DOCUMENTO DE SEGURIDAD

AEROPUERTOS Y SERVICIOS AUXILIARES

Documento clasificado como parcialmente reservado

Diciembre, 2020

Contenido

Introducción

De acuerdo con la Constitución Política de los Estados Unidos Mexicanos en lo sucesivo la CPEUM, la protección de datos personales es un derecho fundamental, que involucra a todas las personas y por el cual los titulares tienen el derecho a que sea respetado por los responsables en el tratamiento sea el sector privado o el sector público.

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

Con la entrada en vigor de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (en lo sucesivo Ley General) publicada en el Diario Oficial de la Federación el 26 de enero de 2017 y los Lineamientos Generales de Protección de Datos Personales para el Sector Público (en lo sucesivo Lineamientos Generales), de fecha 26 de enero de 2018, se establecen una serie de obligaciones y deberes para los responsables en el tratamiento de los datos personales.

Con esta normativa se establecen las bases y principios para el correcto ejercicio y protección de los datos personales, con la finalidad de garantizar el derecho a la protección de datos personales y que el titular tenga el control sobre sus datos personales, para que los responsables que utilizan datos en el desarrollo de sus actividades no afecten a los titulares.

La protección de datos personales es considerado un derecho humano en nuestra legislación, y como parte fundamental encontramos a la autodeterminación informativa que es el derecho que tiene cada persona a decidir qué información dar, a cambiar, modificar o suprimir los datos personales que le atañen de cualquier base de datos. La autodeterminación informativa se puede entender como la capacidad que tenemos para decidir sobre quién y cuáles son los datos que autorizamos sean utilizados, así como, las finalidades en donde señalamos de forma específica para que objetivo entregamos nuestros datos personales.

De acuerdo con la Ley General y los Lineamientos Generales, todas las dependencias y entidades de la administración pública federal son considerados sujetos obligados, que al realizar el tratamiento de datos personales adquieren el carácter de "Responsables", por lo que deberán realizar el tratamiento de los datos personales conforme a los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad, así como establecer y las medidas de seguridad de carácter administrativo, físico y técnico para garantizar la confidencialidad, integridad y disponibilidad de los datos personales.

Aeropuertos y Servicios Auxiliares (en lo sucesivo ASA) es un organismo descentralizado, con personalidad jurídica y patrimonio propios de conformidad con el artículo 1 del DECRETO por el que se modifica el similar que creó al organismo público descentralizado Aeropuertos y Servicios Auxiliares publicado en el Diario Oficial de la Federación el 22 de agosto de 2002, que tiene como objeto entre otras, administrar, operar, conservar, explotar, y, en su caso, construir mantener, ampliar y reconstruir aeropuertos y aeródromos civiles nacionales; realizar la compraventa y prestar

los servicios de abastecimiento y succión de combustibles en los aeropuertos; prestar servicios aeroportuarios, complementarios y comerciales; proporcionar y administrar servicios auxiliares de transporte de pasajeros entre los aeropuertos y las zonas urbanas y establecer terminales de concentración de aeropuertos; desarrollar y transferir tecnología en materia aeroportuaria, así como llevar a cabo investigaciones para desarrollo tecnológico o profesional; recibir y prestar los servicios que puedan ser requerido para llevar a cabo su objeto y en general servicios de consultoría, asesoría, asistencia técnica en materia aeroportuaria a nivel nacional o internacional, y en general llevar a cabo y ejecutar todos los actos, contratos, convenios, operaciones y transacciones relacionadas, incidentales o accesorias para el desarrollo de su objeto.

ASA es un sujeto obligado con el carácter de *Responsable* en el tratamiento de los datos personales en ejercicio de sus atribuciones y funciones. De acuerdo a lo dispuesto en el artículo 31 de la Ley General, los responsables deben establecer y mantener las medidas de seguridad de carácter físico, administrativo y técnico para la protección de datos personales. De esta manera, una de las obligaciones que impone la Ley General para dar cumplimiento al deber de seguridad, es la elaboración del denominado "Documento de Seguridad" de conformidad a lo dispuesto en el artículo 35 de la citada ley.

Asimismo, el numeral 83 de la Ley General, señala que el Comité de Transparencia es la autoridad máxima en materia de protección de datos personales. Dentro de las atribuciones con las que cuenta el Comité de Transparencia se encuentran el coordinar, supervisar y realizar las acciones necesarias para garantizar el derecho a la protección de los datos personales en la organización del responsable, supervisar, en coordinación con las áreas o unidades administrativas competentes, el cumplimiento de las medidas, controles y acciones previstas en el documento de seguridad y establecer programas de capacitación y actualización para los servidores públicos en materia de protección de datos personales.

De acuerdo con el artículo 35 la Ley General, el documento de seguridad debe contener al menos la siguiente información:

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, y
VII. El programa general de capacitación.

Los cuales se señalan en su respectivo capitulo, con las definiciones específicas, su conformación y las acciones que deberán implementar.

Marco Normativo

Para efectos del presente documento de seguridad, la normatividad aplicable es la siguiente:

- Artículos 6 y 16 de la Constitución Política de los Estados Unidos Mexicanos.
- Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados publicados en el Diario Oficial de la Federación el 26 de enero de 2017.
- Ley General de Transparencia y Acceso a la Información Pública, última reforma publicada el 13 de agosto de 2020 en el Diario Oficial de la Federación.
- Ley Federal de Transparencia y Acceso a la Información Pública, última reforma publicada el 27 de enero de 2017 en el Diario Oficial de la Federación.
- Lineamientos Generales de Protección de Datos Personales para el Sector Público, publicados en el Diario Oficial de la Federación el 26 de enero de 2018.
- Estatuto Orgánico de Aeropuertos y Servicios Auxiliares publicado en el Diario Oficial de la Federación el 23 de diciembre de 2011.
- Decreto por el que se modifica el similar que creó al organismo público descentralizado Aeropuertos y Servicios Auxiliares
- Ley de Aeropuertos.
- Reglamento de la Ley de Aeropuertos.

Ámbito de aplicación

Ámbito de aplicación objetivo:

El presente documento de seguridad será aplicable al tratamiento de datos personales físico o automatizado que lleven a cabo las unidades administrativas de ASA.

Para tal efecto, de conformidad con el artículo 3, fracción IX de la Ley General, se entenderá por dato personal: cualquier información concerniente a una persona física identificada o identificable. Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información.

Los datos personales pueden ser expresados en cualquier forma numérica, alfanumérica fotográfica o acústica.

Ámbito de aplicación subjetivo:

Será de observancia obligatoria a todos los servidores públicos que en el desarrollo de sus atribuciones, traten datos personales.

De acuerdo con la Ley General, se entiende por 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.

Como se ha señalado de acuerdo a las obligaciones, como servidores públicos que tengan acceso a los datos personales, está el conocer y aplicar las medidas de seguridad.

Desarrollo

El deber de seguridad, consiste sin importar el sistema en el que se encuentren los datos personales, en la implementación de medidas de seguridad físicas, técnicas y administrativas necesarias para proteger los datos personales contra daño, pérdida, alteración, destrucción, o su uso, acceso o tratamiento no automatizado, así como para garantizar su confidencialidad, integridad y disponibilidad.

Las medidas de seguridad, de acuerdo con el artículo 3 fracción XX de la Ley General, son el conjunto de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permitan proteger los datos personales.

Las medidas de **seguridad administrativas** refieren a las 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.

Por su parte, las **medidas de seguridad físicas** son el conjunto de acciones y mecanismos para proteger el entorno físico de los datos personales y de los recursos involucrados en su tratamiento. De manera enunciativa más no limitativa, se deben considerar las siguientes actividades:

a) Prevenir el acceso no autorizado al perímetro de la organización, sus instalaciones físicas, áreas críticas, recursos e información;
b) Prevenir el daño o interferencia a las instalaciones físicas, áreas críticas de la organización, recursos e información;
c) Proteger los recursos móviles, portátiles y cualquier soporte físico o electrónico que pueda salir de la organización, y
d) Proveer a los equipos que contienen o almacenan datos personales de un mantenimiento eficaz, que asegure su disponibilidad e integridad.

Asimismo, las medidas de **seguridad técnicas** abarcan el 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.

De manera enunciativa más no limitativa, se deben considerar las siguientes actividades:

a) Prevenir que el acceso a las bases de datos o a la información, así como a los recursos, sea por usuarios identificados y autorizados;
b) Generar un esquema de privilegios para que el usuario lleve a cabo las actividades que requiere con motivo de sus funciones;
c) Revisar la configuración de seguridad en la adquisición, operación, desarrollo y mantenimiento del software y hardware, y
d) Gestionar las comunicaciones, operaciones y medios de almacenamiento de los recursos informáticos en el tratamiento de datos personales.

Este deber deberá observarse durante todo el ciclo de vida de los datos personales, desde su obtención hasta su eliminación. Asimismo, de conformidad con el artículo 35 de la Ley General, el responsable deberá elaborar un documento de seguridad, el cual deberá contener, al menos, la siguiente información:

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, y
VII. El programa general de capacitación.

Para la elaboración del **documento de seguridad**, la Unidad de Transparencia en coordinación con las Unidades Administrativas del Organismo que tratan datos personales, realizó un inventario de tratamiento de datos personales, en el cual se menciona el objetivo, finalidad y fundamento legal para llevar a cabo el tratamiento de datos personales.

Es esencial continuar con el trabajo en conjunto entre la Unidad de Trasparencia y las áreas responsables, para sensibilizar sobre la obligación de contar con un documento de seguridad y los instrumentos que lo conforman, conocer los requisitos normativos y la metodología que se debe llevar a cabo respecto a los sistemas de tratamiento de datos personales.

Son necesarias las acciones de capacitación, así como la revisión sobre la implementación y actualización de las medidas de seguridad, basado en la identificación de las medidas de seguridad existentes y la determinación de las medidas de seguridad faltantes y que deberán implementarse.

I. Inventario de datos personales y de los sistemas de tratamiento

La elaboración del inventario de datos personales, es una obligación que tienen todos los sujetos obligados que realizan el tratamiento de datos personales de conformidad con el artículo 33, fracción III y 35, fracción I de Ley General, y el artículo 58 de los Lineamientos Generales.

Para el debido cumplimiento de las obligaciones que se establecen en la Ley General, es necesario contar con el Inventario para realizar un diagnóstico de las siguientes obligaciones:

- Descripción de las obligaciones
- Actividades a realizar para cumplirlas
- Artículos de la Ley General y de los Lineamientos Generales de los que derivan
- Unidad administrativa responsable del cumplimiento
- Listado de comprobación del estado de cumplimiento

La primera acción consistió en identificar exclusivamente aquellos sistemas de tratamiento que manejan datos personales. Todos aquellos sistemas de tratamiento que no manejan datos personales, no forman parte de este procedimiento y para fines del presente documento de seguridad no es necesario inventariarlos. También se señalan los soportes físicos, tales como archiveros, gavetas, anaqueles y bodegas en los cuales se procesan y almacenan dichos datos. Y los soportes electrónicos, tales como aplicaciones, bases de datos, unidades de almacenamiento, equipos y toda aquella infraestructura tecnológica en los cuales se procesan y almacenan dichos datos.

Las preguntas sobre los cuales está conformado el inventario de datos personales son las siguientes:

1. Medio de obtención de los datos personales.
2. Tercero que transfiere los datos personales, en su caso.
3. Finalidades de la transferencia recibida, en su caso.
4. Listado de datos personales.
5. Usa Datos "Sensibles".
6. Formato de la base de datos.
7. Ubicación base de datos.
8. Sección de archivos.
9. Serie de archivos.
10. Subserie de archivos.
11. Finalidades del tratamiento.
12. ¿Requiere consentimiento?
13. Supuesto artículo 22 de la Ley General que se actualiza, en su caso
14. Tipo de consentimiento.
15. Servidores públicos que tienen acceso a la base de datos.
16. Área de adscripción.
17. Finalidad del acceso.
18. Nombre del encargado, en su caso.

19. No. de contrato, pedido o convenio con el encargado, o del instrumento jurídico correspondiente.
20. ¿Se realizan transferencias?
21. Tercero al que se transfieren los datos personales, en su caso.
22. Finalidades de la transferencia.
23. ¿Requiere consentimiento la transferencia?
24. Supuestos previsto en los artículos 22, 66 o 70 de la Ley General que se actualizan, en su caso.
25. Tipo de consentimiento que se requiere para la transferencia.
26. ¿La transferencia requiere la suscripción de cláusulas contractuales, convenios de colaboración u otro instrumento jurídico?
27. Supuesto previsto en el artículo 66 de la Ley General, que se actualiza, en su caso.
28. Difusión de los datos personales.
29. Fundamento jurídico para la difusión.
30. Plazo de conservación.
31. Bloqueo.

A las Unidades Administrativas que realizan el tratamiento de datos personales, les fue informada la necesidad de realizar un diagnóstico de los tratamientos de datos personales que llevan a cabo, lo anterior en razón que son las mismas áreas administrativas quienes conocen y realizan directamente el tratamiento de los datos personales.

De acuerdo a las Unidades Administrativas que conforman el Organismo, en quince de ellas se identificaron tratamientos de datos personales, los cuales se señalan a continuación:

1. Subdirección de Comunicación Corporativa

1.1 Tratamiento para el uso de imagen de los titulares.
1.2 Tratamiento para la contratación de medios de comunicación y de agencias de investigación que brinden servicios de difusión y elaboración de estudios para las campañas de aeropuertos y servicios auxiliares.
1.3 Tratamiento para representantes de medios de comunicación que cubren actividades de aeropuertos y servicios auxiliares.

2. Subdirección de Operaciones y Servicios (Aeropuertos).

2.1 Tratamiento para concursantes en el procedimiento de licitación.
2.2 Tratamiento para el registro de entradas y salidas de las instalaciones.
2.3 Tratamiento para personal de ASA en Aeropuertos.
2.4 Tratamiento para el procedimiento de licitación

3. Gerencia de Seguridad

3.1 Tratamiento de datos personales para concursantes en el procedimiento de licitación.
3.2 Tratamiento de datos personales para el procedimiento de licitación.

4. Gerencia de Gestión Operativa

4.1 Tratamiento de datos personales para la Adquisición de Bienes y Servicios en la Gerencia de Gestión Operativa.
4.2 Tratamiento de datos personales para contacto con posibles proveedores para la Adquisición de Bienes y Servicios en la Gerencia de Gestión Operativa.
4.3 Tratamiento de datos personales para el procedimiento de contratación y pago a proveedores en la Gerencia de Gestión Operativa.

5. Jefaturas Estaciones de Combustibles

5.1 Tratamiento de datos personales para concursantes en el procedimiento de licitación.
5.2 Tratamiento de datos personales para el procedimiento de licitación.
5.3 Tratamiento de datos personales para el procedimiento de contratación y pago a proveedores

6. Gerencia de Ingeniería

6.1 Tratamiento de datos personales para concursantes en el procedimiento de licitación.
6.2 Tratamiento de datos personales para el procedimiento de licitación.

7. Gerencia de Análisis Operacional

7.1 Tratamiento de datos personales para concursantes en el procedimiento de licitación.
7.2 Tratamiento de datos personales para el procedimiento de licitación.

8. Gerencia del Centro Internacional de Instrucción ASA (CIIASA)

8.1 Tratamiento de datos personales para posibles candidatos a capacitación en el CIIASA.
8.2 Tratamiento de datos personales para certificaciones, capacitación y cursos.

9. Gerencia de Innovación y Desarrollo Tecnológico

9.1 Tratamiento de datos personales para concursantes en el procedimiento de licitación.
9.2 Tratamiento de datos personales para el procedimiento de licitación.
9.3 Tratamiento de datos personales para el registro de productos, proyectos y obras de la propiedad industrial e intelectual

10. Gerencia de Administración de Recursos Humanos

10.1 Tratamiento de datos personales para el Centro de Desarrollo Infantil de Aeropuertos y Servicios Auxiliares.
10.2 Tratamiento de datos personales para el personal de Aeropuertos y Servicios Auxiliares.
10.3 Tratamiento de datos personales para la selección y reclutamiento en Aeropuertos y Servicios Auxiliares.
10.4 Tratamiento de datos personales para la atención del servicio médico.
10.5 Tratamiento de datos personales para prestadores de servicio social y prácticas profesionales.

11. Gerencia de Recursos Materiales

11.1 Tratamiento de datos personales para contacto con posibles proveedores para la Adquisición de Bienes y Servicios en la Gerencia de Recursos Materiales.
11.2 Tratamiento de datos personales para el procedimiento de contratación y pago a proveedores en la Gerencia de Recursos Materiales

12. Gerencia de Licitaciones

12.1 Tratamiento de datos personales para concursantes en el procedimiento de licitación.
12.2 Tratamiento de datos personales para el procedimiento de licitación.

13. Gerencia de Ingresos

13.1 Tratamiento de datos personales para la promoción de servicios aeroportuarios.
13.2 Tratamiento de datos personales para servicios aeroportuarios y complementarios.

14. Subdirección de Informática

14.1 Tratamiento de datos personales para concursantes en el procedimiento de licitación.
14.2 Tratamiento de datos personales para el procedimiento de licitación.

15. Unidad de Transparencia

15.1 Tratamiento de datos personales para solicitantes de acceso a la información y solicitudes de atención a derechos ARCO.

Debido al volumen de los treinta y ocho inventarios del tratamiento de datos personales que forman parte del documento de seguridad, se integran como **ANEXO 1** del presente documento.

II. Las funciones y obligaciones de las personas que traten datos personales

De acuerdo con los deberes y obligaciones a que se refiere la Ley General, todas las Unidades Administrativas que realicen el tratamiento de datos personales en el ejercicio de sus atribuciones y funciones deben cumplir con la normativa en la materia de protección de datos personales.

Los servidores públicos involucrados en el tratamiento de datos personales deben cumplir, entre otros con el deber de confidencialidad. Aun cuando dejen de prestar sus servicios en el Organismo o sean cambiados de unidad administrativa, deberán guardar secrecía absoluta.

Es importante señalar que el Organismo deberá establecer y documentar los roles y responsabilidades, así como la parte correspondiente a la rendición de cuentas de todas las personas que traten datos personales.

También se debe implementar al interior del Organismo, un mecanismo para asegurar que todas las personas involucradas en el tratamiento de datos personales conozcan sus funciones para el cumplimiento de los objetivos y las consecuencias de su incumplimiento.

a) Por lo que los involucrados en el tratamiento de datos personales deben estar conscientes de la importancia de:

- Cumplir la política de gestión de datos personales;
- Conocer los objetivos del Sistema de Gestión para la Seguridad de Datos Personales en el Organismo, y
- Mejorar el Sistema de Gestión para la Seguridad de Datos Personales en el Organismo de manera continua;

b) Definir los roles, responsabilidades, cadena de rendición de cuentas y estructura organizacional para el Sistema de Gestión para la Seguridad de Datos Personales en el Organismo, y

c) Asegurar que todos los servidores públicos tengan claro sus roles y funciones, así como su contribución para el logro de los objetivos del Organismo y las consecuencias del incumplimiento.

A continuación, se señalan las funciones y obligaciones de los servidores públicos que realizan el tratamiento de datos personales de acuerdo a lo señalado por las Unidades Administrativas que fueron previamente identificadas.

1. Subdirección de Comunicación Corporativa

Nombre del Tratamiento	1.1 Tratamiento para el uso de imagen de los titulares. 1.2 Tratamiento para la contratación de medios de comunicación y de agencias de investigación que brinden servicios de difusión y elaboración de estudios para las campañas de aeropuertos y servicios auxiliares. 1.3 Tratamiento para representantes de medios de comunicación que cubren actividades de aeropuertos y servicios auxiliares.
Puesto/Perfil	Funciones y Obligaciones
Subdirección de Comunicación Corporativa	I. Recibir, controlar y almacenar la correspondencia interna propia de la Subdirección. II. Supervisar el archivo de la Subdirección. III. Supervisar la recepción y remisión de información electrónica vía correo electrónico. IV. Atender las necesidades del personal adscrito a la Subdirección de Comunicación Corporativa. V. Autorizar las publicaciones en los medios de comunicación. VI. Supervisar y autorizar el uso de imagen de personas. VII. Autorizar la contratación con medios de comunicación. VIII. Supervisión y seguimiento para el envío de información e invitaciones a eventos, a representantes de medios de comunicación que cubren actividades del Organismo.
Puesto/Perfil	Funciones y Obligaciones
Gerencia de Vinculación	I. Apoyar en el control y almacenamiento de la correspondencia interna propia de la Subdirección. II. Apoyar con la recepción y remisión de información electrónica vía correo electrónico. III. Supervisar, tanto el contenido de las publicaciones del Organismo como las labores de redacción y edición de los mismos (Página Web, Portal Interno, Publicaciones, Comunicados y Boletines) IV. Recopilar y revisar documentación para el uso de imagen de personas. V. Revisar la documentación para la autorización de contratación con medios de comunicación. VI. Apoyo para el envío de información e invitaciones a eventos, a representantes de medios de comunicación que cubren actividades de Aeropuertos y Servicios Auxiliares.
Puesto/Perfil	Funciones y Obligaciones
Subcoordinación de Servicios Especializados Aeroportuarios	I. Apoyar en el control y almacenamiento de la correspondencia interna propia de la Subdirección. II. Apoyar con la recepción y remisión de información electrónica vía correo electrónico. III. Elaborar las publicaciones en los medios de comunicación. IV. Recopilar y revisar documentación para el uso de imagen de personas. V. Revisar la documentación para la autorización de contratación con medios de comunicación. VI. Apoyo para el envío de información e invitaciones a eventos, a representantes de

	medios de comunicación que cubren actividades de aeropuertos y servicios auxiliares.

2. Subdirección de Operaciones y Servicios (Administraciones Aeroportuarias).

Nombre del Tratamiento	2.1 Tratamiento para concursantes en el procedimiento de licitación. 2.2 Tratamiento para el registro de entradas salidas de las instalaciones. 2.3 Tratamiento para personal de ASA en Aeropuertos. 2.4 Tratamiento para el procedimiento de licitación.
Nombre del Puesto/Perfil	Funciones y Obligaciones
Administrador Aeroportuario	I. Supervisar que se apliquen las disposiciones generales en la prestación de los servicios, de acuerdo con las condiciones de los contratos suscritos en los aeropuertos. II. Coordinar con los administradores de aeropuertos la adecuada prestación de servicios, la eficiente y eficaz operación y la estricta aplicación de la normatividad vigente. III. Evaluar que las actividades y capacidades del personal asignado en los aeropuertos cumplan con lo establecido en la normatividad, manuales, guías y procedimientos que correspondan. IV. Supervisar la operación y administración de los aeropuertos. V. Coordinar el funcionamiento del aeropuerto a su cargo, contemplando los aspectos de conservación y mantenimiento de edificios, equipos en general, estaciones de combustibles y áreas operacionales. VI. Administrar y coordinar las relaciones y actividades del personal, a efecto de que éstos desempeñen su trabajo con responsabilidad y eficiencia. VII. Supervisar, coordinar y autorizar los procedimientos de licitación para la prestación de bienes o servicios.
Nombre del Puesto/Perfil	Funciones y Obligaciones
Jefe de Mantenimiento y/o Análogo.	I. Apoyar en la prestación de los servicios, de acuerdo con las condiciones de los contratos suscritos en los aeropuertos. II. Auxiliar en la evaluación de las actividades y capacidades del personal asignado en los aeropuertos. III. Concentrar la documentación para reclutamiento y selección de personal, conforme a los requerimientos de recursos humanos. IV. Colaborar en los procedimientos de licitación para la prestación de bienes o servicios. V. Participar en la integración de las investigaciones de mercado y evaluación de propuestas, para la formalización de contratos VI. Digitalizar todos los escritos, así como sus anexos.

3. Gerencia de Seguridad

Nombre del Tratamiento	3.1 Tratamiento de datos personales para concursantes en el procedimiento de licitación. 3.2 Tratamiento de datos personales para el procedimiento de licitación.
Nombre del Puesto/Perfil	Funciones y Obligaciones
Gerente de Seguridad	I. Establecer los programas de capacitación para el personal de los aeropuertos en materia de seguridad operacional, seguridad de la aviación civil, servicios de salvamento y extinción de incendios, protección civil, emergencias y supervisar su aplicación, para asegurar que se encuentren en condiciones de salvaguardar la integridad de las personas, instalaciones y equipos. II. Participar en el desarrollo y seguimiento de los cambios en los procesos, nuevos proyectos y licitaciones, para asegurar el cumplimiento de la normatividad nacional e internacional y requerimientos en materia de seguridad operacional y protección civil aplicable en los aeropuertos y las estaciones de combustibles. III. Supervisar, coordinar y autorizar los procedimientos de licitación para la prestación de bienes o servicios.
Nombre del Puesto/Perfil	Funciones y Obligaciones
Jefe de Departamento y/o Análogo	I. Elaborar, documentar y apoyar en los programas de capacitación para el personal de los aeropuertos en materia de seguridad operacional, seguridad de la aviación civil, servicios de salvamento y extinción de incendios, protección civil, emergencias y supervisar su aplicación, para asegurar que se encuentren en condiciones de salvaguardar la integridad de las personas, instalaciones y equipos. II. Proporcionar, documentar y preparar la información para los procesos, nuevos proyectos y licitaciones, que lleve a cabo la Gerencia de Seguridad. III. Colaborar en la integración de las investigaciones de mercado y evaluación de propuestas, para la formalización de contratos. IV. Digitalizar todos los escritos, así como sus anexos.

4. Gerencia de Gestión Operativa

Nombre del Tratamiento	4.1 Tratamiento de datos personales para la Adquisición de Bienes y Servicios en la Gerencia de Gestión Operativa. 4.2 Tratamiento de datos personales para contacto con posibles proveedores para la Adquisición de Bienes y Servicios en la Gerencia de Gestión Operativa.

	4.3 Tratamiento de datos personales para el procedimiento de contratación y pago a proveedores en la Gerencia de Gestión Operativa.
Nombre del Puesto/Perfil	Funciones y Obligaciones
Gerente de Gestión Operativa	I. Asegurar la provisión de recursos para la adquisición de materiales, equipo, servicios y demás elementos indispensables para garantizar la calidad del producto y la adecuada operación de las Estaciones de Combustibles. II. Planear las adquisiciones de los elementos filtrantes y materiales necesarios, utilizados como insumos por las Estaciones de Combustibles a nivel nacional, a fin de contar con el aprovisionamiento oportuno para realizar las pruebas de control de calidad, de acuerdo a la normatividad aplicable en la materia. III. Verificar que la información de los sistemas de gestión, procedimientos administrativos, inversiones, que sirve de apoyo en contrataciones en las Estaciones de Combustibles se encuentre actualizada y disponible. IV. Supervisar, coordinar y autorizar los procedimientos de licitación para la prestación de bienes o servicios.
Nombre del Puesto/Perfil	Funciones y Obligaciones
Jefe de Departamento y/o Análogo.	I. Coadyuvar en la provisión de recursos para la adquisición de materiales, equipo, servicios y demás elementos indispensables para garantizar la calidad del producto y la adecuada operación de las Estaciones de Combustibles. II. Apoyar en la verificación de la información de los sistemas de gestión, procedimientos administrativos, inversiones, que sirve de apoyo en contrataciones en las Estaciones de Combustibles se encuentre actualizada y disponible. III. Proporcionar, documentar y preparar la información para los procesos, nuevos proyectos y licitaciones, que lleve a cabo la Gerencia de Gestión Operativa. IV. Colaborar en la integración de las investigaciones de mercado y evaluación de propuestas, para la formalización de contratos. V. Digitalizar todos los escritos, así como sus anexos.

5. Jefaturas Estaciones de Combustibles

Nombre del Tratamiento	5.1 Tratamiento de datos personales para concursantes en el procedimiento de licitación. 5.2 Tratamiento de datos personales para el procedimiento de licitación. 5.3 Tratamiento de datos personales para el procedimiento de contratación y pago a proveedores.

Nombre del Puesto/Perfil	Funciones y Obligaciones
Jefe de Estación de Combustibles	I. Administrar, operar y conservar las instalaciones de la planta de almacenamiento de combustibles, equipo de suministro, recursos humanos, recursos materiales y demás recursos disponibles a fin de proporcionar un servicio oportuno, eficiente y seguro, en la estación de combustibles de los aeropuertos que no pertenezcan a la Red de ASA. II. Coordinar, administrar y supervisar los movimientos financieros, presupuestales, de tesorería, cobranza, depósitos, compras y adquisiciones, almacenes, bienes muebles, personal, manejo de fondos y demás, necesarios para el funcionamiento eficiente de la Estación. III. Representar al Organismo ante las dependencias y entidades de la Administración Pública Federal competentes, atendiendo trámites, solicitudes y observaciones resultantes. IV. Coordinar y autorizar los procedimientos de licitación para la prestación de bienes o servicios.
Nombre del Puesto/Perfil	Funciones y Obligaciones
Jefe de Mantenimiento y/o Análogo.	I. Apoyar en la operación y administración de la planta de almacenamiento de combustibles. II. Auxiliar en la administración de actividades financieras, presupuestales, de tesorería, cobranza, depósitos, compras y adquisiciones, almacenes, bienes muebles, personal, manejo de fondos. III. Colaborar en los procedimientos de licitación para la prestación de bienes o servicios. IV. Digitalizar todos los escritos, así como sus anexos.

6. Gerencia de Ingeniería

Nombre del Tratamiento	6.1 Tratamiento de datos personales para concursantes en el procedimiento de licitación. 6.2 Tratamiento de datos personales para el procedimiento de licitación.
Nombre del Puesto/Perfil	Funciones y Obligaciones
Gerente de Ingeniería	I. Programar y asegurar que se cuente con los recursos materiales y económicos necesarios para el desarrollo de los estudios y/o proyectos a través de la planeación del desarrollo de las Estaciones de Combustibles y que son necesarios para la posterior ejecución de las obras o las adquisiciones de equipos. II. Elaborar las especificaciones, criterios y prácticas recomendadas que sean necesarias, a fin de integrarlas a los marcos de referencia y las bases de licitación para concursar los proyectos y obras mayores de las Estaciones de Combustibles, de acuerdo al calendario y los

	plazos establecidos. III. Coordinar con la Gerencia de Obras, el concurso y contratación de los servicios profesionales necesarios para la realización de los proyectos. IV. Coordinar y autorizar los procedimientos de licitación para la prestación de bienes o servicios.
Nombre del Puesto/Perfil	Funciones y Obligaciones
Jefe de Departamento y/o Análogo.	I. Documentar y apoyar en el desarrollo de los estudios y/o proyectos a través de la planeación del desarrollo de las Estaciones de Combustibles y que son necesarios para la posterior ejecución de las obras o las adquisiciones de equipos. II. Proponer especificaciones, criterios y prácticas recomendadas que sean necesarias, a fin de integrarlas a los marcos de referencia y las bases de licitación para concursar los proyectos y obras mayores de las Estaciones de Combustibles. IV. Atender las solicitudes para los concursos y contratación de los servicios profesionales necesarios para la realización de los proyectos. V. Colaborar en los procedimientos de licitación para la prestación de bienes o servicios. VI. Digitalizar todos los escritos, así como sus anexos.

7. Gerencia de Análisis Operacional

Nombre del Tratamiento	**7.1 Tratamiento de datos personales para concursantes en el procedimiento de licitación.** **7.2 Tratamiento de datos personales para el procedimiento de licitación.**
Nombre del Puesto/Perfil	Funciones y Obligaciones
Gerente de Análisis Operacional	I. Determinar las actividades requeridas para implementar los sistemas administrativos, de seguridad y de gestión de la calidad, aplicando su marco normativo nacional e internacional, y en las materias de salud ocupacional y protección del medio ambiente, además de recomendar las nuevas tecnologías en el manejo y suministro de combustibles de aviación y analizar las tendencias de la industria aeronáutica, para reaccionar oportunamente ante los posibles cambios. II. Coordinar los marcos de referencia y las bases de concurso, y supervisar la licitación y contratación de los equipos y de los servicios destinados al logro de los objetivos de la Dirección de Combustibles. III. Coordinar y autorizar los procedimientos de licitación para la prestación de bienes o servicios.
Nombre del Puesto/Perfil	Funciones y Obligaciones

Jefe de Departamento y/o Análogo.	I. Documentar y apoyar en las actividades necesarias para implementar los sistemas administrativos, de seguridad y de gestión de la calidad, aplicando su marco normativo nacional e internacional, y en las materias de salud ocupacional y protección del medio ambiente, además de recomendar las nuevas tecnologías en el manejo y suministro de combustibles de aviación y analizar las tendencias de la industria aeronáutica, para reaccionar oportunamente ante los posibles cambios. II. Participar en la elaboración de los marcos de referencia y las bases de concurso, y apoyar en la licitación y contratación de los equipos y de los servicios destinados al logro de los objetivos de la Dirección de Combustibles. III. Colaborar en los procedimientos de licitación para la prestación de bienes o servicios. IV. Digitalizar todos los escritos, así como sus anexos.

8. Gerencia del Centro Internacional de Instrucción ASA (CIIASA)

Nombre del Tratamiento	**8.1 Tratamiento de datos personales para posibles candidatos a capacitación en el CIIASA.** **8.2 Tratamiento de datos personales para certificaciones, capacitación y cursos.**
Nombre del Puesto/Perfil	Funciones y Obligaciones
Director del Centro Internacional de Instrucción ASA.	I. Establecer altos estándares de capacitación para el personal de la industria aérea nacional e internacional que contribuya a mejorar la seguridad y la eficiencia aeronáutica y aeroportuaria. II. Coordinar el diseño de la oferta educativa del Centro Internacional de Instrucción de ASA para satisfacer las necesidades de formación de autoridades y de los profesionales de la industria aeronáutica y aeroportuaria. III. Establecer a nivel nacional e internacional, convenios de colaboración para el desarrollo de programas de capacitación que atiendan las necesidades de la sociedad y de las instituciones y empresas públicas o privadas.
Nombre del Puesto/Perfil	Funciones y Obligaciones
Gerente del Centro Internacional de Instrucción ASA.	I. Coordinar la capacitación dirigida al personal de la industria área, con base en altos niveles de seguridad en eficiencia aeronáutica y aeroportuaria, bajo estándares nacionales e internacionales. II. Diseñar la oferta educativa del Centro Internacional de Instrucción de ASA para satisfacer las necesidades de formación de las autoridades y los profesionales de la industria aeronáutica y aeroportuaria. III. Coordinar la comunicación del Organismo con instituciones públicas, privadas y sociales relacionadas con la capacitación, instrucción y adiestramiento, para la atención de

	asuntos en materia de su competencia y la aplicación de la normatividad en registros y autorizaciones. IV. Coordinar con la Gerencia de Desarrollo e Integración de Recursos Humanos de ASA los programas y eventos internos, para cubrir las necesidades de capacitación e inducción del Organismo. V. Asegurar la formación de instructores y preparadores de cursos especializados. VI. Establecer las normas, políticas, lineamientos y procedimientos en materia de capacitación y desarrollo para el personal del Organismo. VII. Llevar a cabo la difusión y comercialización de los diplomados, cursos, talleres y conferencias en las materias especializadas de seguridad de la aviación civil/facilitación, seguridad operacional, así como factor y desarrollo humano, impartidos por el Centro Internacional de Instrucción de Aeropuertos y Servicios Auxiliares (CIIASA). VIII. Proveer los servicios y productos de formación, instrucción y capacitación, informar sobre cambios o nuevos productos o servicios, así como establecer comunicación con el participante para aclarar dudas sobre sus datos ya sea por algún error o imprecisión, notificarle la cancelación o cambio de horario y/o de fecha y/o sede de los servicios o dar seguimiento a la conclusión de los mismos. IX. Elaboración o emisión de los certificados, constancias o documentos respectivos. X. Integrar un sistema de registro y control de personas asistentes a los diplomados, cursos, talleres y conferencias en las materias especializadas de seguridad de la aviación civil/facilitación, seguridad operacional, así como factor y desarrollo humano, impartidos por el Centro Internacional de Instrucción de Aeropuertos y Servicios Auxiliares (CIIASA). IX. Generar estadísticas, informes y evaluaciones de los programas de la formación, instrucción y capacitación impartida, hábitos de consumo y necesidades de capacitación.

9. Gerencia de Innovación y Desarrollo Tecnológico

Nombre del Tratamiento	**9.1 Tratamiento de datos personales para concursantes en el procedimiento de licitación.** **9.2 Tratamiento de datos personales para el procedimiento de licitación.** **9.3 Tratamiento de datos personales para el registro de productos, proyectos y obras de la propiedad industrial e intelectual.**
Nombre del Puesto/Perfil	Funciones y Obligaciones
Gerente de Innovación y Desarrollo Tecnológico	I. Coordinar la innovación y el desarrollo tecnológico y generar proyectos y productos que contribuyan a satisfacer las necesidades del Organismo y de la industria aeronáutica y

	aeroportuaria nacional e internacional. II. Asegurar la obtención de los títulos de registro de la propiedad industrial de productos, marcas, patentes y servicios del Organismo. III. Participar en la elaboración de convenios de desarrollo tecnológico e innovación con empresas e instituciones nacionales y extranjeras IV. Participar con el área correspondiente en el proceso de licitaciones públicas nacionales e internacionales en la elaboración de dictámenes técnicos del mobiliario y equipos adquiridos para las diferentes áreas del Organismo.
Nombre del Puesto/Perfil	Funciones y Obligaciones
Jefe de Departamento y/o Análogo.	I. Apoyar en el procedimiento de registro ante el Instituto Mexicano de la Propiedad Industrial de los productos, marcas, patentes y servicios. II. Dar trámite ante el registro de las obras intelectuales ante el Instituto Nacional del Derecho de Autor. III. Proporcionar lo necesario para la elaboración del convenio o cesión de derechos de los proyectos, productos, recursos didácticos y multimedia, así como, obras sujetas a derechos de autor. IV. Coadyuvar en el proceso de pago y facturación por la cesión de derechos del proyecto de desarrollo tecnológico e innovación. V. Colaborar en los procedimientos de licitación para la prestación de bienes o servicios. VI. Digitalizar todos los escritos, así como sus anexos.

10. Gerencia de Administración de Recursos Humanos

Nombre del Tratamiento	**10.1 Tratamiento de datos personales para el Centro de Desarrollo Infantil de Aeropuertos y Servicios Auxiliares.** **10.2 Tratamiento de datos personales para el personal de Aeropuertos y Servicios Auxiliares.** **10.3 Tratamiento de datos personales para la selección y reclutamiento en Aeropuertos y Servicios Auxiliares.** **10.4 Tratamiento de datos personales para la atención del servicio médico.** **10.5 Tratamiento de datos personales para prestadores de servicio social y prácticas profesionales.**
Nombre del Puesto/Perfil	Funciones y Obligaciones
Gerente de Administración de Recursos Humanos	I. Supervisar el cumplimiento de las políticas, normas y procedimientos que en materia de administración de recursos humanos emitan las dependencias globalizadoras, para asegurar su observancia. II. Coordinar la aplicación y evaluación de los programas de recursos humanos, que coadyuven a la eficiencia y productividad laboral. III. Coordinar las actividades de ingreso y

	contratación de personal, para que las áreas del Organismo cuenten con el recurso humano necesario para su operación, vigilando que se cumplan las disposiciones legales en la materia; IV. Coordinar y supervisar los procesos de nómina, seguridad social y control de asistencia, para asegurar que el personal reciba su salario y prestaciones en tiempo y forma, así como cumplir con las obligaciones laborales, fiscales y presupuestales. V. Coordinar las actividades sociales, culturales y deportivas del Organismo, para mantener un espíritu de armonía y colaboración del personal. VI. Coordinar con la Subdirección de Administración, la supervisión de las relaciones laborales con el personal y con el Sindicato de Trabajadores del Organismo. VII. Establecer y evaluar los sistemas de información técnica, estadística y administrativa que generan las áreas dependientes de recursos humanos, para sustentar y fortalecer los procesos de toma de decisiones y en la definición del plan estratégico del Organismo. VIII. Desarrollar las gestiones correspondientes a la aplicación de programas en materia de desarrollo para los servidores públicos, en concordancia con la normatividad en la materia. IX. Supervisar el funcionamiento del Centro de Desarrollo Infantil (CENDI), a fin de crear un ambiente de desarrollo, bienestar y seguridad para los infantes. X. Coordinar la elaboración de los programas de seguridad industrial e higiene conforme a la normatividad vigente, para proteger la integridad física del personal. XI. Supervisar y controlar el presupuesto de servicios personales, a fin de contar con una estructura financiera firme y programada.
Nombre del Puesto/Perfil	Funciones y Obligaciones
Jefe de Departamento y/o Análogo.	I. Integrar el expediente único de posibles candidatos a los perfiles de servidores públicos que se encuentren vacantes y que sean requeridos en las distintas áreas de ASA; acreditar la identidad del solicitante; validar los datos laborales, académicos y años de experiencia de acuerdo al perfil del puesto. II. Apoyar en la Administración de los recursos humanos a través de los procesos de reclutamiento, selección, control, evaluación del desempeño y remuneración. III. Participar el proceso de reclutamiento y selección de personal, conforme a los requerimientos de recursos humanos y con base en los perfiles de los puestos establecidos en la estructura organizacional del Instituto. IV. Documentar y resguardar los expedientes laborales del personal del Instituto; tales como empleados y prestadores de servicios en general. V. Coadyuvar en el control y resguardo de los nombramientos relativos al personal seleccionado y contratado para la integración de la plantilla del Organismo.

Nombre del Puesto/Perfil	Funciones y Obligaciones
Jefe de Departamento y/o Análogo.	I. Prestar en el Centro de Desarrollo Infantil, los servicios educativos y asistenciales a niñas y niños. II. Promover el desarrollo personal del niño a través de situaciones y oportunidades que le permitan ampliar y consolidar su estructura mental, lenguaje, psicomotricidad y afectividad. III. Solicitar los documentos para realizar la inscripción del menor en el Centro de Desarrollo Infantil de Aeropuertos y Servicios Auxiliares (CENDI) y el sistema de la Secretaría de Educación Pública. IV. Integrar el expediente físico del menor, acreditar la identidad de los menores, localización de los padres o tutores y realizar trámites administrativos.
Nombre del Puesto/Perfil	Funciones y Obligaciones
Jefe de Departamento y/o Análogo.	I. Informar al personal sobre temas de prevención de enfermedades generales y de trabajo. II. Apoyar en la capacitación del personal, mediante información sobre seguridad y salud en el trabajo. III. Dar seguimiento a la salud de los trabajadores. IV. Brindar el servicio médico a los trabajadores que así lo soliciten. V. Integrar y elaborar un historial médico que facilite la integración de un diagnóstico clínico integral, que proporcione un tratamiento oportuno y de calidad.

11. Gerencia de Recursos Materiales

Nombre del Tratamiento	**11.1 Tratamiento de datos personales para contacto con posibles proveedores para la Adquisición de Bienes y Servicios en la Gerencia de Recursos Materiales.** **11.2 Tratamiento de datos personales para el procedimiento de contratación y pago a proveedores en la Gerencia de Recursos Materiales.**
Nombre del Puesto/Perfil	Funciones y Obligaciones
Gerente de Recursos Materiales	I. Coordinar y supervisar la integración, elaboración e implementación del programa anual de adquisiciones y de servicios generales, a fin de que sean considerados dentro del presupuesto del Organismo, bajo la normatividad correspondiente. II. Establecer y supervisar el proceso y sistema de adquisiciones de bienes y servicios, de acuerdo con los programas correspondientes para la operación de las áreas del Organismo, conforme a los acuerdos del Comité de Adquisiciones, la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, y demás disposiciones aplicables III. Supervisar el proceso de administración y control de archivos de concentración e histórico

	del Organismo, a fin de garantizar el resguardo y disponibilidad de la documentación, conforme a la normatividad aplicable.
Nombre del Puesto/Perfil	Funciones y Obligaciones
Jefe de Departamento y/o Análogo.	I. Participar en la integración, elaboración e implementación del programa anual de adquisiciones y de servicios generales, a fin de que sean considerados dentro del presupuesto del Organismo, bajo la normatividad correspondiente. II. Apoyar en el proceso y sistema de adquisiciones de bienes y servicios, de acuerdo con los programas correspondientes para la operación de las áreas del Organismo, conforme a los acuerdos del Comité de Adquisiciones, la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, y demás disposiciones aplicables. III. Colaborar en los procedimientos de licitación para la prestación de bienes o servicios. IV. Digitalizar todos los escritos, así como sus anexos.
Nombre del Puesto/Perfil	Funciones y Obligaciones
Jefe de Departamento y/o Análogo.	I. Mantener y operar el proceso de administración y control de archivos de concentración e histórico del Organismo, a fin de garantizar el resguardo y disponibilidad de la documentación, conforme a la normatividad aplicable. II. Colaborar en los procedimientos de licitación para la prestación de bienes o servicios. III. Digitalizar todos los escritos, así como sus anexos.

12. Gerencia de Licitaciones

Nombre del Tratamiento	**12.1 Tratamiento de datos personales para concursantes en el procedimiento de licitación.** **12.2 Tratamiento de datos personales para el procedimiento de licitación.**
Nombre del Puesto/Perfil	Funciones y Obligaciones
Gerente de Licitaciones	I. Coordinar y supervisar la ejecución de las licitaciones para la adquisición de bienes y contratación de servicios, obras y servicios relacionados, apegados a lo que establece la normatividad aplicable. II. Coordinar la preparación de convocatorias y bases para las distintas licitaciones considerando los requerimientos de las áreas usuarias para que sean incorporados en las mismas. III. Autorizar para las licitaciones la publicación de las bases e invitaciones a proveedores, en apego a la normatividad aplicable. IV. Supervisar la apertura de ofertas y el proceso de evaluación de proposiciones para determinar el o los ganadores en cada una de las licitaciones, asegurando se cumpla con la normatividad vigente en término de adquisiciones y contratación de obras y servicios

	relacionados. V. Coordinar la asignación y la notificación de la determinación de ganadores de las licitaciones para completar la entrega de la orden de compra y elaboración de contratos, de acuerdo con las bases técnicas y cuidando se especifiquen los requerimientos y condiciones para los bienes, servicios u obras por adquirir. VI. Coordinar la suscripción, administración, rescisión, suspensión o terminación anticipada de contratos en los términos de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público y Ley de Obras Públicas y Servicios Relacionados con las Mismas. VII. Coordinar el proceso de contratación de los proveedores e integración de sus expedientes para su seguimiento y control administrativo.
Nombre del Puesto/Perfil	Funciones y Obligaciones
Jefe de Departamento y/o Análogo.	I. Participar en la ejecución de las licitaciones para la adquisición de bienes y contratación de servicios, obras y servicios relacionados, apegados a lo que establece la normatividad aplicable. II. Preparar las convocatorias y bases para las distintas licitaciones considerando los requerimientos de las áreas usuarias para que sean incorporados en las mismas. III. Apoyar en la apertura de ofertas y el proceso de evaluación de proposiciones para determinar el o los ganadores en cada una de las licitaciones, asegurando se cumpla con la normatividad vigente en término de adquisiciones y contratación de obras y servicios relacionados. V. Informar la determinación de ganadores de las licitaciones para completar la entrega de la orden de compra y elaboración de contratos, de acuerdo con las bases técnicas y cuidando se especifiquen los requerimientos y condiciones para los bienes, servicios u obras por adquirir. VI. Coadyuvar en el proceso de contratación de los proveedores e integración de sus expedientes para su seguimiento y control administrativo.

13. Gerencia de Ingresos

Nombre del Tratamiento	13.1 Tratamiento de datos personales para la promoción de servicios aeroportuarios. 13.2 Tratamiento de datos personales para servicios aeroportuarios y complementarios.
Nombre del Puesto/Perfil	Funciones y Obligaciones
Gerente de Ingresos	I. Supervisar la emisión oportuna de las facturas correspondientes a los servicios prestados en los Aeropuertos de la Red ASA y estaciones de combustibles. II. Verificar y supervisar el comportamiento de la cartera de clientes, para conocer el estado del mismo y tomar decisiones. III. Coordinar las actividades de cobranza de la cartera de clientes, con el fin de recuperar los

	importes facturados y evitar perjuicios al patrimonio del Organismo. IV. Supervisar que las conciliaciones y el proceso de cierre mensual se lleve a cabo correctamente en todas las áreas. V. Supervisar la suscripción, vigencia y renovación de contratos a personas físicas o morales que requieren servicios aeroportuarios, de abastecimiento de combustibles y Tarifa de Uso de Aeropuerto (TUA), interactuando con el Comité de Contratación de Servicios Aeroportuarios (COCOSA), VI. Asegurar la atención personalizada a representantes de compañías aéreas, con el propósito de efectuar aclaraciones y solucionar problemas sobre cobros, pagos y contratos. VII. Coordinar estudios y evaluar las tarifas de los productos y servicios que ofrece el Organismo en cualquier línea de negocios, venta de combustibles, servicios aeroportuarios, complementarios, auxiliares y especiales.
Nombre del Puesto/Perfil	Funciones y Obligaciones
Jefe de Departamento y/o Análogo.	I. Participar en la atención a la emisión oportuna de las facturas correspondientes a los servicios prestados en los Aeropuertos de la Red ASA y estaciones de combustibles. II. Entregar el comportamiento de la cartera de clientes al Gerente de Ingresos. III. Proponer actividades de cobranza de la cartera de clientes, con el fin de recuperar los importes facturados y evitar perjuicios al patrimonio del Organismo. V. Realizar los contratos a personas físicas o morales que requieren servicios aeroportuarios, de abastecimiento de combustibles y Tarifa de Uso de Aeropuerto (TUA), interactuando con el Comité de Contratación de Servicios Aeroportuarios (COCOSA), VI. Apoyar en la atención personalizada a representantes de compañías aéreas, con el propósito de efectuar aclaraciones y solucionar problemas sobre cobros, pagos y contratos. VII. Participar en estudios y evaluar las tarifas de los productos y servicios que ofrece el Organismo en cualquier línea de negocios, venta de combustibles, servicios aeroportuarios, complementarios, auxiliares y especiales.

14. Subdirección de Informática

Nombre del Tratamiento	14.1 Tratamiento de datos personales para concursantes en el procedimiento de licitación. 14.2 Tratamiento de datos personales para el procedimiento de licitación.
Nombre del Puesto/Perfil	Funciones y Obligaciones
Subdirector de Informática	I. Establecer y coordinar el Programa Estratégico de las Tecnologías de la Información, para coadyuvar al logro de los objetivos del Organismo. II. Coordinar que se proporcionen a todas

	las unidades administrativas del Organismo, los servicios y apoyos informáticos que requieran para su operación y mejora continua. III. Coordinar la evaluación y selección de proveedores de soluciones y servicios de Informática.
Nombre del Puesto/Perfil	Funciones y Obligaciones
Gerencia de Sistemas	I. Coordinar el desarrollo de sistemas informáticos que satisfagan los requerimientos de las áreas y usuarios de las unidades administrativas del Organismo, los cuales permitan mejorar la automatización y operación. II. Coordinar la elaboración de los comparativos de proveedores de tecnología y las bases de licitación en sus aspectos técnicos para el desarrollo de sistemas, integrando los requerimientos al Plan de Adquisiciones de la Subdirección de Informática.
Nombre del Puesto/Perfil	Funciones y Obligaciones
Gerencia de Soluciones Informáticas	I. Administrar el proceso de adjudicación de los contratos y la obtención de las fianzas que garanticen la adquisición de bienes, servicios y trabajos de mantenimiento informático. II. Controlar la preparación y supervisar la administración de todos los contratos que se expidan para la adquisición de bienes y servicios, incluyendo el mantenimiento informático. III. Controlar conforme al presupuesto, la contratación de trabajos de mantenimiento y servicios, la adquisición de bienes de inversión y la aplicación del gasto corriente del área informática. IV. Supervisar el proceso de licitación y vigilar la correcta ejecución de los concursos para la contratación de obras de mantenimiento e instalaciones y para la adquisición de equipos, bienes y servicios, con apego a los procedimientos administrativos y programas presupuestales.

14. Unidad de Transparencia

Nombre del Tratamiento	15.1 Tratamiento para la atención a solicitudes de información y protección de datos personales
Nombre del Puesto/Perfil	Funciones y Obligaciones
Titular de la Unidad de Transparencia	I. Dirigir el cumplimiento de la normatividad en materia de Transparencia y Rendición de Cuentas del Organismo.
Nombre del Puesto/Perfil	Funciones y Obligaciones

Gerencia de Proyectos Especiales	I. Supervisar las funciones de la unidad de enlace para la transparencia y el acceso a la Información Pública Gubernamental, a fin de asegurar que se dé cumplimiento a la normatividad en la materia; II. Asegurar la estricta observancia y cumplimiento en la atención de las solicitudes de acceso a la información de conformidad con la legislación y normatividad correspondiente; III. Supervisar y evaluar la información publicada en la herramienta informática denominada "portal de obligaciones de transparencia", a fin de garantizar que se encuentra actualizada conforme a la normatividad aplicable; y IV. Coordinar las acciones para la operación del Comité de Información del Organismo.

III. Análisis de riesgo

El análisis de riesgos de datos personales, sirve para identificar peligros y estimar los riesgos, 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.

A continuación, se enlistan las actividades que comprende el análisis de riesgos y que deben ser tomados en cuenta en su elaboración:

I. Los requerimientos regulatorios, códigos de conducta o mejores prácticas de un sector específico;
II. El valor de los datos personales de acuerdo con su clasificación previamente definida y su ciclo de vida;
III. El valor y exposición de los activos involucrados en el tratamiento de los datos personales;
IV. Las consecuencias negativas para los titulares que pudieran derivar de una vulneración de seguridad ocurrida;
V. El riesgo inherente a los datos personales tratados, contemplando el ciclo de vida de los datos personales, las amenazas y vulnerabilidades existentes para los datos personales y los recursos o activos involucrados en su tratamiento, como pueden ser, de manera enunciativa más no limitativa, hardware, software, personal o cualquier otro recurso humano o material, entre otros;
VI. La sensibilidad de los datos personales tratados;
VII. El desarrollo tecnológico;
VIII. Las transferencias de datos personales que se realicen;
IX. El número de titulares;
X. Las vulneraciones previas ocurridas en los sistemas de tratamiento, y
XI. 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.

En el desarrollo de este punto, se utilizó el Evaluador de Vulneraciones, que es una herramienta creada por el Instituto Nacional de Transparencia Acceso a la Información y Protección de Datos Personales, la cual permite a los responsables en el tratamiento de datos personales registrar y documentar las medidas de seguridad existente y faltantes, y ayuda a determinar las posibilidades de una vulneración a la seguridad de los datos personales.

Debido al volumen de los análisis de riesgo, los cuales fueron elaborados por cada tratamiento identificado, es decir se elaboraron 38 archivos, los cuales forman parte del documento de seguridad como **ANEXOS 2A y 2B**.

IV. Análisis de Brecha

Para realizar un análisis de brecha, se debe comparar las medidas de seguridad existentes contra las faltantes en la organización del responsable, considerando lo siguiente:

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

El análisis de brecha se puede definir como la concentración de elementos específicos que pueden existir entre lo deseable y lo actual, para ello es necesario definir lo siguiente:

a) ¿Cuál es la brecha que se desea analizar?
b) Identificar quiénes están involucrados.
c) ¿Cuáles son las causas más relevantes que determinan la brecha?
d) Identificar las diferencias de comportamiento entre los sistemas o actores a comparar en la brecha.
e) Identificar los indicadores y/o atributos de la situación actual
f) Elaborar un listado con la finalidad de medir o caracterizar la brecha.

En síntesis, se establece que, para la realización del análisis de brecha, el responsable deberá considerar las medidas de seguridad existentes y efectivas, las medidas de seguridad faltantes y la existencia de nuevas medidas de seguridad que pudieran reemplazar a uno o más controles implementados actualmente.

El análisis de brecha forma parte del presente documento como **ANEXO 3.**

V. Plan de Trabajo

El Plan de Trabajo, consiste en la implementación de las medidas de seguridad faltantes, así como las medidas para el cumplimiento de las políticas de gestión y tratamiento de los datos personales. La elaboración del Plan de Trabajo toma en cuenta los siguientes aspectos:

1. Basado en el análisis de riesgo y análisis de brecha.
2. Actuar sobre las actividades relevantes y urgentes.
3. Tomar en cuenta los recursos designados.
4. Conforme a las fechas de compromiso para la implementación de las medidas de seguridad nuevas o faltantes.

Información que se reserva: Periodo para la implementación de medidas de seguridad.
Fundamento legal: Artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública; 110, fracción VII, de la Ley Federal de Transparencia y Acceso a la Información Pública; y Lineamiento Vigésimo Sexto, de los Lineamientos Generales en Materia de Clasificación y Desclasificación de la Información, así como para la elaboración de versiones públicas.
Motivación: Es información reservada, la publicación podría permitir vulneraciones a la seguridad y obstruir la prevención de los delitos.
Área que clasifica: Jefatura de Análisis de Factibilidad
Fecha: 04 de mayo de 2022
Rúbrica del titular del área:

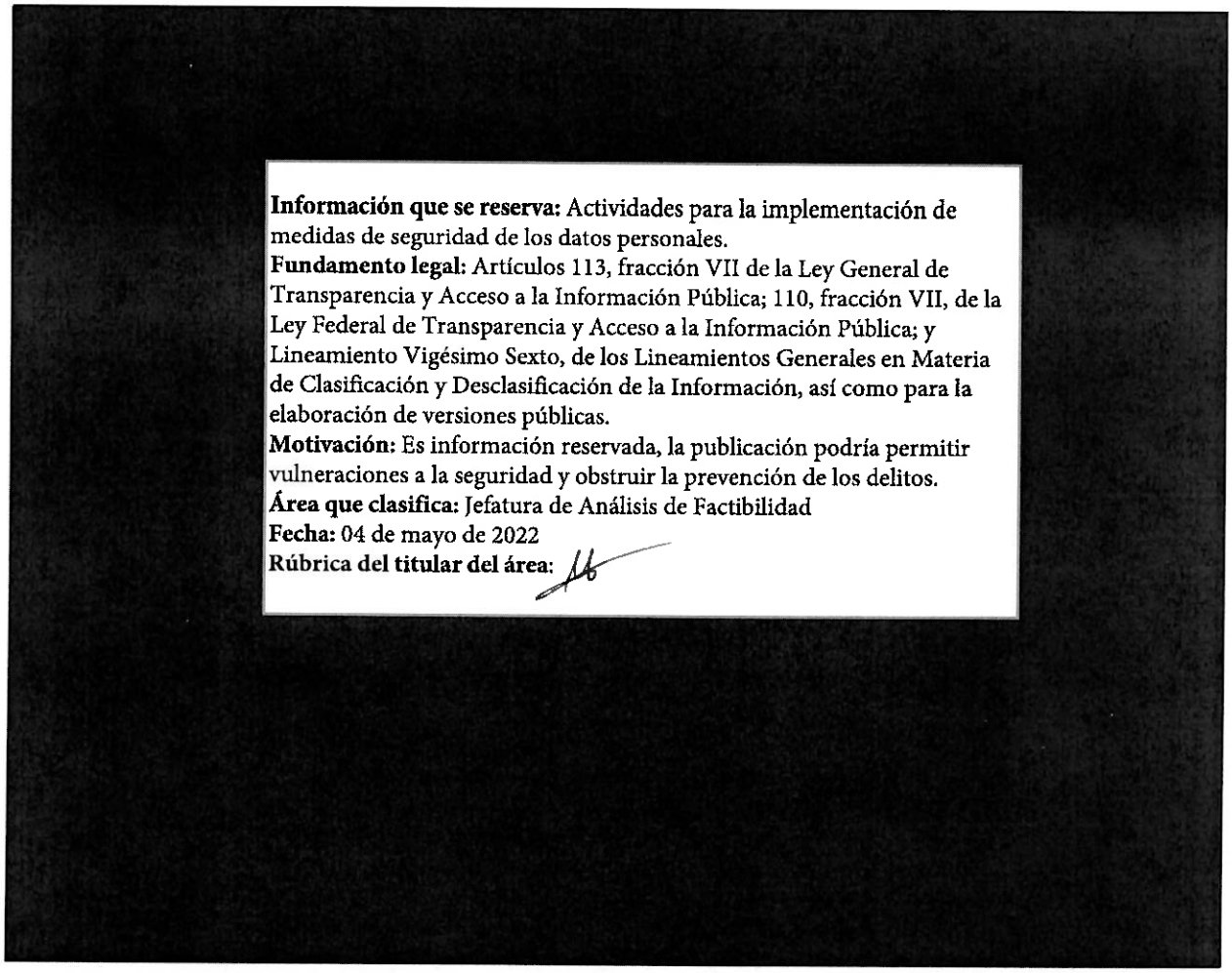
CRONOGRAMA DE ACTIVIDADES

[redacted]

Información que se reserva: Actividades para la implementación de medidas de seguridad de los datos personales.
Fundamento legal: Artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública; 110, fracción VII, de la Ley Federal de Transparencia y Acceso a la Información Pública; y Lineamiento Vigésimo Sexto, de los Lineamientos Generales en Materia de Clasificación y Desclasificación de la Información, así como para la elaboración de versiones públicas.
Motivación: Es información reservada, la publicación podría permitir vulneraciones a la seguridad y obstruir la prevención de los delitos.
Área que clasifica: Jefatura de Análisis de Factibilidad
Fecha: 04 de mayo de 2022
Rúbrica del titular del área:

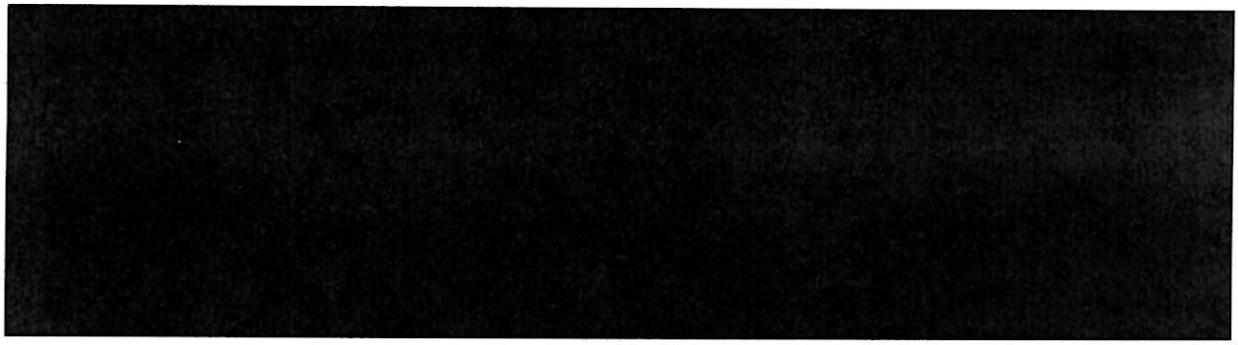
De acuerdo con las etapas y las acciones que se deben llevar a cabo en materia de seguridad, se presenta el siguiente cronograma de actividades:

[redacted]



Información que se reserva: Actividades para la implementación de medidas de seguridad de los datos personales.
Fundamento legal: Artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública; 110, fracción VII, de la Ley Federal de Transparencia y Acceso a la Información Pública; y Lineamiento Vigésimo Sexto, de los Lineamientos Generales en Materia de Clasificación y Desclasificación de la Información, así como para la elaboración de versiones públicas.
Motivación: Es información reservada, la publicación podría permitir vulneraciones a la seguridad y obstruir la prevención de los delitos.
Área que clasifica: Jefatura de Análisis de Factibilidad
Fecha: 04 de mayo de 2022
Rúbrica del titular del área:

Del mes 7 al 12 Actividades Prioritarias en la Seguridad



[redacted]

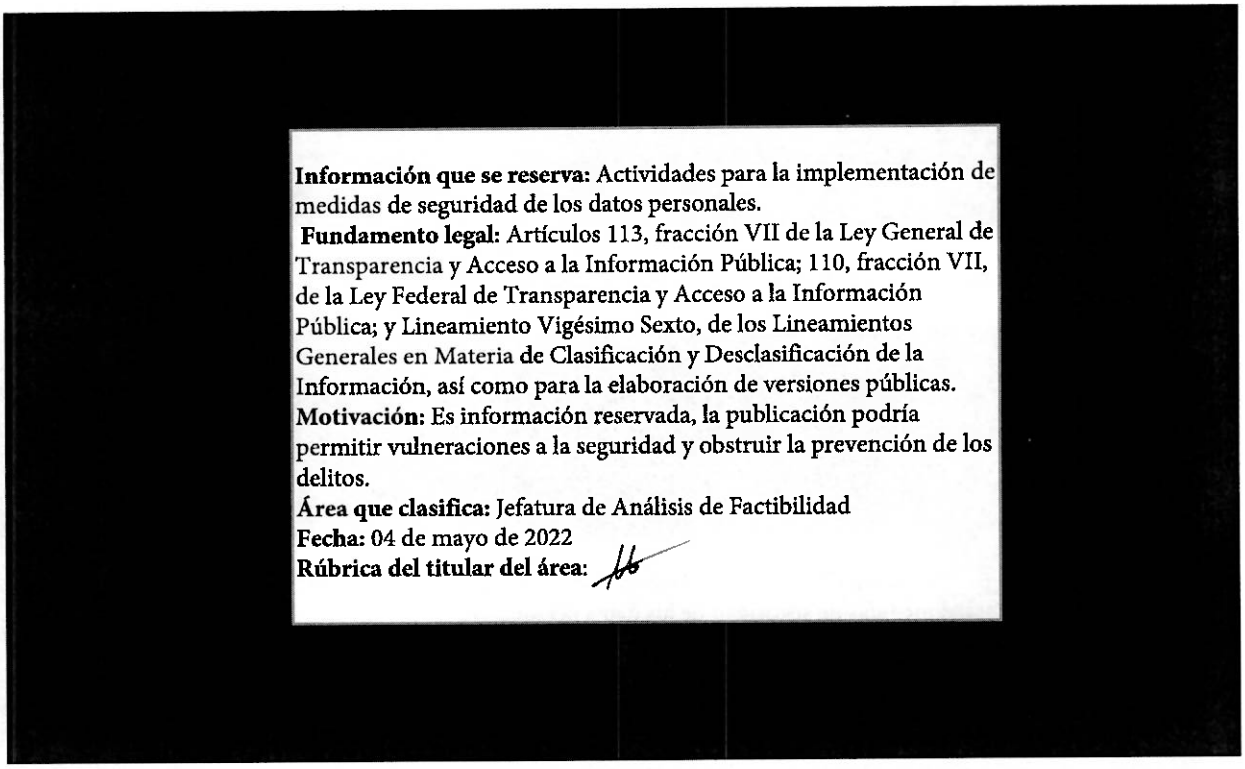
Información que se reserva: Actividades para la implementación de medidas de seguridad de los datos personales.
Fundamento legal: Artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública; 110, fracción VII, de la Ley Federal de Transparencia y Acceso a la Información Pública; y Lineamiento Vigésimo Sexto, de los Lineamientos Generales en Materia de Clasificación y Desclasificación de la Información, así como para la elaboración de versiones públicas.
Motivación: Es información reservada, la publicación podría permitir vulneraciones a la seguridad y obstruir la prevención de los delitos.
Área que clasifica: Jefatura de Análisis de Factibilidad
Fecha: 04 de mayo de 2022
Rúbrica del titular del área:

[redacted]

Del mes 13 al 17 Actividades Faltantes en la Seguridad

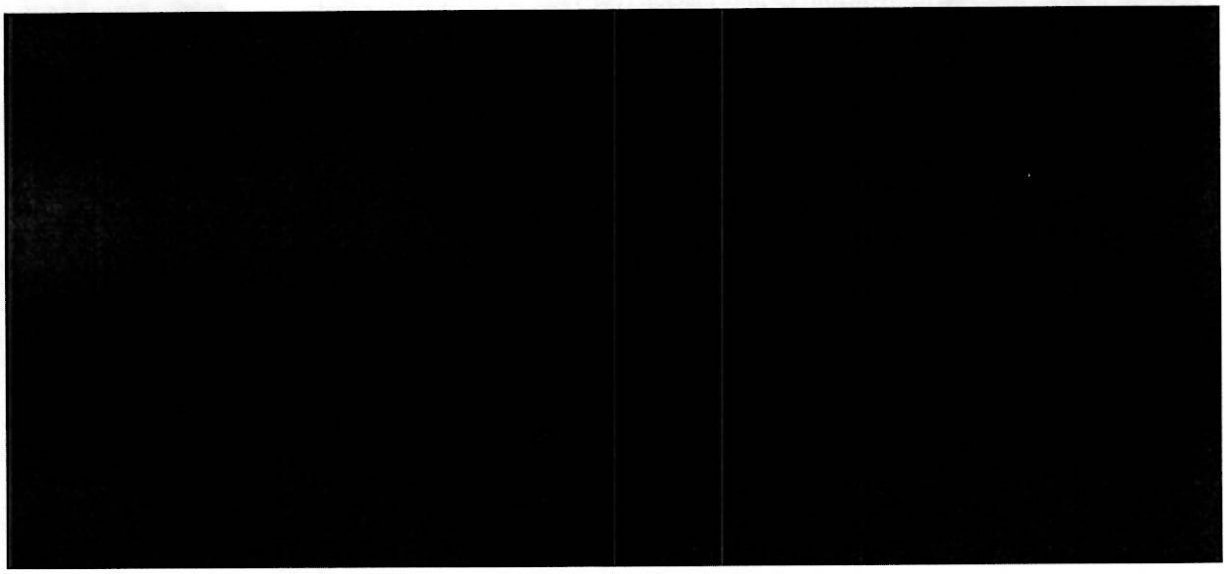
[redacted]

Información que se reserva: Actividades para la implementación de medidas de seguridad de los datos personales.
Fundamento legal: Artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública; 110, fracción VII, de la Ley Federal de Transparencia y Acceso a la Información Pública; y Lineamiento Vigésimo Sexto, de los Lineamientos Generales en Materia de Clasificación y Desclasificación de la Información, así como para la elaboración de versiones públicas.
Motivación: Es información reservada, la publicación podría permitir vulneraciones a la seguridad y obstruir la prevención de los delitos.
Área que clasifica: Jefatura de Análisis de Factibilidad
Fecha: 04 de mayo de 2022
Rúbrica del titular del área:



Información que se reserva: Actividades para la implementación de medidas de seguridad de los datos personales.
Fundamento legal: Artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública; 110, fracción VII, de la Ley Federal de Transparencia y Acceso a la Información Pública; y Lineamiento Vigésimo Sexto, de los Lineamientos Generales en Materia de Clasificación y Desclasificación de la Información, así como para la elaboración de versiones públicas.
Motivación: Es información reservada, la publicación podría permitir vulneraciones a la seguridad y obstruir la prevención de los delitos.
Área que clasifica: Jefatura de Análisis de Factibilidad
Fecha: 04 de mayo de 2022
Rúbrica del titular del área:

Del mes 19 al 24 Actividades de Mejora en los Sistemas de Seguridad



[redacted]

Información que se reserva: Actividades para la implementación de medidas de seguridad de los datos personales.
Fundamento legal: Artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública; 110, fracción VII, de la Ley Federal de Transparencia y Acceso a la Información Pública; y Lineamiento Vigésimo Sexto, de los Lineamientos Generales en Materia de Clasificación y Desclasificación de la Información, así como para la elaboración de versiones públicas.
Motivación: Es información reservada, la publicación podría permitir vulneraciones a la seguridad y obstruir la prevención de los delitos.
Área que clasifica: Jefatura de Análisis de Factibilidad
Fecha: 04 de mayo de 2022
Rúbrica del titular del área:

VI. Los mecanismos de monitoreo y revisión de las medidas de seguridad

De acuerdo a lo dispuesto por la Ley General, el responsable tiene la obligación de monitorear y revisar de manera periódica las medidas de seguridad implementadas, así como las amenazas y vulneraciones a las que se pueda estar sujetos los datos personales.

En este proceso, se evalúan y miden los resultados de las políticas, planes, procesos y procedimientos implementados, se realizan con el fin de verificar que se haya logrado la mejora esperada.

De conformidad con el artículo 63 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público, en las revisiones se deben realizar las siguientes actividades:

I. Los activos que se incluyan en la gestión de riesgos.
II. Las modificaciones necesarias a los activos como podría ser el cambio o migración tecnológica.
III. Las nuevas amenazas que podrían estar activas dentro y fuera de la organización y no han sido valoradas.
IV. La posibilidad de que vulneraciones nuevas o incrementadas sean explotadas por las amenazas correspondientes.
V. Las vulneraciones identificadas para determinar aquellas expuestas a amenazas nuevas o pasadas que vuelvan a surgir.
VI. El cambio en el impacto o consecuencia de amenazas valoradas, vulnerabilidades y riesgos en conjunto, que resulten en un nivel aceptable de riesgo, y
VII. Los incidentes y vulneraciones de seguridad ocurridas.

Para cumplir con el monitoreo periódico de las medidas de seguridad implementadas, las amenazas y vulnerabilidades a los que estén sujetos los datos personales, se realizará una **auditoría interna anualmente**.

Debido a que ASA no cuenta con una Unidad Administrativa encargada de la seguridad de la información, la Unidad de Transparencia con la participación de las unidades administrativas actuará como apoyo en la elaboración de la mejora de las medidas de seguridad y seguimiento en la auditoria.

Auditoria Interna
Se realizará en conjunto con la Unidad de Transparencia a las áreas involucradas en el tratamiento de datos personales.

Para ello y con base en el Plan de Trabajo planteado por el Organismo, se estará solicitando al Administrador de cada uno de los sistemas de tratamiento de datos personales envíe a la Unidad de Transparencia, la evidencia que sustente las acciones realizadas.

El requerimiento, se hará en forma anual durante el mes de agosto, a efecto de que el área de una respuesta dentro de los primeros 10 días hábiles del mes de septiembre.

La efectividad de las medidas de seguridad implementadas se estará evaluando en conjunto con los titulares de las unidades administrativas, con la finalidad de evitar alteración, pérdida o acceso no autorizado a los datos personales objeto de tratamiento en los distintos sistemas.

El programa de auditoría debe monitorear la eficacia y eficiencia de la seguridad de los datos personales. El programa debe establecerse conforme a la política de gestión de datos personales y revisar lo siguiente:

a) Considerar si el Organismo está operando de acuerdo a la política de gestión de datos personales y los procedimientos establecidos.
b) Si se han implementado y mantenido de acuerdo a los requerimientos tecnológicos.

Establecer el objetivo del programa de auditoria, consiste en revisar los tratamientos de datos personales internos, identificar a los custodios de la información, y en establecer criterios para llevar a cabo la auditoria.

Para lograr la objetividad e imparcialidad de la auditoría se debe elegir apropiadamente a los auditores y la forma de conducción de la auditoría.

Revisión de los Factores de Riesgo:
Se debe monitorear y revisar el riesgo con sus factores relacionados, es decir;

a) Medir el valor de los activos[1].
b) Las amenazas.
c) Las vulnerabilidades
d) El impacto
e) La probabilidad de ocurrencia.

Los incisos señalados en el párrafo anterior, sirven para identificar cualquier cambio en el contexto del alcance y objetivos de la organización y así mantener una visión general del riesgo.

El riesgo no es estadístico: las amenazas, vulnerabilidades, probabilidad y consecuencias pueden cambiar abruptamente sin previo aviso. Esta situación exige la revisión de cada riesgo por separado, así como la suma de ellos, para conocer el impacto potencial acumulado de las amenazas.

El Organismo deberá monitorear los siguientes puntos:

- Nuevos activos que se incluyan en los alcances de la gestión de riesgo.
- Modificaciones necesarias a los activos, por ejemplo, cambio o migración tecnológica.
- Nuevas amenazas que podrían estar activas dentro y fuera de la organización y que no han sido valoradas.
- La posibilidad de que vulnerabilidades nuevas o incrementadas sean explotadas por las amenazas correspondientes.

[1] Activo: La información, el conocimiento sobre los procesos, el personal, hardware, software y cualquier otro recurso involucrado en el tratamiento de los datos personales, que tenga valor para la Institución.

- Vulnerabilidades identificadas para determinar aquéllas expuestas a amenazas nuevas o pasadas que vuelven a surgir.
- Cambio en el impacto o consecuencias de amenazas valoradas, vulnerabilidades y riesgos en conjunto, que resulten en un nivel inaceptable de riesgo.
- Incidentes y vulneraciones de seguridad. Los factores que determinan la probabilidad de ocurrencia y consecuencias podrían cambiar, lo que afectaría la conveniencia y costos de las opciones de tratamiento. Los cambios mayores que afectan a la organización deben ser revisados de manera específica, no obstante que las actividades de monitoreo requieren de regularidad y periodicidad.

El resultado del monitoreo, puede afectar los tratamientos de datos personales, y en consecuencia el contenido del Sistema de Gestión de Seguridad de Datos Personales que se establezca en la organización.

Resultados de la Auditoria Interna

Se obtendrán como resultados de la auditoria, observaciones que determinen los posibles riesgos existentes, con la finalidad de realizar medidas preventivas. Dicho de otra forma, qué controles se pueden establecer para que no ocurra una vulneración a la seguridad.

La auditoría debe dar información respecto a los cambios ocurridos al Sistema de Gestión de Seguridad de Datos Personales. También, que medidas correctivas deben ser implementadas de inmediato.

Auditorias Voluntarias

El Organismo de manera voluntaria podrá solicitar una auditoría por parte del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), con el fin de verificar la eficiencia de los controles, medidas y mecanismos implementados en la Protección de Datos Personales, así como identificar deficiencias en su sistema y proponer acciones o recomendaciones correctivas que en su caso correspondan (Art. 151 Ley General).

Una vez que el Organismo, cuente con el Sistema de Gestión de Seguridad de Datos Personales, es recomendable una auditoría voluntaria que se realizará a solicitud del Organismo.

El procedimiento para solicitar una auditoría voluntaria es el siguiente:

- Presentación de la solicitud por parte del responsable, con los requisitos establecidos en los artículos 220 y 221 de los Lineamientos Generales.
- Respuesta del INAI a la solicitud de auditoría voluntaria ya sea que ha sido aceptada o se ha emitido una prevención.
- Planeación de la auditoría, definición de objetivos, alcance, actividades, recursos y tiempos que serán requeridos para su desarrollo.
- Inicio de la auditoría ya sea una revisión en las instalaciones del INAI o en el sitio del responsable donde se realiza el tratamiento de datos personales que será evaluado.
- Ejecución de la auditoría a través de la recopilación de datos y registros, análisis, evaluación, redacción de los hallazgos y conclusiones.

- Presentación de informe de auditoría, a través de una reunión de cierre.
- La duración máxima de una auditoría voluntaria es de 50 días.

Resultado de la Auditoria Voluntaria

Una auditoría voluntaria permitirá a los responsables:

- Conocer el grado de cumplimiento de las medidas implementadas para la protección de los datos personales.
- Obtener recomendaciones de la autoridad ya sea el INAI o de organismos garantes.
- Establecer acciones preventivas o correctivas para atender los hallazgos de auditoría que se encuentran en incumplimiento, de tal forma que se mejoren los controles o medidas actualmente implementados para la protección de datos personales.
- Brindará transparencia y confianza al responsable sobre las medidas que ha implementado en los tratamientos que realiza.

Vulneraciones a la Seguridad

Como parte de las políticas para la protección de datos, se realizará un procedimiento para la atención de las vulneraciones que puedan ocurrir en el Organismo.

La vulnerabilidad es la "falta o debilidad de seguridad en un activo o grupo de activos que puede ser explotada por una o más amenazas", la vulneración de datos personales es la materialización de las amenazas pudiendo estar enfocadas a la pérdida o destrucción no autorizada de los datos personales en posesión de las personas físicas o morales que realizan el tratamiento de los datos, el robo, extravío o copia no autorizada de los mismos, su uso, acceso o tratamiento no autorizado, así como el daño, alteración o modificación no autorizada. Estas vulneraciones están comprendidas en el artículo 38 de la Ley General.

Es obligación del Organismo contar con un procedimiento para tomar acciones que permitan el manejo de las vulneraciones de seguridad que puedan ocurrir, considerando lo siguiente:

1) Identificación de la vulneración.

En caso de un incidente de seguridad, el responsable debe identificar:

a) Los activos afectados junto con el personal a cargo
b) Los titulares afectados
c) Partes interesadas que requieran estar informadas y/o puedan tomar parte en la toma de decisiones para mitigar las consecuencias de la vulneración.

2) Notificación de la vulneración.

Una vez identificada la vulneración, ésta se debe comunicar a los titulares de los datos personales para que puedan tomar medidas que mitiguen o eviten una posible afectación.

Dependiendo del riesgo que implique para los titulares, la notificación de una vulneración puede ser a través de medios masivos como un anuncio en su página web, periódico, radio y televisión o bien, de manera personalizada.

El responsable debe 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.

3) Remediación del incidente.

Una vez identificada la vulneración y después de haber realizado la respectiva notificación, se debe profundizar en el análisis de las causas del incidente para establecer medidas correctivas, las cuales incluyen medidas inmediatas para reducir los efectos de la vulneración, así como medidas a largo plazo por ejemplo, implementar controles técnicos o actualizar las políticas del Sistema de Gestión de Seguridad de Datos Personales, para evitar que incidentes similares o relacionados vuelvan a ocurrir.

Las revisiones, auditorías y los tratamientos de una vulneración a la seguridad deben estar debidamente documentados, incluyendo un resumen de los hallazgos y los planes para aplicar medidas preventivas y correctivas con objeto de contar con evidencia suficiente para mostrar al Instituto su diligencia en tomar las acciones necesarias para evitar o mitigar una vulneración a la seguridad de los datos personales, además de que estos procesos proporcionan información que sirve como entrada para los procesos de mejora continua.

VII. Programa General de Capacitación

El Programa General de Capacitación, tiene como objetivo que los servidores públicos puedan comprender el alcance del derecho humano a la protección de datos personales, como ya se ha señalado, es obligación de los sujetos obligados establecer las medidas de seguridad. Para lograr la implementación de un adecuado sistema en la seguridad, es necesario crear conciencia en los servidores públicos quienes día con día en el desempeño de sus funciones, realizan algún tipo de tratamiento de datos personales, los servidores públicos necesitan conocer qué actos se pueden o no realizar, así como las consecuencias y sanciones por las posibles violaciones.

Si los servidores públicos del Organismo tienen conocimiento de las obligaciones y principios que deben cumplirse, será más fácil la prevención a posibles violaciones sobre los datos personales. Como finalidad última, se pretende generar una cultura sobre la protección de datos, que los mismos servidores entiendan la importancia de cumplir con la normativa y conozcan sus derechos como titulares.

Son tres las etapas que se plantean en el Programa General de Capacitación, y son las siguientes:

a) La primera será desarrollar en el Programa General de Capacitación, la actualización sobre las obligaciones y deberes en materia de protección de datos personales.

   Para cumplir, será necesario que los servidores públicos del Organismo tengan conocimiento de la normativa básica. (La Ley General y los Lineamientos Generales).

   Así como, los Acuerdos emitidos por el Instituto Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales.

b) La capacitación y actualización, en materia de protección de datos personales deben comprender tanto a los servidores públicos del organismo y a los encargados, ya que actúan a nombre y cuenta del Organismo.

c) Por último, es necesario para la implementación del Programa General de Capacitación, identificar los niveles de responsabilidad de acuerdo a sus atribuciones y funciones, es decir la capacitación también deberá realizarse de acuerdo a las responsabilidades respecto del tratamiento de los datos personales, seguridad de los datos personales y el perfil de los puestos.

Una vez que se ha determinado el objetivo, tenemos como meta principal, desarrollar que la aplicación de la capacitación sea por niveles, basado en las atribuciones y las responsabilidades de quienes realizan el tratamiento de datos personales.

El programa de capacitación deberá tomar en cuenta los siguientes niveles, para determinar el tipo de capacitación que requieren los servidores públicos:

a) Concienciación: programas a corto plazo para la difusión en general de la protección de datos personales en Aeropuertos y Servicios Auxiliares;

b) Entrenamiento: programas a mediano plazo que buscan capacitar al personal de manera específica respecto a sus funciones y responsabilidad en el tratamiento de los datos personales, y

c) Educación: programa general a largo plazo que tiene por objetivo incluir la protección de los datos personales dentro de la cultura de la organización.

Basado en las actividades y resultados obtenidos en el desarrollo de este Documento de Seguridad, se identificaron algunas deficiencias relevantes y la identificación de las Unidades Administrativas que realizan mayor o menor tratamiento de datos personales. Tomando en consideración estos resultados derivados del análisis del inventario de datos personales, análisis de brecha y análisis de riesgo, se identifican las necesidades y el tipo de capacitación necesaria para el personal.

El Programa General está basado en una **periodicidad anual** y será necesario realizar las **evaluaciones** para medir el nivel de eficiencia y eficacia de la capacitación, a través de criterios de evaluación que determinen el nivel de competencia aceptado por el sujeto obligado, y mantener un registro por servidor público.

NIVEL 1 PROGRAMAS A CORTO PLAZO

Temáticas:

1. Introducción a la Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados.

Dirigida a todos los servidores públicos del organismo para conocer la normativa básica. Con la entrada en vigor de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y los Lineamientos Generales de Protección de Datos Personales para el Sector Público, los Sujetos Obligados, que traten datos personales, deberán cumplir una serie de obligaciones con objeto de garantizar a las personas el derecho a la protección de su información personal. La protección de datos personales es un derecho humano, reconocido en los artículos 6 y 16 de la Constitución Política de los Estados Unidos Mexicanos.

Áreas o personal	Período	Objetivos
Dirigida a todos los servidores públicos del organismo; se realizará en forma cuatrimestral	3 Cursos por año. En forma Cuatrimestral	Se pretende proporcionar apoyo técnico para el cumplimiento de la normatividad de la materia, para facilitar el cumplimiento de las obligaciones en materia de protección de datos personales. Reflexionar sobre el derecho a la protección de datos personales; su contenido y alcances, así como la relación que guarda con la protección de la privacidad de las personas.

		Identificar el marco jurídico nacional e internacional que regula al derecho a la protección de datos personales. Analizar los principios de protección de datos personales, e identificar los deberes y obligaciones, así como las sanciones derivadas por su incumplimiento.

2. Principios y deberes.

Facilitar el cumplimiento de las obligaciones en materia de protección de datos personales, identificación de los principios y deberes.

Áreas o personal	Periodo	Objetivos
Dirigida a todos los servidores públicos del organismo, se realizará en forma trimestral	3 Cursos por año. En forma Cuatrimestral	➢ Conocer los estándares, es decir, recomendaciones para el cumplimiento de los principios y deberes en materia de protección de datos personales, para el sector público. ➢ Analizar los principios y deberes de protección de datos personales, así como las sanciones derivadas por su incumplimiento.

NIVEL II PROGRAMAS A MEDIANO PLAZO

3. Derechos ARCO

Conocer los derechos de los titulares frente a los responsables, identificar por qué es importante el cuidado de la información personal, cómo pueden ejercerlo los titulares y ante quién pueden quejarse en caso de que consideren que no ha sido respetado su derecho.

Áreas o personal	Periodo	Objetivos
Dirigida exclusivamente a los servidores públicos del organismo: **a) Que realicen directamente dentro de sus actividades el**	2 Cursos por año. En forma Semestral	➢ Proporcionar a los responsables las recomendaciones, capacidades, y requisitos para la debida atención a las solicitudes de derechos ARCO, para que las personas los puedan ejercer de manera informada y cuando lo requieran para la defensa y protección de sus intereses.

tratamiento de datos personales. **b) Servidores públicos que en sus atribuciones tengan la obligación de realizar algún tratamiento de datos personales.**		

4. Aviso de Privacidad

Conocer la importancia del principio de información, para que los responsables del tratamiento de datos personales cumplan la obligación de elaborar y poner a disposición de los titulares de los datos, el correspondiente Aviso de Privacidad, en el que comuniquen todos los elementos informativos establecidos en la normativa.

Áreas o personal	Periodo	Objetivos
Dirigida exclusivamente a los servidores públicos del organismo: **a) Que realicen directamente dentro de sus actividades el tratamiento de datos personales.** **b) Servidores públicos que en sus atribuciones tengan la obligación de realizar algún tratamiento de datos personales.**	2 Cursos por año. En forma Semestral	➢ Proporcionar a los responsables del tratamiento de los datos personales, una herramienta que le sea de utilidad a las Unidades Administrativas, para que puedan elaborar su aviso de privacidad, dirigido a los distintos titulares. ➢ Facilitar a estas áreas administrativas, la elaboración y puesta a disposición de los avisos a los titulares, identificando elementos comunes y en la generalidad qué tipo de datos se recaban.

5. Taller de Medidas de Seguridad

Conocer la importancia de la seguridad de los datos personales, como establecer y mantener las medidas de seguridad administrativas, físicas y técnicas. Identificar los riesgos en el manejo de los datos personales.

Áreas o personal	Periodo	Objetivos
Dirigida exclusivamente a los	1 Curso. En forma Anual	➢ Importancia de la seguridad de los datos personales.

servidores públicos del organismo: **Que cuentan con alto nivel de responsabilidad y funciones en el tratamiento de datos personales.**	En Coordinación con el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.	➢ Publicaciones en materia de seguridad del INAI. ➢ Definiciones útiles. ➢ Implementación de un Sistema de Gestión de Seguridad de Datos Personales.

6. Vulneraciones a la seguridad

La gestión de incidentes es el proceso de planeación, comunicación y capacidad de acción cuando ocurre un incidente de seguridad. Por lo tanto, elaborar un plan de respuesta a incidentes es probablemente una de las tareas más complejas en seguridad de la información.

Áreas o personal	Periodo	Objetivos
Dirigida exclusivamente a los servidores públicos del Organismo: **Que cuentan con alto nivel de responsabilidad y funciones en el tratamiento de datos personales.**	1 Curso. En forma Anual En Coordinación con el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.	➢ Mitigar los efectos de una vulneración a la seguridad. ➢ Evita sanciones a los servidores públicos. ➢ La relación entre las alertas y los incidentes de seguridad. ➢ Las características particulares de un incidente de seguridad cuando involucra datos personales ➢ Las etapas del plan de respuesta a incidentes de seguridad.

NIVEL 3 PROGRAMAS A LARGO PLAZO

7. Autorregulación (certificación en materia de protección datos personales)

En materia de protección de datos personales, la autorregulación es la posibilidad que tienen los responsables y encargados de establecer y autoimponerse voluntariamente reglas para el debido tratamiento de datos personales que complementen lo previsto por la normativa, elevando los estándares de protección de ésta y considerando las particularidades de los responsables o encargados que desarrollan y adoptan esta clase de reglas.

Conocer el modelo de certificación, así como los requisitos mínimos que deben satisfacer estos esquemas para su evaluación, validación o reconocimiento del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.

Áreas o personal	Periodo	Objetivos
Dirigida exclusivamente a los servidores públicos del organismo: **Que cuentan con alto nivel de responsabilidad y funciones en el tratamiento de datos personales.**	1 Cursos por año. En forma Anual En Coordinación con el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.	➢ Clases de esquemas de autorregulación. ➢ Procedimiento y requisitos para obtener una certificación. ➢ Sistemas de certificación y sus actores.

VIII. Actualizaciones

Cuando se produzcan situaciones que incidan en el tipo de datos personales que se utilizan o se afectan de alguna manera los tratamientos se debe actualizar el documento de seguridad, entre otros tenemos los siguientes momentos.

- Cuando se identifiquen o desarrollen nuevos tratamientos de datos personales;
- Se produzcan modificaciones sustanciales al tratamiento de datos personales que deriven en un cambio en el nivel de riesgo;
- Como resultado de un proceso de mejora continua, derivado del monitoreo y revisión del sistema de gestión;
- Como resultado de un proceso de mejora para mitigar el impacto de una vulneración a la seguridad ocurrida, e
- Implementación de acciones correctivas y preventivas ante una vulneración de seguridad.

Glosario de Términos

Activo	La información, el conocimiento sobre los procesos, el personal, hardware, software y cualquier otro recurso involucrado en el tratamiento de los datos personales, que tenga valor para la Institución.
Bases de datos	Conjunto ordenado de datos personales referentes a una persona física identificada o identificable, condicionados a criterios determinados, con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización;
Comité de Transparencia	Instancia a la que hace referencia el artículo 43 de la Ley General de Transparencia y Acceso a la Información Pública.
Datos personales	Cualquier información concerniente a una persona física identificada o identificable. Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información.
Datos personales sensibles	Aquellos que se refieran a la esfera más íntima de su titular, o cuya utilización indebida puedan 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.
Encargado	La persona física o moral, pública o privada, ajena a la organización del responsable, que sola o conjuntamente con otras, trata datos personales por cuenta del responsable, como consecuencia de la existencia de una relación jurídica que le vincula con el mismo y delimita el ámbito de su actuación para la prestación de un servicio.
Enlace de datos:	Servidor público que deberá conocer sobre el tratamiento de los datos personales en determinada Unidad Administrativa del Organismo. Así, como dar seguimiento a las acciones de capacitación y atender los requerimientos de la Unidad de Transparencia.
Evaluación de impacto en la protección de datos personales:	Documento mediante el cual los sujetos obligados que pretendan poner en operación o modificar políticas públicas, programas, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento intensivo o relevante de datos personales, valoran los impactos reales respecto de determinado tratamiento de datos personales, a efecto de identificar y mitigar posibles riesgos relacionados con los principios, deberes y derechos de los titulares, así como los deberes de los responsables y encargados, previstos en la normativa aplicable.
Forma de obtención de los datos personales	Puede ser directa o indirecta. La directa es aquella que se recaba directamente del titular de los datos personales y la indirecta se refiere a aquella inferida, derivada, creada, generada u obtenida a partir del análisis o el tratamiento efectuado por el responsable sobre los datos personales proporcionado directamente por el titular en algún otro sistema.

Impacto	Una medida del grado de daño a los activos o cambio adverso en el nivel de objetivos alcanzados por una Institución.
Incidente.	Escenario donde una amenaza explota una vulnerabilidad o conjunto de vulnerabilidades. • **Amenaza**. Circunstancia o evento con la capacidad de causar daño a una Institución. • **Vulnerabilidad**. Falta o debilidad de seguridad en un activo o grupo de activos que puede ser explotada por una o más amenazas.
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. De manera enunciativa más no limitativa, se deben considerar las siguientes actividades: a) Prevenir el acceso no autorizado al perímetro de la organización, sus instalaciones físicas, áreas críticas, recursos e información; b) Prevenir el daño o interferencia a las instalaciones físicas, áreas críticas de la organización, recursos e información; c) Proteger los recursos móviles, portátiles y cualquier soporte físico o electrónico que pueda salir de la organización, y d) Proveer a los equipos que contienen o almacenan datos personales de un mantenimiento eficaz, que asegure su disponibilidad e integridad; • **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. De manera enunciativa más no limitativa, se deben considerar las siguientes actividades: a) Prevenir que el acceso a las bases de datos o a la información, así como a los recursos, sea por usuarios identificados y autorizados; b) Generar un esquema de privilegios para que el usuario lleve a cabo las actividades que requiere con motivo de sus funciones; c) Revisar la configuración de seguridad en la adquisición, operación, desarrollo y mantenimiento del software y hardware, y d) Gestionar las comunicaciones,

	operaciones y medios de almacenamiento de los recursos informáticos en el tratamiento de datos personales.
Portabilidad de datos personales	Derecho que tienen el titular de los datos a obtener una copia de sus datos personales, cuando se encuentren en un formato estructurado y comúnmente utilizado, o a solicitar su transmisión a un responsable receptor, cuando es técnicamente posible, el titular hubiera facilitado directamente sus datos al responsable transmisor y el tratamiento de estos se base en su consentimiento o en la suscripción de un contrato.
Remisión	Toda comunicación de datos personales realizada exclusivamente entre el responsable y encargado, dentro o fuera del territorio mexicano.
Responsable	Los 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.
Responsable del Sistema	Es el Titular de la Unidad Administrativa que administra el sistema, quien deberá informar a la Unidad de Transparencia, los sistemas que administre, responsabilizar y designar al administrador del sistema, y verificar que la información solicitada sea la estrictamente necesaria e idónea para cumplir con trámite, servicios o actividad legal para la cual fueron obtenidos los datos personales.
Riesgo	Combinación de la probabilidad de un evento y su consecuencia desfavorable.
Riesgo de seguridad	Potencial de que cierta amenaza pueda explotar las vulnerabilidades de un activo o grupo de activos en perjuicio de la Institución. • **Valorar el riesgo**. Proceso para asignar valores a la probabilidad y consecuencias del riesgo. • **Comunicar el riesgo**. Compartir o intercambiar información entre el comité de transparencia, custodios y demás involucrados acerca del riesgo. • **Tratar el riesgo:** Procesos que se realizan para modificar el nivel de riesgo. • **Aceptar el riesgo**. Decisión informada para coexistir con un nivel de riesgo. • **Compartir el riesgo.** Proceso donde se involucra a terceros para mitigar la pérdida de información generada por un riesgo en particular, sin que el dueño del activo afectado reduzca su responsabilidad. • **Evitar el riesgo**. Acción para retirarse de una situación de riesgo o decisión para no involucrarse en ella. • **Reducir el riesgo**. Acciones tomadas para disminuir la probabilidad, las consecuencias negativas, o ambas, asociadas al riesgo.

	• **Retención del riesgo**. Aceptación de la pérdida generada por un riesgo en particular. Esta acción implica monitoreo constante del riesgo retenido. • **Riesgo residual**. El riesgo remanente después de tratar el riesgo.
Seguridad de la información	Preservación de la confidencialidad, integridad y disponibilidad de la información, así como otras propiedades delimitadas por la normatividad aplicable. • **Confidencialidad**. Propiedad de la información para no estar a disposición o ser revelada a personas, entidades o procesos no autorizados. • **Disponibilidad**. Propiedad de un activo para ser accesible y utilizable cuando lo requieran personas, entidades o procesos autorizados. • **Integridad**. La propiedad de salvaguardar la exactitud y completitud de los activos.
Sistema de Gestión de Seguridad de Datos Personales (SGSDP)	Es aquel que permite planificar, establecer, implementar, operar, monitorear, mantener, revisar y mejorar las medidas de seguridad de carácter administrativo, físico y técnico aplicadas a los datos personales; tomando en consideración los estándares nacionales e internacionales en materia de protección de datos personales y seguridad
Supresión	La baja archivística de los datos personales conforme a la normativa archivística aplicable, que resulte en la eliminación, borrado o destrucción de los datos personales bajo las medidas de seguridad previamente establecidas por el responsable.
Titular	La persona física a quien corresponden los datos personales.
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.
Transferencia de datos	Toda comunicación de datos personales dentro o fuera del territorio mexicano, realizada a persona distinta del titular, del responsable o del encargado.