personales, advirtiendo sobre las particularidades que presenta el riesgo de vulneración de datos personales.

ACCIÓN 2. ESTRATEGÍA DE EVALUACIÓN INTERNA DE CUMPLIMIENTO

La finalidad es que se tenga mayor presencia en la vigilancia de las actividades que implican tratamientos de datos personales, para resolver dudas, posibles vulneraciones, riesgos, debilidades en los procesos, siempre desde una perspectiva de respeto, responsabilidad y buena fe.

ACCIÓN 3. CUESTIONARIOS DE MONITOREOS

Los cuestionarios de monitoreo han tenido como propósito evaluar el nivel de conocimiento e involucramiento del personal de este **Administración Portuaria Integral de**

Tamaulipas, S. A. de C.V., que interviene en el tratamiento de datos personales en torno a los conceptos y temas en la materia. Tuvieron el carácter de voluntarios, por tanto, las respuestas que se registraron fueron anónimas. Derivado de la alta respuesta por parte de todas las personas que intervienen en el tratamiento de datos personales.

VII. PROGRAMA GENERAL DE CAPACITACIÓN EN DATOS PERSONALES

El programa de capacitación es una de las medidas de seguridad administrativa del tipo preventivo, efectiva y eficiente, en razón de que, permite que el tratamiento de datos personales se haga de una manera correcta y se evite el mal uso, sustracción y divulgación.

Ocultamiento, alteración, mutilación, destrucción total o parcial y de manera indebida de datos personales, que pongan en peligro la confidencialidad, integridad y disponibilidad de la información.

El objetivo principal del programa de capacitación es capacitar y concientizar a las y los servidores públicos de la Administración Portuaria Integral de Tamaulipas, S.A de C.V., en materia de protección de datos personales para el mejor desempeño de sus atribuciones, la especialización de sus funciones, el óptimo cumplimiento de los objetivos institucionales y promoción de la profesionalización en el servicio público.

Es de destacar que la capacitación en términos de protección de la información, permite a las personas identificar el tipo de información que manejan y el nivel de sensibilidad de la misma, además de conocer las mejores prácticas de tratamiento de la información desde el punto de vista de seguridad.

Los planes de capacitación deben diseñarse e instrumentarse de acuerdo con el perfil y las responsabilidades de las personas a lo largo del ciclo de vida de los datos personales. Resulta indispensable la obtención de técnica y perfeccionamiento de buenas prácticas en el

tratamiento de los datos personales para el debido cumplimiento de las atribuciones de todo servidor público dentro de la Administración Portuaria Integral de Tamaulipas, S,A de C.V.

La parte de capacitación se considera una acción sumamente importante dentro del proceso de mejora continua.

Del mismo modo se busca garantizar la protección del tratamiento de los datos personales obtenidos como sujeto obligado, optimizar recursos, maximizar beneficios, establecer directrices para el correcto uso de la información en términos de su seguridad y generar esquemas de capacitación diferenciales e integrales que atiendan los siguientes rubros:

- Desarrollar los niveles de competencias laborales a través del perfeccionamiento de conocimientos, habilidades, actitudes y valores.
- Elevar los niveles de apropiación del conocimiento en materia de protección de datos personales.
- Establecer herramientas para realizar un efectivo tratamiento de datos personales y el ejercicio de los derechos de acceso, rectificación, cancelación y oposición (ARCO).
- Garantizar la observancia de los principios de protección de datos personales previstos en la Ley y demás disposiciones que resulten aplicables en la materia.
- Promover, fomentar y difundir una cultura de protección de datos personales.

Art. 27 fracción VIII de la Ley.