MARINA
GRUPO AEROPORTUARIO

POLÍTICA INTERNA DE GESTIÓN Y TRATAMIENTO DE LOS DATOS PERSONALES

AEROPUERTO INTERNACIONAL DE LA CIUDAD DE MÉXICO, S.A. DE C.V.

INDICE

PRESENTACIÓN

El derecho a la protección de datos personales, es el derecho que tienen todas las personas para decidir, de manera libre e informada, sobre el uso de su información personal. Es un derecho humano reconocido por el artículo 16, segundo párrafo, de la Constitución Política de los Estados Unidos Mexicanos. Es un derecho fundamental de tercera generación que busca la protección de la persona en relación con el tratamiento de su información personal.

El titular de los datos personales, es el dueño de los mismos, aun cuando éstos se encuentren en posesión de un tercero para su tratamiento.

Aeropuerto Internacional de la Ciudad de México, S.A. de C.V. (AICM) al ser una empresa de participación estatal mayoritaria, en términos del artículo 3 de la Ley Orgánica de la Administración Pública Federal, tiene la obligación de proteger los datos personales que obran en sus archivos y sobre los cuales efectúa algún tratamiento y es responsable de lo que suceda con los mismos, el tiempo que estén bajo su guarda y custodia.

En este documento se presenta la Política interna de gestión y tratamiento de los datos personales, emitida en cumplimiento a lo dispuesto por el artículo 27, fracción I de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y al artículo 56 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público.

I. MARCO JURÍDICO.

- Constitución Política de los Estados Unidos Mexicanos.
- Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.
- Ley General de Transparencia y Acceso a la Información Pública.

- Lineamientos Generales de Protección de Datos Personales para el Sector Público.
- Acuerdo mediante el cual se aprueban los Instrumentos Técnicos que refiere el Título Décimo de los Lineamientos Generales de Protección de Datos Personales para el Sector Público.
- Manual General de Organización de Aeropuerto Internacional de la Ciudad de México, S.A. de C.V.

II. DEFINICIONES.

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

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 pueda 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.

Persona Encargada: La persona física o jurídica, pública o privada, ajena a la organización AICM que, sola o conjuntamente con otras trate datos personales a nombre y por cuenta de la Entidad.

.

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

Lineamientos: Lineamientos Generales de Protección de Datos Personales para el Sector Público.

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.

Unidades Administrativas: Direcciones, Subdirecciones y Gerencias que integran a la Entidad AICM.

Unidades Responsables: Unidades Administrativas responsables del tratamiento de datos personales.

III. OBJETIVO Y ALCANCE.

Establecer los principios que deben observar y los deberes que deben cumplir los servidores públicos de Aeropuerto Internacional de la Ciudad de México, S.A. de C.V., para el tratamiento y protección de los datos personales, conforme a lo previsto en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO) y los Lineamientos de Protección de Datos Personales para el Sector Público.

La Política es de aplicación y observancia general y obligatoria para todas las personas servidoras públicas que conforma las Unidades Administrativas de AICM y, en particular, para quienes conforme a sus atribuciones realicen tratamiento de datos personales, es decir, obtengan, usen, registren, organicen, conserven, elaboren, utilicen, comuniquen, difundan, almacenen, posean, manejen, aprovechen, divulguen, transfieran o dispongan de los datos personales.

IV. DISPOSICIONES GENERALES.

1. El tratamiento de datos personales se debe realizar con base en las atribuciones conferidas a cada una de las Unidades Administrativas de AICM (Unidades Responsables) y con el consentimiento de la persona titular**.**
2. Es obligación de todas las personas servidoras públicas de AICM que administren, actualicen o tengan acceso a bases de datos personales, conservar, manejar y mantener de manera estrictamente confidencial dicha información y no revelarla a terceros.
3. La Unidades Responsables deben asegurar que las Personas Encargadas que tratan datos personales en nombre de AICM cumplen con lo establecido en la normatividad en materia de protección de datos personales, así como en lo establecido en la Política Interna de Datos Personales y el Documento de Seguridad de AICM.
4. Las Unidades Responsables deben contar con los avisos de privacidad integral y simplificado, que contengan todos los elementos informativos que exige la normatividad.
5. Las Unidades Responsables deben publicar sus avisos de privacidad en el portal de Internet de AICM, de manera impresa, en donde se traten datos personales, en un lugar visible y de fácil consulta para las personas titulares.
6. Al momento de recabar datos personales, las Unidades Responsables deberán hacer del conocimiento de la persona titular la finalidad con la cual se reciben.
7. Las Unidades Responsables deberán solicitar a la persona titular, de manera tácita o expresa, el consentimiento para la obtención y uso de sus datos personales, salvo las excepciones prevista en la Ley.
8. Cuando se recaben datos personales de menores de edad, se deberá obtener el consentimiento expreso de quien o quienes ejerzan la patria potestad o tutela sobre ellos.

V. PRINCIPIOS

En términos del artículo 10 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y artículo 7 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público, se establece que en todo tratamiento de datos personales se deberán observar los principios rectores de la protección de datos personales.

1. **Licitud:** La Unidad Responsable debe tratar los datos personales sujetándose a las atribuciones y facultades que la normatividad le otorga.

   Para cumplir con el principio de Licitud las Unidades Responsables deben seguir las siguientes recomendaciones:

   a. Revisar que los datos personales se traten conforme a la LGPDPPSO, Lineamientos Generales de Protección de Datos Personales para el Sector Público y demás normativa aplicable.
   b. Conocer la normativa que en lo particular regule sus atribuciones, funciones y responsabilidades con relación al tratamiento de los datos personales.
   c. Incluir los supuestos sobre la obligación de cumplir con este principio en las cláusulas, contratos u otros instrumentos jurídicos que se firmen con terceros.

2. **Finalidad:** Los datos personales sólo pueden ser tratados para cumplir con el propósito, motivo o razón para el que fueron solicitados e informados a la persona titular en el aviso de privacidad y, en su caso, consentidas por ésta.

   Para cumplir con este principio, las Unidades responsables deben:

   a. Verificar que el aviso de privacidad incluye todas las finalidades para las cuales se tratarán los datos personales.
   b. Asegurar que los datos personales serán tratados únicamente para la finalidad o finalidades informadas en el aviso de privacidad y consentidas por la persona titular.

c. Identificar y distinguir en el aviso de privacidad entre las finalidades primarias, es decir, se deberá precisar el motivo por el cual se solicitaron los datos personales, así mismo, si fuera el caso se deberá precisar las finalidades secundarias, es decir precisar además cuales serían los demás supuestos por los cuales se utilizarían los datos personales.
d. Ofrecer a la persona 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.
e. Cuando el aviso de privacidad se dé a conocer a través de un medio indirecto, es decir se ponga a la vista del titular de los datos personales, informar a la persona titular que tiene cinco días hábiles para manifestar su negativa para el tratamiento de su información para finalidades secundarias.
f. No condicionar el tratamiento para finalidades primarias, a que se puedan llevar a cabo las finalidades secundarias

3. **Lealtad.** La obtención de los datos personales no podrá hacerse a través de medios engañosos, ni fraudulentos.

   Para cumplir con este principio, las Unidades Administrativas deben verificar que:

   a. En los procedimientos y formatos utilizados para recabar datos personales no se utilicen prácticas que lleven a la obtención de los datos de manera dolosa, de mala fe o con negligencia.
   b. Los tratamientos no den lugar a discriminación o trato injusto o arbitrario en contra de la persona titular.

4. **Consentimiento.** Se debe contar con el consentimiento de la persona titular para el tratamiento de sus datos personales, de acuerdo con las finalidades concretas señaladas en el aviso de privacidad.

   Para cumplir con este principio, las Unidades Responsables deben:

a. Precisar las finalidades para las que se requiere el consentimiento de los titulares y definir el tipo de consentimiento que se requiere: tácito, es decir: inactividad o silencio del titular de los datos personales o expreso, dejando constancia de su consentimiento para tratar sus datos.
b. Cuando los datos personales se obtengan directamente de su titular o representante se debe solicitar el consentimiento previo a la obtención de los datos personales y después de la puesta a disposición del aviso de privacidad.
c. Cuando los datos personales no los proporcione personal o directamente la persona titular o su representante, se deberá enviar el aviso de privacidad a la persona titular por el medio de contacto que se tenga registrado, informándole que cuenta con un plazo de 5 días hábiles para manifestar su negativa para el tratamiento de sus datos personales para aquellas finalidades que requieran su consentimiento.
d. En caso de que el tratamiento de los datos requiera consentimiento expreso, la Unidad Responsable debe:
    - Solicitar el consentimiento en el aviso de privacidad o en un instrumento aparte.
    - Proveer los mecanismos para solicitar el consentimiento expreso y para facilitar a la persona titular un medio sencillo y gratuito para manifestar su voluntad.
    - Redactar la solicitud de consentimiento en forma concisa e inteligible, con un lenguaje claro y sencillo, acorde con el perfil del titular.
e. No se podrán tratar los datos personales si no cuenta con el consentimiento expreso de la persona titular.

5. **Calidad.** Conforme a la finalidad o finalidades para las que se requieren los datos personales, estos deben ser:

    - Exactos: Reflejan la realidad de la situación de su titular, es decir, son verdaderos o fieles.

- Completos: No falta ninguno de los que se requieren para la finalidad o finalidades para las cuales se obtuvieron, de forma tal que no se cause un daño o perjuicio a la persona titular.
- Actualizados: Corresponden a la situación real de su titular.
- Correctos: Cumplen con todas las características anteriores, es decir, son exactos, completos y actualizados.

Para cumplir con este principio, las Unidades Responsables deberán:

a. Adoptar las medidas necesarias para procurar que los datos personales sean correctos.
b. 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.
c. Bloquear los datos personales antes de suprimirlos. Durante el periodo de bloqueo sólo tratarlos para su almacenamiento y acceso en caso de que se requiera determinar posibles responsabilidades en relación con el tratamiento de los datos personales.
d. Suprimir los datos personales, previo bloqueo, cuando haya concluido el plazo de conservación.

6. **Proporcionalidad.** Se deberán tratar solo los datos personales que resulten necesarios, adecuados y relevantes en relación con las finalidades para las cuales se obtuvieron.

   Para cumplir con este principio, las Unidades Responsables deben:

   a. Tratar el menor número posible de datos personales.
   b. Limitar al mínimo posible el periodo de tratamiento de datos personales sensibles.

c. Crear bases de datos con datos personales sensibles sólo cuando sea por cumplimiento a la normatividad o para finalidades legítimas, concretas y acordes con las actividades o fines explícitos que persiga.

7. **Información:** Las Unidades Responsables están obligadas a informar a las personas titulares, a través del aviso de privacidad integral y simplificado, las características principales del tratamiento al que serán sometidos sus datos, a fin de que pueda tomar decisiones informadas al respecto.

   Para cumplir con este principio, las áreas deben:

   a. Redactar el aviso de privacidad de manera sencilla, comprensible y con una estructura y diseño que facilite su entendimiento.
   b. Poner a disposición de las personas titulares el aviso de privacidad:
      - Previo a la obtención de los datos personales cuando se obtengan de manera directa.
      - Al primer contacto que se tenga con el titular, 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.
      - Previo a iniciar el uso de los datos personales, cuando éstos no se hayan obtenido **de manera directa de la persona titular**, el tratamiento no requiera del contacto con ésta y se cuente con datos para contactarle.
      - Previo a iniciar el uso de los datos personales para nuevas finalidades, distintas y no compatibles con aquéllas para las cuales los recabó inicialmente.
   c. Comunicar el aviso de privacidad a encargados y terceros a los que remita o transfiera datos personales.

8. **Responsabilidad.** Se deben adoptar las medidas para acreditar el cumplimiento de los principios, deberes y obligaciones en torno a la protección de los datos personales.

   Para cumplir con este principio, las Unidades Responsables deben:

a. Establecer y mantener medidas de seguridad tanto técnicas, físicas y administrativas, que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado.
b. Establecer un sistema de supervisión y vigilancia para comprobar el cumplimiento de las políticas en materia de protección de datos personales.
c. Cumplir con el programa anual de capacitación en materia de protección de datos personales y temas relacionados, publicado por la Subdirección de Recursos Humanos, como enlace de capacitación de AICM en materia de transparencia ante el Órgano Administrativo Desconcentrado Transparencia para el Pueblo.

VI. DEBERES.

1. Las Unidades Responsables deben establecer y mantener las medidas de seguridad de carácter administrativo, físico y técnico que garanticen la confidencialidad, integridad y disponibilidad de los datos personales, así como la protección contra:
    - Daño, pérdida, alteración, o destrucción.
    - Uso, acceso o tratamiento no autorizado.
2. Las medidas de seguridad deben estar documentadas y contenidas en un sistema de gestión.
3. Las Unidades Responsables deben establecer, mantener y supervisar las medidas de seguridad contenidas en el Documento de Seguridad, elaborado por la Subdirección de Sistemas.
4. Las Unidades Responsables deben observar como medidas mínimas de seguridad las siguientes:
    a. Registrar a las personas que realicen el tratamiento de datos personales.
    b. Implementar las medidas necesarias para que las personas que recaben datos personales estén plenamente identificadas ante los titulares.
    c. Garantizar la restricción de acceso a terceros no autorizados, a los lugares donde se resguarden datos personales.

d. Asignar contraseñas seguras a las personas con acceso a datos personales contenidos en medios electrónicos y establecer mecanismos para registrar el alta, modificación y baja de dichas contraseñas.
e. Resguardar bajo llave los datos personales contenidos en medios físicos, en espacios que garanticen su adecuada conservación.
f. Instruir al personal que los papeles de oficina que contengan datos personales, no pueden ser utilizados como papel de doble uso.
g. Advertir a las personas que tengan acceso a datos personales, que está estrictamente prohibido reproducirlos o difundirlos mediante ningún medio físico o electrónico, a menos que sea necesario para el ejercicio de sus funciones.
h. En caso de que sea necesario remitir datos personales a otras áreas, comunicar por escrito que la información corresponde a datos personales y especificar las finalidades para las cuales se hace la entrega, así como la obligación que se tiene de guardar confidencialidad de los mismos.

5. Los datos personales en poder de AICM podrán ser utilizados para efectos estadísticos, garantizando la disociación de estos datos para que no sea factible identificar a las personas involucradas en los informes que se generen.
6. Las personas que participen en el tratamiento de datos personales, deben cumplir con la capacitación en materia de protección de datos personales que al efecto apruebe el Comité de Transparencia.
7. Los titulares de las áreas que traten datos personales deberán informar al Comité de Transparencia las vulneraciones de seguridad que se llegaran a presentar, así como las acciones llevadas a cabo en consecuencia, a fin de que éste informe a los titulares afectados para que puedan tomar las medidas correspondientes para la defensa de sus derechos.

VII. CICLO DE VIDA DE LOS DATOS PERSONALES.

Las Unidades Responsables deben establecer mecanismos para:

1. Identificar el flujo y ciclo de vida de los datos personales, específicamente:

- Momento y medio por el cual se recaban
- Procesos que se utilizan
- Unidades Administrativas o personas con las que se comparten
- Momento en el que se suprimen.
- Medio por el que se suprimen,

2. Elaborar y mantener actualizado el inventario de datos personales conforme a lo establecido en el Documento de Seguridad.
3. Bloquear, cancelar, suprimir o destruir los datos personales, en los casos establecidos en la normatividad aplicable.

VIII. ROLES Y RESPONSABILIDADES.

1. Las Unidades Responsable deben
   a. Determinar las funciones y responsabilidades de las personas que lleven a cabo el tratamiento de los datos personales.
   b. Establecer una cadena de rendición de cuentas de todas las personas que participen en el tratamiento de datos personales.

IX. SANCIONES.

1. Serán causas de sanción por incumplimiento de las obligaciones en materia de protección de datos personales, las establecidas en el artículo 132 de la LGPDPPSO.
2. El Comité de Transparencia deberá dar vista al Órgano Interno de Control, a través del Titular de la Unidad de Transparencia, de los casos en que tenga conocimiento, en el ejercicio de sus atribuciones, de una presunta irregularidad respecto al tratamiento de datos personales, particularmente en casos relacionados con la declaración de inexistencia que manifiesten las Unidades Administrativas ante alguna solicitud para el ejercicio de derechos ARCO.

X. PROCESO GENERAL PARA EL ESTABLECIMIENTO, ACTUALIZACIÓN, MONITOREO Y REVISIÓN DE LOS MECANISMOS Y MEDIDAS DE SEGURIDAD.

Conforme a lo establecido en la fracción VI del artículo 35 de la Ley General, los mecanismos de monitoreo y revisión forman parte del Documento de Seguridad.

1. La Subdirección de Sistemas debe elaborar, difundir y actualizar el Documento de Seguridad.
2. La Subdirección de Sistemas llevará a cabo el monitoreo y revisión, de manera periódica, de las medidas de seguridad implementadas, así como de las amenazas y vulneraciones a las que están sujetos los datos personales, principalmente:
    a. Monitoreo del entorno físico: condiciones del lugar donde se resguarda el archivo físico, seguridad, control de accesos.
    b. Monitoreo del entorno electrónico: vulnerabilidad de los sistemas ante ataques cibernéticos, existencia y funcionalidad de medidas de seguridad y acceso.
3. La Subdirección de Sistemas en coordinación con los Unidades Responsables podrán actualizar el plan de trabajo del Documento de Seguridad, con base en los resultados del monitoreo.
4. El Titular de la Unidad de Transparencia de AICM y los titulares de las Unidades Responsables, podrán someterse a auditorías voluntarias por parte de la Secretaría Anticorrupción y Buen Gobierno o Autoridades Garantes en términos del artículo 120 de la LGPDPPSO, las cuales tiene por objeto verificar la adaptación, adecuación y eficacia de los controles, medidas y mecanismos implementados para el cumplimiento de las disposiciones previstas en la Ley General. y demás disposiciones jurídicas aplicables.

XI. PROCESO GENERAL DE ATENCIÓN DE LOS DERECHOS ARCO

Los derechos de ACCESO, RECTIFICACIÓN, CANCELACIÓN u OPOSICIÓN de datos personales, conocidos como derechos ARCO, solo pueden ser ejercidos por la persona titular o un representante previa acreditación de ambos.

La atención de las personas titulares que deseen ejercer alguno de los derechos ARCO se llevará a cabo conforme a:

1. Las solicitudes de ACCESO a datos personales se recibirán a través de la Plataforma Nacional de Transparencia y serán atendidas por la Unidad de Transparencia con base en los tiempos y procedimientos establecidos para ello. Las Unidades Administrativas que reciban solicitudes de ACCESO a datos personales deberán orientar a la persona para que lo haga a través de la Plataforma o en las instalaciones de la Unidad.
2. Las solicitudes de RECTIFICACIÓN, CANCELACIÓN y OPOSICIÓN deberán presentarse ante la Unidad Responsable, con base en lo establecido en su Aviso de Privacidad.
3. Las Unidades Responsables informarán semestralmente al Comité de Transparencia el número de solicitudes de RECTIFICACIÓN, CANCELACIÓN y OPOSICIÓN recibidas, a fin de que AICM estén en posibilidad de cumplir con el artículo 118 de los Lineamientos.