POLÍTICAS DE PROTECCIÓN DE DATOS PERSONALES

AEROPUERTOS Y SERVICIOS AUXILIARES

Abril, 2022

Avenida 602, Núm. 161, Col. Zona Federal Aeropuerto Internacional Ciudad de México, C.P. 15620
Alcaldía Venustiano Carranza, CDMX. Tel: (55) 5133 1000 www.gob.mx/asa

Contenido

Avenida 602, Núm. 161, Col. Zona Federal Aeropuerto Internacional Ciudad de México, C.P. 15620
Alcaldía Venustiano Carranza, CDMX. Tel: (55) 5133 1000 www.gob.mx/asa

Avenida 602, Núm. 161, Col. Zona Federal Aeropuerto Internacional Ciudad de México, C.P. 15620
Alcaldía Venustiano Carranza, CDMX. Tel: (55) 5133 1000 www.gob.mx/asa

1. CONSIDERACIONES

Aeropuertos y Servicios Auxiliares (en lo sucesivo ASA y/u Organismo) 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.

ASA tiene como objeto principal administrar, operar, construir, remodelar y en su caso, ampliar aeropuertos y aeródromos civiles nacionales, principalmente aquellos que pertenecen a su red, además de prestar servicios aeroportuarios, complementarios y comerciales en ellos, y realizar la compraventa, almacenamiento y abastecimiento de combustibles que se requieran en aeropuertos nacionales; desarrollar tecnología en materia aeroportuaria, llevar a cabo investigaciones para el desarrollo tecnológico y profesional, y en general prestar servicios de consultoría, asesoría, asistencia técnica en materia aeroportuaria tanto a nivel nacional como internacional; siempre con la mejor calidad a fin de consolidarse en el mediano plazo, como una empresa que garantiza de forma transparente y confiable, la eficacia y eficiencia de sus servicios.

En este sentido, resulta importante tener en cuenta que de acuerdo con la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (en lo sucesivo Ley General) y los Lineamientos Generales de Protección de Datos Personales para el Sector Público (en lo sucesivo Lineamientos Generales), todas las dependencias y entidades de la administración pública federal son considerados sujetos obligados, motivo por el cual, siempre que realicen algún tratamiento de datos personales, adquieren el carácter de "Responsables" de los mismos y por lo tanto, tienen la obligación de apegarse a los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad; así como establecer las medidas de seguridad de carácter administrativo, físico y técnico que garanticen la confidencialidad, integridad y disponibilidad de los datos personales.

De manera particular, en el artículo 14 fracción VI, se establece la obligación del Sistema Nacional de Transparencia, Acceso a la Información y Protección de Datos de formular, establecer y ejecutar políticas generales en materia de protección de datos personales que en nuestro caso, formen parte del Sistema de Gestión de Seguridad de Datos Personales de ASA, las cuales determinan el alcance y objetivo de cumplir con los principios, deberes y demás obligaciones que establece la normatividad en la materia.

Asimismo, en los artículos 30, fracciones I, II, IV y VII de la Ley General y 47 de los Lineamientos Generales, se establece que, entre las acciones que deberán realizar los responsables del tratamiento de datos personales para cumplir con el principio de responsabilidad, está la elaboración de **políticas y programas** de protección de datos personales, obligatorios y exigibles al interior de la organización del responsable, en este caso ASA, así como destinar los recursos necesarios para la implementación de dichos programas y políticas.

Asimismo, el artículo 33 de la Ley General, establece en la fracción I, la obligación de los responsables de contar con **políticas** internas para el tratamiento y protección de los datos personales.

Lo señalado en el párrafo anterior, se establece con fundamento en el artículo 34 de la Ley General que a la letra dispone lo siguiente:

> ***"Artículo 34****. Las acciones relacionadas con las medidas de seguridad para el tratamiento de los datos personales deberán estar documentadas y contenidas en un sistema de gestión.*
>
> *Se entenderá por sistema de gestión al conjunto de elementos y actividades interrelacionadas para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el tratamiento y seguridad de los datos personales, de conformidad con lo previsto en la presente Ley y las demás disposiciones que le resulten aplicables en la materia."*

Avenida 602, Núm. 161, Col. Zona Federal Aeropuerto Internacional Ciudad de México, C.P. 15620
Alcaldía Venustiano Carranza, CDMX. Tel: (55) 5133 1000 www.gob.mx/asa

2. DISPOSICIONES GENERALES

a) Objetivo

El objetivo del presente documento, es establecer las Políticas de Protección de Datos Personales que operan al interior de ASA, estas políticas establecen las reglas y principios relacionados con el tratamiento de datos personales en ASA. El propósito es que el Organismo, use los datos de forma coherente y conforme los principios de la Ley General y los Lineamientos Generales.

Los tratamientos de datos personales que realicen las unidades administrativas deberán cumplir con los principios, deberes y obligaciones que prevé la normativa.

b) Fundamento

ASA en el ejercicio de sus atribuciones y funciones, realiza actividades comerciales, capacitación, licitación, y es necesario que el Organismo obtenga datos personales para llevar a cabo las diversas actividades.

En algunos tratamientos se incluye la necesidad de compartir datos personales con encargados y en algunos casos transferencias con terceros. Cualquier manejo de los datos personales conlleva el riesgo como la pérdida o divulgación accidental o no autorizada. Es por ello la necesidad de establecer una Política, para establecer las bases de la protección y de reconocer la importancia y la responsabilidad del Organismo en respetar los principios en la protección de datos personales.

La creación de la Política, representa también parte del Sistema de Gestión de Protección de Datos Personales, para salvaguardar la información y hacer uso responsable de la información a las que se tiene acceso.

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.
- Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal y el Protocolo Adicional al Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal, a las Autoridades de Control y a los Flujos Transfronterizos de Datos. Publicado en Diario Oficial de la Federación el 28 de septiembre de 2018.
- 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.
- Ley de Aeropuertos.
- Reglamento de la Ley de Aeropuertos.
- Lineamientos Generales de Protección de Datos Personales para el Sector Público, última reforma publicada en el Diario Oficial de la Federación el 25 de noviembre de 2020.
- Decreto por el que se modifica el similar que creó al organismo público descentralizado Aeropuertos y Servicios Auxiliares.

- Estatuto Orgánico de Aeropuertos y Servicios Auxiliares publicado en el Diario Oficial de la Federación el 23 de diciembre de 2011.

c) Ámbito de Aplicación

Estas políticas se aplican a todos los tratamientos de datos personales que el Organismo, en el ejercicio de sus atribuciones realice con motivo de un servicio, contrato u obligación.

El cumplimiento de estas Políticas de protección de datos personales es obligatorio para todo el personal del Organismo, sea que el tratamiento se lleve a cabo en oficinas centrales o en cualquier aeropuerto o estación de combustibles de la Red ASA.

d) Vigencia

Estas políticas, tendrán una vigencia hasta en tanto no se reformen la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados o en su caso; se emitan nuevas disposiciones que obliguen al Organismo a realizar tratamientos de datos personales en forma distinta.

3. PRINCIPIOS BASICOS

Aeropuertos y Servicios Auxiliares, se sujeta al tratamiento de los datos personales conforme a las atribuciones o facultades que la normatividad le confiere en su carácter de sujeto obligado; así como, en estricto apego y cumplimiento a lo dispuesto por la Ley General, los Lineamientos Generales, y, en su caso, el derecho internacional, respetando los derechos y libertades de los titulares.

Con la conformación de estas políticas se busca el cumplimiento en el Organismo de todos los principios que establece el artículo 16 de la Ley General, el cual a la letra ordena lo siguiente:

> *"Artículo 16. El responsable deberá observar los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad en el tratamiento de datos personales."*

Cada Unidad Administrativa designará un servidor público vinculado al tratamiento de datos personales, quién será el encargado de apoyar al Titular de la Unidad Administrativa de su adscripción para realizar lo establecido en las presentes Políticas y tendrá las siguientes funciones:

I. Adoptar las medidas de seguridad físicas, administrativas o técnicas, para la protección de los sistemas de tratamiento de datos personales bajo su responsabilidad, sea en soporte físico o electrónico, de forma que se evite su alteración, pérdida o acceso no autorizado;

II. Llevar una relación actualizada de las personas que tengan acceso al o los sistemas de datos personales que se encuentran en soporte físico o electrónico;

III. Coadyuvar en la aplicación y vigilancia del cumplimiento de las medidas de seguridad para la conservación y resguardo de los datos personales en el Organismo.

IV. Recibir la capacitación especializada en materia de protección de datos personales.

V. Coadyuvar en las auditorías que autorice el Comité de Transparencia o en los requerimientos que realice el INAI con motivo de un revisión o verificación del cumplimiento de la Ley General.

3.1 Licitud

Es obligación del Organismo, tratar y recabar datos personales de manera lícita, conforme a las disposiciones establecidas por la Ley General y Lineamientos Generales.

Los datos personales tienen que ser tratados por el responsable de manera lícita, lo que supone que el responsable debe sujetarse a las facultades o atribuciones que la normatividad aplicable le otorga.

El tratamiento de datos personales es una actividad que depende de las atribuciones o facultades que previamente le otorga la ley a los Sujetos Obligados, en consecuencia, no deben tratarse datos personales si no se tienen facultades previamente otorgadas.

El Organismo a través de sus Unidades Administrativas tiene las siguientes obligaciones en torno al principio de licitud:

1. Tratar siempre los datos personales de conformidad con las atribuciones o facultades conferidas por la normatividad, actuando con apego a la legislación mexicana, por lo que el responsable sólo podrá hacer con los datos personales aquello que esté legalmente permitido, como cualquier acto de autoridad.
2. El tratamiento se debe realizar tomando en consideración los derechos de los titulares.

3.2 Consentimiento

Es obligación del Organismo, sujetar el tratamiento de datos personales al consentimiento del titular, salvo las excepciones previstas por la Ley General.

El responsable deberá contar con el consentimiento del titular para el tratamiento de sus datos personales. La solicitud del consentimiento deberá ser conforme a las finalidades concretas que se informen en el aviso de privacidad, es decir, el consentimiento se deberá solicitar solo para las finalidades específicas.

El consentimiento debe ser informado, por lo que previo a su obtención, es necesario que el titular conozca el aviso de privacidad.

ASA realizará las siguientes actividades para respetar el consentimiento del titular:

1. ASA obtendrá el consentimiento del titular para el tratamiento de los datos personales, cuando no se actualice alguno de los supuestos de excepción del artículo 22 de la Ley General;
2. Solicitará el consentimiento conforme a las finalidades específicas e informadas en el aviso de privacidad;
3. Determinará el tipo de consentimiento que se requiere: tácito, expreso o expreso y por escrito;
4. Solicitará el consentimiento expreso y por escrito para los datos personales sensibles, cuando sea procedente;
5. Por regla general se solicitará el consentimiento previo a la obtención de los datos personales.

Avenida 602, Núm. 161, Col. Zona Federal Aeropuerto Internacional Ciudad de México, C.P. 15620
Alcaldía Venustiano Carranza, CDMX. Tel: (55) 5133 1000 www.gob.mx/asa

6. Implementará medios sencillos y gratuitos para la obtención del consentimiento, de acuerdo con el tipo de consentimiento que se requiera (tácito, expreso o expreso y por escrito)[1];
7. Llevará un control para identificar a los titulares que negaron su consentimiento, así como las finalidades concretas para las cuales no se podrán tratar los datos personales;
8. Esperar el plazo de cinco días hábiles que señala el artículo 15 de los Lineamientos Generales, para utilizar los datos personales, cuando éstos se hayan obtenido de manera indirecta, el aviso de privacidad se haya dado a conocer por un medio que no permita el contacto directo o personal con el titular y se requiera el consentimiento tácito;
9. Documentará la actuación de ASA para acreditar que se cumplió con el principio de consentimiento, y
10. Solicitará de nuevo el consentimiento cuando se realicen cambios a las finalidades.

3.3 Información

El Organismo debe Informar a los titulares de los datos, la información que se recaba de ellos y con qué fines, a través del aviso de privacidad.

Por medio del principio de información ASA se encuentra obligado a informar a los titulares, las características principales del tratamiento al que será sometida su información personal, para que puedan tomar decisiones informadas y ejercer su derecho a la protección de sus datos, esto se materializa a través del aviso de privacidad.

En torno a este principio, ASA deberá cumplir de manera puntual con lo siguiente:

1. Poner a disposición de los titulares el aviso de privacidad, aunque no se requiera el consentimiento de los titulares para el tratamiento de los datos personales;
2. Poner a disposición del titular el aviso de privacidad en forma previa a la obtención de los datos personales, cuando éstos se obtengan de manera personal y directa del titular;
3. Poner a disposición del titular el aviso de privacidad al primer contacto que se tenga con éste, cuando los datos personales se hayan obtenido de una transferencia consentida, de una que no requiera el consentimiento, o bien de una fuente de acceso público;
4. Poner a disposición del titular el aviso de privacidad previo a iniciar el uso de los datos personales para las nuevas finalidades, cuando el responsable requiera tratar los datos personales para finalidades distintas y no compatibles con aquéllas para las cuales los recabó inicialmente;
5. Redactar el aviso de privacidad de manera que sea claro, comprensible, con una estructura y diseño que facilite su entendimiento, para su elaboración tomará en cuenta el perfil de los titulares y atender lo

[1] **a) Consentimiento tácito**: se actualiza cuando, habiéndose puesto a disposición del titular el aviso de privacidad, éste no manifieste su oposición al tratamiento de sus datos. Es válido para dar tratamiento a cualquier tipo de dato personal con excepción de aquellos datos que revistan el carácter de datos personales patrimoniales, financieros o sensibles.
b) Consentimiento expreso: se actualiza cuando el titular de los datos personales manifiesta su voluntad verbalmente, ya sea por escrito, por medios electrónicos, ópticos, por cualquier otra tecnología, o por signos inequívocos. Dicho consentimiento es requerido cuando así lo exija una ley o reglamento, se trate de datos financieros o patrimoniales, datos sensibles, lo solicite el responsable para acreditar el mismo, o lo acuerden así el titular y el responsable.
c) Consentimiento expreso y por escrito: es obligatorio cuando se tratan datos personales sensibles. Se debe obtener a través de firma autógrafa, firma electrónica, o cualquier mecanismo de autenticación equivalente.

Avenida 602, Núm. 161, Col. Zona Federal Aeropuerto Internacional Ciudad de México, C.P. 15620
Alcaldía Venustiano Carranza, CDMX. Tel: (55) 5133 1000 www.gob.mx/asa

siguiente: no usar frases inexactas, ambiguas o vagas; incluir textos o formatos que induzcan al titular a elegir una opción en específico; no premarcar casillas en las que se solicite el consentimiento del titular, y no remitir a textos o documentos que no estén disponibles;

6. Ubicar el aviso de privacidad en un lugar visible y que facilite su consulta, con independencia del medio de difusión o reproducción que se utilice;
7. Comunicar el aviso de privacidad a encargados y terceros a los que remita o transfiera datos personales;
8. Demostrar el cumplimiento del principio de información, en caso de que así se requiera;
9. No establecer cobros para la consulta del aviso de privacidad, y
10. Poner a disposición de los titulares un **nuevo aviso de privacidad** en los siguientes casos:
    a) cambie la identidad del responsable;
    b) se requiera recabar nuevos datos personales sensibles, patrimoniales o financieros y se requiera el consentimiento del titular;
    c) se requiera tratar los datos personales para nuevas finalidades que requieran el consentimiento del titular, y
    d) se requiera realizar nuevas transferencias que requieran el consentimiento del titular.

3.4 Calidad

Cada Unidad Administrativa es responsable del tratamiento de datos personales, por lo que deberá adoptar las medidas necesarias para mantener exactos, completos, correctos y actualizados los datos personales en su posesión, a fin de que no se altere la veracidad de éstos.

El principio de calidad implica los siguientes elementos:

a) Procurar que los datos personales tratados sean exactos, correctos, completos y actualizados.

- **Exactos:** Se considera que los datos personales son exactos cuando reflejan la realidad de la situación de su titular, es decir, son verdaderos o fieles. También cuando no presentan errores que pudieran afectar su veracidad.
- **Completos:** Los datos personales están completos cuando no falta ninguno de los que se requieran para las finalidades para las cuales se obtuvieron y son tratados, de forma tal que no se cause un daño o perjuicio al titular.
- **Actualizados:** Los datos personales están actualizados cuando están al día y corresponden a la situación real del titular. De forma análoga, los Lineamientos Generales para la administración pública precisan que este elemento se cumple cuando los datos responden fielmente a la situación actual del titular.
- **Correctos:** Son correctos cuando cumplen con todas las características anteriores. Asimismo, son correctos cuando no presentan errores que pudieran afectar su veracidad.

b) Suprimir los datos personales cuando hayan dejado de ser necesarios para el cumplimiento de las finalidades para las cuales se obtuvieron.

Los plazos de conservación se determinan con base en la legislación en materia de archivos. El Organismo, a través de las Unidades Administrativas, debe considerar las disposiciones específicas para la conservación y supresión de la información.

Por lo tanto, debe existir un procedimiento para la supresión de los datos personales y se deben atender a los medios de almacenamiento, ya sean físicos o electrónicos.

c) Utilizar los datos personales únicamente el tiempo necesario y para el cumplimiento de las finalidades establecidas. Al término de las finalidades, los datos personales deben cancelarse previo periodo de bloqueo.[2]

El Organismo tiene las siguientes obligaciones en torno al principio de calidad:

- Adoptar las medidas que considere convenientes para procurar que los datos personales cumplan con las características de ser exactos, completos, actualizados y correctos, a fin de que no se altere la veracidad de la información.
- Conservar los datos personales exclusivamente por el tiempo que sea necesario para llevar a cabo las finalidades que justificaron el tratamiento y para cumplir con aspectos legales, administrativos, contables, fiscales, jurídicos e históricos y el periodo de bloqueo;
- Bloquear los datos personales antes de suprimirlos, y durante el periodo de bloqueo sólo tratarlos para su almacenamiento y acceso, en caso de que se requiera determinar posibles responsabilidades en relación con su tratamiento;
- Suprimir los datos personales, previo bloqueo, cuando haya concluido el plazo de conservación, de conformidad con lo establecido por la Ley General de Archivos;
- Establecer y documentar procedimientos para la conservación, bloqueo y supresión de los datos personales.
- Demostrar que los datos personales se conservan, bloquean y suprimen cumpliendo los plazos previstos para ello, o bien, en atención a una solicitud de ejercicio del derecho de cancelación.

3.5 Finalidad

Se entiende por finalidad del tratamiento, el propósito, motivo o razón por el cual se tratan los datos personales. El Organismo debe limitarse al tratamiento de los datos personales únicamente para el cumplimiento de las finalidades previstas en el aviso de privacidad.

Los datos personales obtenidos por ASA, serán utilizados para uno o más propósitos específicos y lícitos.

Los datos personales sólo pueden ser tratados para cumplir con la finalidad o finalidades que hayan sido informadas al titular en el aviso de privacidad y, en su caso, consentidas por éste.

Las finalidades deben ser concretas, explícitas, lícitas y legítimas:

[2] Bloqueo: Consiste en la identificación y conservación de datos personales una vez que cumplida la finalidad para la cual fueron recabados, con el único propósito de determinar posibles responsabilidades en relación con su tratamiento, hasta el plazo de prescripción legal o contractual de éstas. Durante dicho periodo, los datos personales no podrán ser objeto de tratamiento y, transcurrido éste, se procederá a su cancelación en la base de datos que corresponde.

- **Concretas:** Cuando el tratamiento de los datos personales atiende a la consecución de fines específicos o determinados, sin que admitan errores, distintas interpretaciones o provoquen incertidumbre, dudas o confusión en el titular.
- **Explícitas:** Tienen lugar cuando las finalidades se expresan y dan a conocer de manera clara en el aviso de privacidad.
- **Lícitas:** Cuando las finalidades que justifican el tratamiento de los datos personales son acordes con las atribuciones o facultades del responsable, conforme a lo previsto en la legislación mexicana y el derecho internacional que le resulte aplicable.
- **Legítimas:** Cuando las finalidades que motivan el tratamiento de los datos personales se encuentran habilitadas por el consentimiento del titular, salvo que se actualice alguna de las causales de excepción previstas en el artículo 22 de la Ley General.

Derivado del cumplimiento al principio de finalidad, el Organismo tiene las siguientes obligaciones:

1. Tratar los datos personales únicamente para la finalidad o finalidades que hayan sido informadas al titular en el aviso de privacidad y, en su caso, consentidas por éste.
2. Informar en el aviso de privacidad todas las finalidades para las cuales se tratarán los datos personales, y redactarlas de forma tal que sean específicas.
3. Identificar y distinguir en el aviso de privacidad entre las finalidades primarias que dan origen al tratamiento, de aquellas que son secundarias a las que lo originaron, pero se consideran compatibles y/o análogas.
4. Ofrecer al titular de los datos personales un mecanismo para que pueda manifestar su negativa al tratamiento de sus datos personales, para todas o algunas de las finalidades secundarias;
5. Cuando el aviso de privacidad se dé a conocer a través de un medio indirecto, como el correo postal, informar al titular que tiene cinco días hábiles para manifestar su negativa para el tratamiento de su información;
6. No tratar los datos personales para finalidades distintas que no resulten compatibles o análogas con aquéllas para las que se hubiese recabado de origen los datos personales y que hayan sido previstas en el aviso de privacidad, al menos que lo permita una ley o reglamento, o se obtenga el consentimiento del titular de los datos.

3.6 Lealtad

El Organismo, no obtendrá datos personales a través de medios fraudulentos y respetará la expectativa razonable de privacidad del titular.

De acuerdo con este principio la obtención de los datos personales no podrá hacerse a través de medios engañosos, ni fraudulentos, lo que implica que:

- No se recaben datos personales con dolo, mala fe o negligencia;
- No tratar los datos de tal manera que genere discriminación o un trato injusto contra los titulares.
- No se vulnere la confianza del titular con relación a que sus datos personales serán tratados conforme a lo acordado; y
- Se informen todas las finalidades del tratamiento en el aviso de privacidad.

Avenida 602, Núm. 161, Col. Zona Federal Aeropuerto Internacional Ciudad de México, C.P. 15620
Alcaldía Venustiano Carranza, CDMX. Tel: (55) 5133 1000 www.gob.mx/asa

ASA tiene las siguientes obligaciones en torno al principio de lealtad:

1) No hacer uso de medios engañosos o fraudulentos para la obtención de los datos personales.
2) Respetar en todo momento la expectativa razonable de privacidad del titular. [3]

3.7 Proporcionalidad

De acuerdo con este principio, el Organismo tratará el menor número de datos personales que sea posible para la consecución de la finalidad prevista, y sólo recabará aquéllos que resulten necesarios, adecuados y relevantes en relación con las finalidades previstas en el aviso de privacidad.

Los datos deben ser adecuados y pertinentes acordes a la finalidad identificada y no deben exceder el propósito para el cual se obtuvieron.

El Organismo, realizará esfuerzos para que los datos personales tratados sean los mínimos necesarios para lograr la finalidad o finalidades para las cuales se obtuvieron, conforme a las atribuciones del Organismo, señaladas en el aviso de privacidad.

En relación al principio de proporcionalidad, el Organismo realizará las siguientes actividades:

- Tratar sólo aquellos datos personales que resulten necesarios, adecuados y relevantes en relación con las finalidades para las cuales se obtuvieron.
- Limitar al mínimo posible el periodo de tratamiento de datos personales sensibles.
- Crear bases de datos con datos personales sensibles sólo cuando se cuente con el consentimiento expreso de su titular o en su defecto, se trate de los casos establecidos en el artículo 22 de la Ley General en la materia.

3.8 Responsabilidad

El principio de responsabilidad, significa que el Organismo debe adoptar las medidas necesarias para el cumplimiento de todos los principios.

El Organismo está obligado a velar por la protección de los datos personales aun y cuando los datos estén siendo tratados por encargados.

Entre las medidas que debe adoptar el Organismo para cumplir con principio de responsabilidad, el artículo 30 de la Ley General establece lo siguiente:

> *"I. Destinar recursos autorizados para establecer programas y políticas de protección de datos personales;*
> *II. Elaborar políticas y programas de protección de datos personales, obligatorios y exigibles al interior de la organización del responsable;*

[3] Expectativa razonable de privacidad del titular: se entiende como "la confianza que deposita cualquier persona en otra, respecto de que los datos personales proporcionados entre ellos serán tratados conforme a lo que acordaron las partes en los términos establecidos por la Ley".

III. Poner en práctica un programa de capacitación y actualización del personal sobre las obligaciones y demás deberes en materia de protección de datos personales;
IV. Revisar periódicamente las políticas y programas de seguridad de datos personales para determinar las modificaciones que se requieran;
V. Establecer un sistema de supervisión y vigilancia interna y/o externa, incluyendo auditorías, para comprobar el cumplimiento de las políticas de protección de datos personales;
VI. Establecer procedimientos para recibir y responder dudas y quejas de los titulares;
VII. Diseñar, desarrollar e implementar sus políticas públicas, programas, servicios, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento de datos personales, de conformidad con las disposiciones previstas en la presente Ley y las demás que resulten aplicables en la materia, y
VIII. Garantizar que sus políticas públicas, programas, servicios, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento de datos personales, cumplan por defecto con las obligaciones previstas en la presente Ley y las demás que resulten aplicables en la materia."

El Organismo tiene las siguientes obligaciones en torno al principio de responsabilidad:

- Velar por el cumplimiento de los principios y responder por el tratamiento de los datos personales, aún por aquéllos comunicados a encargados;
- Adoptar medidas para garantizar el debido tratamiento, privilegiando los intereses del titular y la expectativa razonable de privacidad, y
- Tomar medidas para que los terceros con quienes mantiene una relación jurídica que implique el tratamiento de los datos personales, respeten el aviso de privacidad en el que se establezcan las condiciones de dicho tratamiento.

3.9 Seguridad

Con el fin de garantizar la confidencialidad e integridad de los datos personales, es necesario poner en práctica adecuadas medidas de seguridad físicas, técnicas y administrativas en el Organismo.

El Organismo deberá establecer y mantener las medidas de seguridad de carácter administrativo, físico y técnico, que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción, uso, acceso o tratamiento no autorizado, así como garantizar su confidencialidad, integridad y disponibilidad.

Con la finalidad de atender al principio de Seguridad, ASA deberá considerar realizar 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.
e) Prevenir que el acceso a las bases de datos o a la información, así como a los recursos, sea por usuarios identificados y autorizados;

Avenida 602, Núm. 161, Col. Zona Federal Aeropuerto Internacional Ciudad de México, C.P. 15620
Alcaldía Venustiano Carranza, CDMX. Tel: (55) 5133 1000 www.gob.mx/asa

f) Generar un esquema de privilegios para que el usuario lleve a cabo las actividades que requiere con motivo de sus funciones;
g) Revisar la configuración de seguridad en la adquisición, operación, desarrollo y mantenimiento del software y hardware, y
h) Gestionar las comunicaciones, operaciones y medios de almacenamiento de los recursos informáticos en el tratamiento de datos personales.

Las acciones relacionadas con las medidas de seguridad para el tratamiento de los datos personales que implementen las Unidades Administrativas, deberán estar documentadas y contenidas en el Sistema de Gestión de Protección de Datos Personales.

3.10 Confidencialidad

El personal del Organismo debe mantener la confidencialidad de los datos personales, incluso una vez finalizada la relación con el Organismo.

Por confidencialidad se entiende que el responsable debe establecer controles o mecanismos que tengan por objeto que todas aquellas personas que traten datos personales, en cualquier fase del tratamiento mantengan en secreto la información, así como evitar que la información sea revelada a personas no autorizadas y prevenir la divulgación no autorizada de la misma.

Por lo anterior, la confidencialidad implica la obligación de guardar secreto respecto de los datos personales que son tratados, para evitar causar un daño a su titular.

Cuando se tratan datos personales, ASA adoptará medidas para evitar que quienes tengan acceso a los datos personales, divulguen la información, incluso una vez que finalice la relación jurídica, a través de cláusulas de confidencialidad establecidas en los instrumentos jurídicos suscritos entre el responsable del tratamiento y quien tenga acceso a los datos personales.

4. DERECHOS DE LOS TITULARES

Los titulares, tienen derecho a acceder a sus datos personales, rectificarlos, a solicitar que se eliminen o cancelen, así como a oponerse a su uso. A estos se les conoce como Derechos ARCO y están reconocidos en el artículo 16 de la Constitución Política de los Estados Unidos Mexicanos.

Como cualquier otro derecho, el de protección de datos personales tiene excepciones, por lo que los derechos ARCO no podrán ejercerse o su ejercicio se verá limitado por cuestiones de seguridad nacional; orden, seguridad y salud públicos, así como por derechos de terceros.

El derecho a la protección de datos personales es un derecho personalísimo, por lo que solamente el titular de tus datos personales o, en su caso, su representante legal podrá solicitar el ejercicio de los derechos ARCO.
Los servidores públicos están obligados en todo momento a garantizar las condiciones y requisitos necesarios para el adecuado tratamiento, así como la debida administración y custodia de los datos personales que se encuentren bajo su resguardo, con el objeto de maximizar el ejercicio de los derechos ARCO.

4.1 Acceso

Se debe permitir a los titulares, el derecho a solicitar el acceso a sus datos personales que están en las bases de datos, sistemas, archivos, registros o expedientes del Organismo que los posee, almacena o utiliza, así como de conocer información relacionada con el uso que se da a su información personal.

4.2 Rectificación

Es el derecho de los titulares de solicitar la modificación o corrección de sus datos personales, cuando éstos sean inexactos o incompletos o no se encuentren actualizados. Es decir, los titulares cuentan con el derecho a solicitar a quien posea o utilice tus datos personales que los corrija.

4.3 Cancelación

Es el derecho a solicitar a los responsables, que sus datos personales se eliminen de los archivos, registros, expedientes, sistemas, bases de datos del Organismo, cuando los posee, almacena o utiliza.

Sin embargo, es importante señalar que no en todos los casos se podrán eliminar tus datos personales, principalmente cuando sean necesarios por alguna cuestión legal o para el cumplimiento de obligaciones.

4.4 Oposición

Es el derecho a solicitar que los datos personales no se utilicen para ciertos fines, o de requerir que se concluya el uso de los mismos para evitar un daño a tu persona. Aunque, no siempre se podrá impedir el uso de los datos personales, cuando sean necesarios por alguna cuestión legal o para el cumplimiento de obligaciones.

Para el ejercicio de los derechos ARCO será necesario acreditar la identidad del titular y, en su caso, la identidad y personalidad con la que actúe el representante. En los casos en que el ejercicio de los derechos ARCO de menores de edad o de personas que se encuentren en estado de interdicción o incapacidad, de conformidad con las leyes civiles, se estará a las reglas de representación dispuestas en la misma legislación.

Las solicitudes para el ejercicio de los derechos ARCO deberán presentarse ante la Plataforma Nacional de Transparencia o en forma presencial ante la Unidad de Transparencia, por medio de escrito libre, formatos o medios electrónicos.

5. TRATAMIENTO DE DATOS PERSONALES EN ASA

El Organismo realizará el tratamiento de datos personales conforme al Sistema de Gestión de Seguridad de Datos Personales (Sistema de Gestión) y del cual las presentes políticas forman parte. La implementación del Sistema de Gestión de seguridad de Datos Personales se traduce en la puesta en práctica de los deberes de seguridad y confidencialidad.

5.1 Seguridad de los datos personales

Para una efectiva protección de los datos personales ASA disppone con un Sistema de Gestión de Seguridad de Datos Personales (Sistema de Gestión), que permite planificar, implementar, monitorear y mejorar las medidas de seguridad de carácter administrativo, físico y técnico, a través de una serie de actividades interrelacionadas y documentadas, tomando en consideración los estándares nacionales e internacionales en materia de protección de datos personales y seguridad.

Avenida 602, Núm. 161, Col. Zona Federal Aeropuerto Internacional Ciudad de México, C.P. 15620
Alcaldía Venustiano Carranza, CDMX. Tel: (55) 5133 1000 www.gob.mx/asa

La seguridad de la información debe preservar la confidencialidad, integridad y disponibilidad de los datos personales, los cuales se definen a continuación:

- **Integridad**: es la propiedad de salvaguardar la exactitud y completitud de la información, así como evitar la modificación no autorizada o accidental de la misma.
- **Confidencialidad**: es la propiedad de la información que impide la disposición a personas distintas a los titulares, así como la posibilidad de que sea revelada a personas no autorizadas.
- **Disponibilidad**: es la propiedad de un dato para que se encuentre accesible y utilizable por los titulares o personal autorizado, y que además previene interrupciones no autorizadas.

El Sistema de Gestión de Seguridad de Datos Personales (Sistema de Gestión) está basado en el ciclo PHVA (Planear-Hacer-Verificar-Actuar).

5.3 Vulneraciones a la seguridad

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

La vulnerabilidad es la "falta o debilidad en la 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, así como 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 plan para tomar acciones que permitan el manejo de las vulneraciones de seguridad que puedan ocurrir, considerando lo siguiente:

a) Identificación de la vulneración.

En caso de un incidente de seguridad, ASA debe identificar los recursos o activos afectados, el personal a cargo; los titulares afectados; partes interesadas para la toma de decisiones para terminar, suspender o mitigar la vulneración.

b) 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 preventivas o evitar una posible afectación.

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.

c) Remediación del incidente.

Una vez identificada la vulneración y después de haber realizado la respectiva notificación, se deben analizar las causas del incidente, a fin de establecer medidas en forma inmediata para reducir los efectos de la vulneración.

Las revisiones, auditorías y los tratamientos de una vulneración a la seguridad deben estar debidamente documentados con objeto de contar con evidencia suficiente.

El Organismo deberá analizar las causas por las cuales se presentó la vulneración y deberá implementar acciones preventivas y correctivas para adecuar las medidas de seguridad, a fin de evitar que vuelva a ocurrir una vulneración.

5.4 Evaluaciones de impacto de protección de datos personales

En caso de que se decida elaborar nuevos programas, políticas, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento intensivo o relevante de datos personales, se solicitara la evaluación correspondiente al INAI conforme al procedimiento establecido.

Lo anterior, con la finalidad de identificar y mitigar posibles riesgos relacionados con los principios, deberes y derechos de los titulares antes de su posible ocurrencia, así como verificar el cumplimiento de los deberes de los responsables y encargados.

6. TRANSFERENCIAS DE DATOS PERSONALES

6.1 Transferencias de Datos Personales

La Ley General define como transferencia en el artículo 3 fracción XXXII, a toda comunicación de datos personales dentro o fuera del territorio mexicano, realizada a persona distinta del titular, del responsable o del encargado.

La transferencia de datos personales puede ser nacional o internacional, según el destino de los datos personales. Este tipo de transferencias están reguladas de forma distinta y es necesario que se cumpla con todos los principios y deberes de la protección de datos que establecen la Ley General y los Lineamientos Generales.

Para que ASA pueda transferir los datos personales, dentro o fuera de México, es necesario que:

1. Se informe al titular en el aviso de privacidad quien es el destinatario de las transferencias ya sea en el ámbito público como privado, y además se deberán señalar las finalidades de esas transferencias. En caso de ser una transferencia que requiera consentimiento, se deberán habilitar los mecanismos correspondientes.

2. El titular haya otorgado su consentimiento para que la transferencia se realice, salvo los casos de excepción previstos en los artículos 22, 66 y 70 de la Ley General (este tipo de transferencias es opcional incluirlas en el aviso de privacidad integral). Es importante precisar que en algunos casos no se requerirá el consentimiento de los titulares para realizar transferencias, como pueden ser:

- Por disposición expresa de una ley;
- Cuando las transferencias se realicen entre responsables, para el ejercicio de facultades propias, compatibles o análogas con la finalidad que motivó el tratamiento;
- Cuando exista una orden judicial, resolución o mandato fundado y motivado de autoridad competente;
- Para el reconocimiento o defensa de derechos del titular ante autoridad competente;

- Para ejercer un derecho o cumplir obligaciones derivadas de una relación jurídica;
- Cuando exista una situación de emergencia;
- Asistencia sanitaria;
- Los datos se encuentren en fuentes de acceso público;
- Los datos personales sean sometidos a un procedimiento de disociación;
- El titular de los datos sea una persona reportada como desaparecida;
- Cuando la transferencia sea nacional y se realice entre responsables en virtud del cumplimiento de una disposición legal;
- Cuando la transferencia sea internacional, en cumplimiento en una ley o tratado internacional suscrito y ratificado por el estado mexicano;
- A petición de una autoridad u organismo extranjero, competente en su carácter de receptor, cuyas facultades sean homólogas;
- Cuando la transferencia sea necesaria para ejecutar un contrato celebrado o por celebrar en interés del titular;
- La transferencia sea necesaria por razones de seguridad.
- Por otra parte, el receptor en su carácter de responsable, deberá cumplir con lo establecido en la normatividad aplicable en materia de datos personales, ya sea que pertenezca al sector público o privado.

6.2 Acuerdos de Transferencia de Datos Personales

Teniendo en cuenta los posibles riesgos de protección de datos personales que implican las transferencias a terceros, el Organismo debe atender las siguientes obligaciones, antes de autorizar las transferencias de datos personales:

1. Todas las transferencias sean nacionales e internacionales deben formalizarse mediante la suscripción de un instrumento jurídico, para demostrar el alcance del tratamiento de los datos personales, las obligaciones y responsabilidades contraídas por las partes, salvo en las siguientes excepciones:

    a) Cuando la transferencia sea nacional y se realice en virtud del cumplimiento de una disposición legal o en el ejercicio de las atribuciones expresamente conferidas.
    b) Cuando la transferencia sea internacional y se encuentre prevista en una ley o tratado suscrito y ratificado por México, o derivado de una petición de la autoridad extranjera u organismo internacional en su carácter de receptor,
    c) Cuando las facultades entre el sujeto obligado y el responsable receptor sean homólogas o las transferencias sean análogas respecto de aquéllas que dieron origen al tratamiento.

2. Sólo hacer transferencias fuera del territorio nacional cuando el tercero receptor se obligue a proteger los datos personales conforme a los principios y deberes que establece la Ley General y demás disposiciones aplicables en la materia.
3. Comunicar el aviso de privacidad respectivo al tercero receptor en las transferencias nacionales e internacionales que se realicen.
4. Solicitar el consentimiento para las transferencias nacionales e internacionales, salvo en los siguientes casos:

Avenida 602, Núm. 161, Col. Zona Federal Aeropuerto Internacional Ciudad de México, C.P. 15620
Alcaldía Venustiano Carranza, CDMX. Tel: (55) 5133 1000 www.gob.mx/asa

a) Cuando la transferencia sea nacional y se realice entre ASA y otros responsables en virtud del cumplimiento de una disposición legal o en el ejercicio de atribuciones expresamente conferidas a éstos;
b) Cuando la transferencia se encuentre prevista en una ley o tratado suscrito y ratificado por México;
c) Cuando la transferencia sea entre responsables y derivado de sus atribuciones análogas o compatibles con la finalidad que dio origen al tratamiento;
d) No será necesario el consentimiento cuando se trate una transferencia legalmente exigida para la investigación y persecución de los delitos, o bien, la procuración o administración de justicia;
e) Cuando la transferencia sea precisa para el reconocimiento, ejercicio o defensa de un derecho;
f) Cuando la transferencia tenga como finalidad el mantenimiento o cumplimiento de una relación jurídica entre el sujeto obligado y el titular;
g) Cuando la transferencia sea necesaria por virtud de un contrato en interés del titular, por el sujeto obligado y un tercero;
h) Cuando se trate de los casos en los que ASA no esté obligado a recabar el consentimiento del titular para el tratamiento y transmisión de sus datos personales, conforme a lo dispuesto en el artículo 22 de la Ley General, y
i) Sea necesaria por razones de seguridad nacional.

3. ASA deberá establecer el medio para obtener el consentimiento expreso del titular de forma previa a la transferencia de los datos personales.
4. En caso de que la transferencia sea nacional, el receptor deber observar la confidencialidad y la obligación de utilizar los datos personales únicamente para los fines que fueron transferidos atendiendo a lo convenido en el aviso de privacidad

7. MECANISMOS DE MONITOREO Y SUPERVISIÓN

7.1 Estructura de rendición cuentas y supervisión

De acuerdo con lo dispuesto por la Ley General, los responsables tienen la obligación de monitorear y revisar de manera periódica las medidas de seguridad implementadas, así como las amenazas y vulneraciones a las que puedan estar sujetos los datos personales.

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

Con el fin de garantizar el tratamiento de datos personales de acuerdo con las Políticas, y así disponer de una estructura de rendición de cuentas y supervisión, el Organismo puede elegir por una auditoría interna o externa.

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.*

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). El resultado de la Auditoria Voluntaria por parte del INAI nos permite identificar lo siguiente:

- 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.
- Brindar transparencia y confianza al responsable sobre las medidas que ha implementado en los tratamientos que realiza.

7.2 Comité de Transparencia de ASA

ASA cuenta con un Comité de Transparencia, que de conformidad con el artículo 83 de la Ley General, es la autoridad máxima en materia de protección de datos personales.

Dicho Comité de Transparencia tiene las siguientes atribuciones y funciones en materia de protección de datos personales, de acuerdo con lo dispuesto por el artículo 84 de la Ley General:

> *"I. Coordinar, supervisar y realizar las acciones necesarias para garantizar el derecho a la protección de los datos personales en la organización del responsable, de conformidad con las disposiciones previstas en la presente Ley y en aquellas disposiciones que resulten aplicables en la materia;*
>
> *II. Instituir, en su caso, procedimientos internos para asegurar la mayor eficiencia en la gestión de las solicitudes para el ejercicio de los derechos ARCO;*
>
> *III. Confirmar, modificar o revocar las determinaciones en las que se declare la inexistencia de los datos personales, o se niegue por cualquier causa el ejercicio de alguno de los derechos ARCO;*
>
> *IV. Establecer y supervisar la aplicación de criterios específicos que resulten necesarios para una mejor observancia de la presente Ley y en aquellas disposiciones que resulten aplicables en la materia;*
>
> *V. Supervisar, en coordinación con las áreas o unidades administrativas competentes, el cumplimiento de las medidas, controles y acciones previstas en el documento de seguridad;*
>
> *VI. Dar seguimiento y cumplimiento a las resoluciones emitidas por el Instituto y los organismos garantes, según corresponda;*

VII. Establecer programas de capacitación y actualización para los servidores públicos en materia de protección de datos personales, y

VIII. Dar vista al órgano interno de control o instancia equivalente en aquellos casos en que tenga conocimiento, en el ejercicio de sus atribuciones, de una presunta irregularidad respecto de determinado tratamiento de datos personales; particularmente en casos relacionados con la declaración de inexistencia que realicen los responsables."

7.3 Oficial de Datos Personales

El Organismo analizará la posibilidad de nombrar a un Oficial de Protección de Datos, que permita al Organismo implementar políticas y medidas de seguridad, así como los programas en la materia de datos personales.

En ese entendido, el Oficial de Protección de Datos Personales, tendrá entre otras funciones las siguientes:

- Asesorar al Comité de Transparencia respecto a los temas que sean sometidos a su consideración en materia de protección de datos personales;
- Proponer al Comité de Transparencia políticas, programas, acciones y demás actividades que correspondan para el cumplimiento de la Ley General y los Lineamientos Generales;
- Implementar políticas, programas, acciones y demás actividades que correspondan para el cumplimiento de la Ley General y los Lineamientos Generales, previa autorización del Comité de Transparencia;
- Asesorar permanentemente a las áreas adscritas a ASA en materia de protección de datos personales, y
- Proporcionar asesoramiento, apoyo y capacitación en materia de protección de datos y la presente Política.
- Mantener inventarios de información proporcionada por los enlaces de la Unidades Administrativas y los puntos focales de protección de datos, evaluaciones de impacto de protección de datos, notificaciones de filtración de datos y quejas de los titulares de los datos;
- Fomentar activamente que los controladores de datos y otros actores pertinentes adopten medidas encaminadas al cumplimiento de esta Política;
- Monitorear y presentar informes sobre el cumplimiento de esta Política;
- Coordinar con los enlaces administrativos según sea necesario en virtud de la presente Política.
- Las demás que determine ASA y la normatividad que resulte aplicable.

8. DEFINICIONES

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 su integridad. 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.

Avenida 602, Núm. 161, Col. Zona Federal Aeropuerto Internacional Ciudad de México, C.P. 15620
Alcaldía Venustiano Carranza, CDMX. Tel: (55) 5133 1000 www.gob.mx/asa

- **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.

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.

Avenida 602, Núm. 161, Col. Zona Federal Aeropuerto Internacional Ciudad de México, C.P. 15620
Alcaldía Venustiano Carranza, CDMX. Tel: (55) 5133 1000 www.gob.mx/asa

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.

El presente documento denominado “Políticas de Protección de Datos Personales de Aeropuertos y Servicios Auxiliares, fue aprobado por unanimidad por el Comité de Transparencia de Aeropuertos y Servicios Auxiliares en su octava sesión extraordinaria del 04 de mayo de 2022, de conformidad con los artículos 30 fracción II, 83 y 84 fracción I y 87 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y 47 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público.