

POLÍTICA INTERNA DE GESTIÓN Y TRATAMIENTO DE LOS DATOS PERSONALES

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

INDICE

I. MARCO JURÍDICO.....	4
II. DEFINICIONES.....	5
III. OBJETIVO Y ALCANCE.....	7
IV. DISPOSICIONES GENERALES.....	8
V. PRINCIPIOS.....	9
VI. DEBERES.....	14
VII. CICLO DE VIDA DE LOS DATOS PERSONALES.....	16
VIII. ROLES Y RESPONSABILIDADES.....	17
IX. SANCIONES.....	17
X. PROCESO GENERAL PARA EL ESTABLECIMIENTO, ACTUALIZACIÓN, MONITOREO Y REVISIÓN DE LOS MECANISMOS Y MEDIDAS DE SEGURIDAD.....	19
XI. PROCESO GENERAL DE ATENCIÓN DE LOS DERECHOS ARCO.....	20

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) y Servicios Aeroportuarios de la Ciudad de México, S.A. de C.V. (SACM) al ser empresas de participación estatal mayoritaria, en términos del artículo 3 de la Ley Orgánica de la Administración Pública Federal, encargadas de la operación y administración del “*Aeropuerto Internacional Benito Juárez Ciudad de México*” tienen la obligación de proteger los datos personales que obran en sus archivos y sobre los cuales efectúa algún tratamiento y son responsables 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 para ambas Entidades, en cumplimiento a lo dispuesto por el artículo 33, 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.
- Ley Federal 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.
- Ley General de Responsabilidades Administrativas
- Manual General de Organización de AICM y SACM

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.

Encargado: La persona física o jurídica, pública o privada, ajena a la organización de SACM o AICM que, sola o conjuntamente con otras trate datos personales a nombre y por cuenta de cualquiera de las dos Entidades.

Instituto: Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, organismo garante de la Federación en materia de protección de datos personales en posesión de los sujetos obligados.

LGPDPPO o la Ley General: 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, Gerencias y Subgerencias que integran a las Entidades AICM y SACM.

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

OICE: Órgano Interno de Control Específico en el Aeropuerto Internacional de la Ciudad de México, S.A. de C.V. y Servicios Aeroportuarios de la Ciudad de México, S.A. de C.V.

MGO: Manual General de Organización de Aeropuerto Internacional de la Ciudad de México, S.A. de C.V. y Servicios Aeroportuarios de la Ciudad de México, S.A. de C.V.

Documento de Seguridad: Instrumento que describe y da cuenta de manera general sobre las medidas de seguridad técnicas, físicas y administrativas adoptadas por el responsable para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que posee.

III. OBJETIVO Y ALCANCE.

Establecer los principios y deberes que deben observar y cumplir las personas servidoras públicas de Aeropuerto Internacional de la Ciudad de México, S.A. de C.V. (AICM) y Servicios Aeroportuarios de la Ciudad de México, S.A. de C.V. (SACM), para el tratamiento y protección de los datos personales, conforme a lo previsto en la LGPDPSO y los Lineamientos de Protección de Datos Personales para el Sector Público.

Así como, de establecer las medidas necesarias que garanticen la seguridad de los datos personales que en el ámbito de su competencia posean, recaben o transmitan, a fin de evitar su alteración, daño, destrucción o su uso, acceso o tratamiento no autorizado, pérdida y transmisión, debiendo asegurar su propósito para los cuales se hayan obtenido.

La Política es de aplicación y observancia general y obligatoria para todas las personas servidoras públicas adscritas a las Entidades AICM y SACM.

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 y SACM de acuerdo con el MGO (Unidades Responsables) y con el consentimiento de la persona titular.
2. Es obligación de todas las personas servidoras públicas de AICM y SACM que administren, actualicen o tengan acceso a bases de datos personales, el conservar, manejar y mantener de manera estrictamente confidencial dicha información y no revelarla a terceros.
3. Las Unidades Responsables deben asegurar que los Encargados que tratan datos personales en nombre de SACM o AICM den cumplimiento a 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 SACM y 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 y SACM y, de manera impresa, en donde se traten datos personales, se deberán poner 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 para 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 16 de la Ley General y el artículo 7 de los Lineamientos Generales, se establece que en todo tratamiento de datos personales se deberán observar los principios rectores siguientes:

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

Para cumplir con este principio las Unidades Responsables deben seguir las siguientes recomendaciones:

- a. Revisar que los datos personales se traten conforme a la LGPDPPSO, 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, se le deberá informar 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 de los avisos 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 y SACM en materia de transparencia ante el INAI.

VI. DEBERES.

1. Las Unidades Administrativas 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 el Documento de Seguridad.
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 SACM y 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 Responsables 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 163 de la Ley General, las que se describen a continuación:
 - I. Actuar con negligencia, dolo o mala fe durante la sustanciación de las solicitudes para el ejercicio de los derechos ARCO;
 - II. Incumplir los plazos de atención previstos en la presente Ley para responder las solicitudes para el ejercicio de los derechos ARCO o para hacer efectivo el derecho de que se trate;
 - III. Usar, sustraer, divulgar, ocultar, alterar, mutilar, destruir o inutilizar, total o parcialmente y de manera indebida datos personales, que se encuentren bajo su custodia o a los cuales tengan acceso o conocimiento con motivo de su empleo, cargo o comisión;
 - IV. Dar tratamiento, de manera intencional, a los datos personales en contravención a los principios y deberes establecidos en la presente Ley;
 - V. No contar con el aviso de privacidad, o bien, omitir en el mismo alguno de los elementos a que refiere el artículo 27 de la presente Ley, según sea el caso, y demás disposiciones que resulten aplicables en la materia;
 - VI. Clasificar como confidencial, con dolo o negligencia, datos personales sin que se cumplan las características señaladas en las leyes que resulten aplicables. La

sanción sólo procederá cuando exista una resolución previa, que haya quedado firme, respecto del criterio de clasificación de los datos personales;

VII. Incumplir el deber de confidencialidad establecido en el artículo 42 de la presente Ley;

VIII. No establecer las medidas de seguridad en los términos que establecen los artículos 31, 32 y 33 de la presente Ley;

IX. Presentar vulneraciones a los datos personales por la falta de implementación de medidas de seguridad según los artículos 31, 32 y 33 de la presente Ley;

X. Llevar a cabo la transferencia de datos personales, en contravención a lo previsto en la presente Ley;

XI. Obstruir los actos de verificación de la autoridad;

XII. Crear bases de datos personales en contravención a lo dispuesto por el artículo 5 de la presente Ley;

XIII. No acatar las resoluciones emitidas por el Instituto y los Organismos garantes, y

XIV. Omitir la entrega del informe anual y demás informes a que se refiere el artículo 44, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública, o bien, entregar el mismo de manera extemporánea.

2. El Comité de Transparencia deberá dar vista al Órgano Interno de Control Específico, 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.

Los incumplimientos de la Ley General pueden derivar, además de faltas administrativas, en delitos y responsabilidades civiles, dichas responsabilidades se determinarán, en forma autónoma, a través de los procedimientos previstos en las leyes aplicables y las sanciones que, en su caso, se impongan por las autoridades competentes, también se ejecutarán de manera independiente.

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 de AICM y SACM deberá elaborar, difundir y actualizar el Documento de Seguridad.
2. Las Unidades Responsables y la Subdirección de Sistemas dentro del ámbito de competencia de cada una deberán llevar 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 de AICM y SACM 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 SACM y AICM y los titulares de las Unidades Responsables, podrán solicitar al INAI, auditorías voluntarias en términos del artículo 218 de los Lineamientos, 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 los Lineamientos.

XI. PROCESO GENERAL DE ATENCIÓN DE LOS DERECHOS ARCO

Toda persona, como titular de sus datos personales o a través de su representante, tiene derecho a **A**cceder a ellos, a **R**ectificarlos, a solicitar su **C**ancelación u **O**ponerse a su tratamiento.

Los derechos ARCO son derechos independientes, por lo que el ejercicio de cualquiera de ellos no es requisito previo ni impide el ejercicio del otro, por ello, según el derecho que se pretenda ejercer, el titular de los datos personales presentará la solicitud que desee, para lo cual deberá observar lo siguiente:

- **Acceso:** Este derecho consiste en acceder a los datos personales en posesión de AICM y SACM, así como conocer la información relacionada con las condiciones y generalidades de su tratamiento.
- **Rectificación:** Este derecho consiste en corregir los datos personales que AICM y SACM tenga en sus bases, registros o publicaciones, en caso de que sean incorrectos, inexactos, imprecisos, incompletos o estén desactualizados.
- **Cancelación:** Este derecho consiste en solicitar la eliminación de los datos de las bases que tenga AICM y SACM, por tanto, se deberá dejar de usarlos, ya que se considera que no están siendo utilizados o tratados conforme a las obligaciones y atribuciones de estas Entidades. Los datos deberán ser bloqueados y posteriormente, suprimidos de las bases de datos. Esta solicitud procede cuando la información personal ya no es necesaria para las actividades relacionadas con AICM

y SACM, sin embargo, la eliminación no procede en el caso de que por disposición legal sea necesaria su conservación.

• **Oposición:** Este derecho consiste en la facultad que tiene el titular de los datos para solicitar a AICM y SACM que se abstenga del uso o tratamiento de sus datos personales, por no ser esta la razón específica para la cual fueron otorgados o recabados.

La atención de las personas titulares o sus representantes 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 oficinas que ocupa la Unidad de Transparencia.
2. Las solicitudes de RECTIFICACIÓN de los datos personales, 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 SACM y AICM estén en posibilidad de cumplir con el artículo 118 de los Lineamientos

En todos los casos, el plazo de respuesta para el ejercicio de los derechos es de 20 días hábiles, a partir de que se ingrese la solicitud, el cual podrá ser ampliado hasta por 10 días hábiles más. Para mayor información podrá consultar el siguiente link

<https://www.aicm.com.mx/wp-content/uploads/2018/07/ProcedimientoARCOAICM.pdf>



MARINA
SECRETARÍA DE MARINA



AEROPUERTO INTERNACIONAL
BENITO JUÁREZ
CIUDAD DE MÉXICO



Referencia bibliográfica

Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, publicada en el Diario Oficial de la Federación el 26 de enero de 2017.

Disponible en https://www.dof.gob.mx/nota_detalle.php?-codigo=5469949&fecha=26/01/2017)

Lineamientos Generales para la Protección de Datos Personales en el Sector Público, publicados en el Diario Oficial de la Federación el 26 de enero de 2018.

Disponible en: http://dof.gob.mx/nota_detalle.php?codigo=5511540&fecha=26/01/2018

Recomendaciones para la elaboración de las Políticas Internas de Gestión y Tratamientos de los Datos Personales Sector Público

Resolución CT-AICM/221223-01

Los miembros del Comité de Transparencia de Aeropuerto Internacional de la Ciudad de México, S.A. de C.V. (AICM), con fundamento en artículo 33, fracción I de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y al artículo 47 y 56 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público, resuelven lo siguiente:

PRIMERO.- Aprobar el documento POLÍTICA INTERNA DE GESTIÓN Y TRATAMIENTO DE LOS DATOS PERSONALES de AEROPUERTO INTERNACIONAL DE LA CIUDAD DE MÉXICO, S.A. DE C.V. y SERVICIOS AEROPORTUARIOS DE LA CIUDAD DE MÉXICO, S.A. DE C.V.

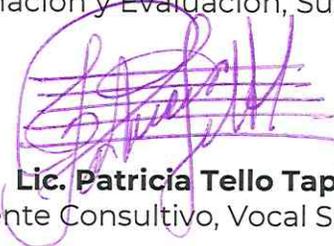
SEGUNDO.- Instruye a la Unidad de Transparencia, para la publicación del documento aprobado en el numeral anterior, en nuestro Sitio web (www.aicm.com.mx), en la sección Protección de Datos Personales, aplicable para ambas Entidades. Así como su difusión al interior de las mismas.

Así lo resolvieron, por unanimidad, los CC. Lic. Patricia Cravioto Galindo, Gerente de Información y Evaluación, Suplente del Presidente; Lic. Patricia Tello Tapia, Gerente Consultivo, Vocal Suplente; y Lic. Agustín Burgoa Maldonado, Titular del Área de Responsabilidades, Vocal Suplente (voto emitido mediante Oficio No. 09/448/TR-289/2023); en la Trigésima Sexta Sesión celebrada en la Ciudad de México, el 22 de diciembre de 2023.



Lic. Patricia Cravioto Galindo

Gerente de Información y Evaluación, Suplente del Presidente



Lic. Patricia Tello Tapia

Gerente Consultivo, Vocal Suplente



**ÓRGANO INTERNO DE CONTROL ESPECÍFICO EN
AEROPUERTO INTERNACIONAL DE LA CIUDAD DE
MÉXICO, S.A. DE C.V. Y SERVICIOS AEROPORTUARIOS
DE LA CIUDAD DE MÉXICO, S.A. DE C.V.
ÁREA DE RESPONSABILIDADES**

Oficio No. 09/448/TR-289/2023
Ciudad de México, 15 de diciembre de 2023

**LIC. PATRICIA CRAVIOTO GALINDO
GERENTE DE INFORMACIÓN Y EVALUACIÓN
PRESENTE**

Me refiero al Proyecto del documento **“Política Interna de Gestión y Tratamiento de los Datos Personales” del Aeropuerto Internacional de la Ciudad de México S.A. de C.V. y Servicios Aeroportuarios de la Ciudad de México S.A. de C.V.**, enviado a este Órgano Interno de Control Específico (**OICE**) para su revisión y comentarios, como miembro del Comité de Transparencia de AICM y SACM.

Al respecto, y derivado de la revisión a las mismas, con fecha 26 de septiembre de 2023, se enviaron las observaciones y recomendaciones correspondientes, mismas que fueron atendidas por el área a su cargo.

Por lo anterior, y toda vez que con fecha 24 de noviembre de 2023, se publicó en el Diario Oficial de la Federación el **“ACUERDO por el que se señalan y determinan como inhábiles los días del segundo periodo de vacaciones de 2023 de la Secretaría de la Función Pública”** (18 de diciembre de 2023 a 02 de enero de 2024), me permito informar que con esta fecha, por parte de este **OICE** no se tienen comentarios adicionales al documento propuesto, por lo que se informa el **voto a favor** para su aprobación en el Comité de Transparencia que se celebre para tal fin.

Sin otro particular, aprovecho la oportunidad para enviarle un cordial saludo.

**ATENTAMENTE
EL TITULAR DEL ÁREA DE RESPONSABILIDADES**

LIC. AGUSTÍN BURGOA MALDONADO



C.c.p. **Lic. José Antonio Montero Villa**. Titular del Órgano Interno de Control en AICM y SACM.

