Instituto Nacional de
Transparencia,
Acceso a la Información y
Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES
SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES
DIRECCIÓN GENERAL DE NORMATIVIDAD Y CONSULTA

Expediente: INAI/SPDP/DGNC/EIPDP/001/2023.

Oficio núm.: INAI/SPDP/DGNC/065/2023.

Asunto: Notificación de dictamen de evaluación de impacto en la protección de datos personales y recomendaciones no vinculantes.

Ciudad de México, a 01 de marzo de 2023.

Rogelio Gerardo Tejada Guerrero
Subdirector de Sistemas del Aeropuerto Internacional
Felipe Ángeles, S.A. de C.V.
Domicilio: Kilómetro 33 Santa Lucía, Circuito Exterior Mexiquense,
Zumpango, Código Postal 55600, Estado de México.
P r e s e n t e

Por instrucciones del Dr. Jonathan Mendoza Iserte, Secretario de Protección de Datos Personales del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, de conformidad con lo establecido en los artículos 77 y 78 de la Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados; 25, fracción XIII, 29, fracciones XXX y XL, 42, fracciones IV y XIII del Estatuto Orgánico del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales y 28 fracción II de las Disposiciones administrativas de carácter general para la elaboración, presentación y valoración de evaluaciones de impacto en la protección de datos personales; de manera adjunta encontrará el Dictamen de la evaluación de impacto en la protección de datos personales con motivo de la implementación del ***"Sistema de Procesamiento de Pasajeros del AIFA"***; recaído en el expediente registrado con el número INAI/SPDP/DGNC/EIPDP/001/2023.

Atentamente

Luis Ricardo Sánchez Hernández
Director General de Normatividad y Consulta

C.c.p. Dr. Jonathan Mendoza Iserte, Secretario de Protección de Datos Personales. Para su conocimiento.

LRSH/LIPDR/PHM-ELE

Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE NORMATIVIDAD Y CONSULTA

Expediente: INAI/SPDP/DGNC/EIPDP/001/2023.

En la Ciudad de México, a los veintiocho días del mes de febrero del año dos mil veintitrés; con fundamento en los artículos 74, 77 y 78 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados; 23, 27, 29 y 30 de las Disposiciones administrativas de carácter general para la elaboración, presentación y valoración de evaluaciones de impacto en la protección de datos personales y 42, fracciones IV y XIII del Estatuto Orgánico del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, se emite el presente:

DICTAMEN

I. Glosario.

Para efectos del presente dictamen se entenderá por:

- **Acuerdo del pasaporte electrónico:** Acuerdo por el que se establece el contenido de los pasaportes electrónicos mexicanos.[1]
- **ACUS:** Sistema Aeroportuario de Uso Común de Amadeus (*Airport Cloud Use Services*). Componente tecnológico de la solución de Procesamiento de Pasajeros que permite la integración entre Sistema de Autoservicio de Uso Común; Sistema de Uso Común para el Procesamiento de Pasajeros de documentación y abordaje; E-gates y los sistemas de las aerolíneas.
- **AIDX:** *Aviation Information Data Exchange* (Estándar para el Intercambio de Datos de Información de Aviación).
- **AIFA:** Aeropuerto Internacional Felipe Ángeles. S.A. de C.V.
- **Anexo 9:** Anexo 9 denominado "Facilitación".
- **Anexo 17:** Anexo 17 al Convenio sobre Aviación Civil Internacional Seguridad. Protección de la aviación civil internacional contra los actos de interferencia ilícita.
- **APP:** Aplicación Móvil del AIFA en donde el usuario se toma una fotografía con su teléfono celular para identificar al pasajero y validarlo.
- **APV:** *Amadeus Passenger Verification* (Sistema de Verificación de Pasajeros de Amadeus). El APV es un componente tecnológico de la solución de Procesamiento de Pasajeros que permite la integración entre las *E-Gate* de Pre-Seguridad y abordaje con sistemas de las aerolíneas. Con el objetivo de validar la elegibilidad del pasajero para ingresar al área estéril del Aeropuerto Internacional Felipe Ángeles.
- **BCBP o Pase de abordar:** *Bar Code Boarding Pass* (Pase de Abordar).

[1] Publicado en el Diario Oficial de la Federación el 23 de septiembre de 2021, sin cambios desde su publicación. Disponible para su consulta en https://www.dof.gob.mx/nota_detalle.php?codigo=5630645&fecha=23/09/2021, consultado por última vez el 28/02/2023.

- **CG91:** Acuerdo número INE/CG91/2020, relativo al Acuerdo del Consejo General del Instituto Nacional Electoral por el que se aprueban las adecuaciones para ampliar y fortalecer el servicio de verificación de datos de la credencial para votar emitido por el Instituto Nacional Electoral[2].
- **CG92:** Acuerdo número INE/CG92/2016, relativo al Acuerdo del Consejo General del Instituto Nacional Electoral, por el que se aprueba la implementación del servicio de verificación de los datos de la credencial para votar, que servirá para garantizar el derecho de protección de datos de los ciudadanos, contenidos en el padrón electoral[3].
- **Concesión del AIFA:** Título de Concesión que otorga la Secretaría de Comunicaciones y Transportes, a favor de la Empresa de Participación Estatal Mayoritaria Aeropuerto Internacional Felipe Ángeles, S.A. de C.V.[4]
- **Convenio de Chicago:** Convenio sobre Aviación Civil Internacional[5].
- **Constitución:** Constitución Política de los Estados Unidos Mexicanos[6].
- **Convenio 108**: Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal y su Protocolo Adicional relativo a las Autoridades de Control y a los Flujos Transfronterizos de Datos[7], hechos en Estrasburgo, Francia, el 28 de enero de 1981, y el 8 de noviembre de 2001.
- **Convenio 108+:** Protocolo por el que se modifica el Convenio para la protección de las personas con respecto al Tratamiento Automatizado de Datos Personales.[8]
- **CUPPS:** *Common Use Passenger Procesing System* (Sistema de Uso Común para el Procesamiento de Pasajeros). Es una solución de tecnologías de la información que permite

---

[2] Disponible para su consulta en el siguiente vínculo electrónico: https://repositoriodocumental.ine.mx/xmlui/bitstream/handle/123456789/113983/CGex202005-15-ap-2-Gaceta.pdf, enlace consultado por última vez el 28/02/2023.

[3] Disponible para su consulta en el siguiente vínculo electrónico: https://repositoriodocumental.ine.mx/xmlui/bitstream/handle/123456789/87473/CGor201602-26_ap_13.pdf?sequence=1&isAllowed=y, enlace consultado por última vez el 28/02/2023.

[4] Publicado en el Diario Oficial de la Federación el 15 de octubre de 2021, disponible para su consulta en: https://dof.gob.mx/nota_detalle.php?codigo=5632851&fecha=15/10/2021, sin reformas, consultado por última vez el 28/02/2023.

[5] Disponible para su consulta en el siguiente vínculo electrónico: https://www.gob.mx/cms/uploads/attachment/file/599624/convenio-de-chicago.pdf, consultado por última vez el 28/02/2023

[6] Publicada en el Diario Oficial de la Federación (en adelante, DOF), Órgano del Gobierno Provisional de la República Mexicana, el 05 de febrero de 1917, disponible en el vínculo: https://www.dof.gob.mx/index_113.php?year=1917&month=02&day=05, cuyo texto puede obtenerse del vínculo siguiente: http://www.diputados.gob.mx/LeyesBiblio/ref/cpeum/CPEUM_orig_05feb1917.pdf, basado en el contenido de la información que se desprende de la imagen original disponible en el enlace: http://www.diputados.gob.mx/LeyesBiblio/ref/cpeum/CPEUM_orig_05feb1917_ima.pdf; última reforma publicada en el Diario Oficial de la Federación el 18 de noviembre de 2022, disponible en el siguiente vínculo electrónico: https://www.dof.gob.mx/nota_detalle.php?codigo=5671829&fecha=18/11/2022#gsc.tab=0; texto consolidado por la Cámara de Diputados del H. Congreso de la Unión en formato de documento portable, denominado como pdf por sus siglas en inglés, incorporando las diversas reformas de dicho ordenamiento jurídico en el sitio siguiente: https://www.diputados.gob.mx/LeyesBiblio/pdf/CPEUM.pdf; enlaces consultados por última ocasión el 28/02/2023.

[7] Disponible para su consulta en el siguiente vínculo electrónico: http://www.oas.org/es/sla/ddi/docs/u12%20convenio%20n%20108.pdf, consultado por última vez el 28/02/2023.

[8] Disponible para su consulta en el siguiente vínculo electrónico: https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1; consultado por última vez el 28/02/2023.

que múltiples aerolíneas, utilicen una infraestructura común uniforme, asignada de manera dinámica por el AIFA, para compartir el *check-in* físico o las posiciones de las puertas de embarque (ya sea de manera simultánea o consecutiva).

- **CUSS:** *Common Use Service System* (Sistema de Autoservicio de Uso Común). Se trata de una plataforma de autoservicio, (Quiosco de autoservicio) que permite a los pasajeros que deseen, llevar a cabo su proceso de *check-in* o enrolamiento biométrico de manera independiente a la atención personalizada que ofrecen las aerolíneas, apoyando las soluciones sin contacto.
- **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, conforme a lo dispuesto en el artículo 3, fracción IX de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.
- **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 conllevar un grave riesgo para éste. De manera enunciativa más no limitativa, se considerán sensibles aquéllos que puedan revelar aspectos como origen étnico o racial, estado de salud presente o futuro, información genética, creencias religiosas, filosóficas y morales, opiniones políticas y preferencia sexual de conformidad con el artículo 3, fracción X de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.
- **Derechos ARCO:** Los derechos de acceso, rectificación, cancelación y oposición al tratamiento de datos personales, de conformidad con el artículo 3, fracción XI de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.
- **Derecho de Portabilidad:** Derecho contemplado por el artículo 57 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, relativo a que cuando se traten datos personales por vía electrónica en un formato estructurado y comúnmente utilizado, el titular tendrá derecho a obtener del responsable una copia de los datos objeto de tratamiento en un formato electrónico estructurado y comúnmente utilizado que le permita seguir utilizándolos. Cuando el titular haya facilitado los datos personales y el tratamiento se base en el consentimiento o en un contrato, tendrá derecho a transmitir dichos datos personales y cualquier otra información que haya facilitado y que se conserve en un sistema de tratamiento automatizado a otro sistema en un formato electrónico comúnmente utilizado, sin impedimentos por parte del responsable del tratamiento de quien se retiren los datos personales. Sobre el particular, el Sistema Nacional de Transparencia, Acceso a la Información Pública y Protección de datos personales, ha establecido mediante lineamientos los parámetros a considerar para determinar los supuestos en los que se está en presencia de un formato estructurado y comúnmente utilizado, así como las normas técnicas, modalidades y procedimientos para la transferencia de datos personales, a través del

documento denominando: *"Lineamientos que establecen los Parámetros, Modalidades y Procedimientos para la Portabilidad de Datos Personales"*[9].

- **DGNC o Dirección General:** Dirección General de Normatividad y Consulta del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.
- **Disposiciones administrativas:** Disposiciones administrativas de carácter general para la elaboración, presentación y valoración de evaluaciones de impacto en la protección de datos personales[10].
- **Documento 9303:** Documentos de viaje de lectura mecánica[11].
- **E-GATES:** Puertas Electrónicas automáticas (proceso biométrico y no biométrico). Las puertas electrónicas (*E-gates*) están instaladas en el área previa a los puntos de inspección de seguridad (pre-seguridad) y previa al abordaje.
- **Encargado:** La persona física o jurídica, de carácter público o privado, ajena a la organización del responsable, que sola o juntamente con otras, trata datos personales a nombre y por cuenta del responsable; de conformidad con el artículo 3, fracción XV de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.
- **Estatuto Orgánico:** Estatuto Orgánico del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales[12].
- **Evaluación de impacto:** Evaluación de impacto en la protección de datos personales consistente en el 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

---

[9] Publicados en el Diario Oficial de la Federación el 12 de febrero de 2018, disponibles en el vínculo siguiente: http://dof.gob.mx/nota_detalle.php?codigo=5512847&fecha=12/02/2018, consultados por última ocasión el 28/02/2023.

[10] Publicados el 23 enero de 2018, disponible para su consulta en el siguiente vínculo electrónico: https://dof.gob.mx/nota_detalle.php?codigo=5511113&fecha=23/01/2018, sin reformas; consultadas por última vez el 28/02/2023.

[11] Disponible para su consulta en https://www.icao.int/publications/Documents/9303_p1_cons_es.pdf, consultado por última vez el 28/02/2023.

[12] El Estatuto Orgánico del Instituto Nacional del Transparencia, Acceso a la Información y Protección de Datos Personales, fue aprobado el 1 de noviembre de 2016 y publicado en el Diario Oficial de la Federación el 17 de enero de 2017, el mismo se encuentra disponible en el vínculo electrónico siguiente:http://diariooficial.gob.mx/nota_detalle.php?codigo=5469197&fecha=17/01/2017; posteriormente fue modificado el 5 de julio de 2017 y publicado en el Diario Oficial de la Federación el 11 de agosto de 2017, el cual se encuentra disponible en el vínculo electrónico siguiente: http://diariooficial.gob.mx/nota_detalle.php?codigo=5493659&fecha=11/08/2017; siendo modificado el 6 de diciembre de 2017 y publicado en el Diario Oficial de la Federación el 13 de febrero de 2018, mismo que se encuentra disponible en el vínculo electrónico siguiente: http://diariooficial.gob.mx/nota_detalle.php?codigo=5512945&fecha=13/02/2018, posteriormente fue modificado el 11 de septiembre de 2019 y publicado en el Diario Oficial de la Federación el 24 de septiembre de 2019, el cual se encuentra disponible en el vínculo electrónico http://diariooficial.gob.mx/nota_detalle.php?codigo=5573281&fecha=24/09/2019, posteriormente fue modificado el 15 de septiembre de 2020 y publicado en el Diario Oficial de la Federación el 23 de septiembre de 2020, el cual se encuentra disponible en el vínculo electrónico https://dof.gob.mx/nota_detalle.php?codigo=5601082&fecha=23/09/2020, por último, fue modificado el 10 de marzo del 2021 y publicado en el Diario Oficial de la Federación el 18 de marzo del 2021, disponible en el vínculo electrónico https://www.dof.gob.mx/nota_detalle.php?codigo=5613883&fecha=18/03/2021 enlaces consultados por última vez el 28/02/2023.

responsables y encargados, previstos en la normativa aplicable de conformidad con lo dispuesto en el artículo 3, fracción XVI de la Ley General.

- **Evaluación de impacto del Sistema de Procesamiento:** Documento remitido por el AIFA denominado Evaluación de Impacto en la Protección de Datos Personales Sistema de Procesamiento de Pasajeros del Aeropuerto Internacional "Felipe Ángeles" (AIFA).
- **INE:** Instituto Nacional Electoral.
- **INAI o Instituto:** Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.
- **LFPDPPP**: Ley Federal de Protección de Datos Personales en Posesión de los Particulares[13].
- **LGA**: Ley General de Archivos.[14]
- **Ley General:** Ley General de Protección de Datos Personales en Posesión de Sujetos Obligado[15].
- **Lineamientos generales:** Lineamientos Generales de Protección de Datos Personales para el Sector Público[16].
- **OACI:** Organización de Aviación Civil Internacional.
- **PDE:** Envoltura de Datos Personales (Personal Data Envelope).
- **Remisión:** Toda comunicación de datos personales realizada exclusivamente entre el responsable y encargado, dentro o fuera del territorio mexicano de conformidad con lo dispuesto en el artículo 3, fracción XXVII de la Ley General.
- **Responsable:** Cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, fideicomisos y fondos públicos y partidos políticos, del orden federal, que decide sobre determinado tratamiento de datos personales de conformidad con lo dispuesto en los artículos 1 y 3, fracción XXVIII de la Ley General.
- **Resolución del AIFA:** Resolución por la que se autoriza la constitución de una Empresa de Participación Estatal Mayoritaria denominada Aeropuerto Internacional Felipe Ángeles, S.A.

---

[13] Publicada en el Diario Oficial de la Federación el 5 de julio de 2010 disponible en el siguiente vínculo electrónico: http://dof.gob.mx/nota_detalle.php?codigo=5150631&fecha=05/07/2010, sin reformas; texto consolidado en formato de documento portable, pdf por sus siglas en inglés, por parte de la Cámara de Diputados del H. Congreso de la Unión, en el siguiente vínculo electrónico: http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf, enlaces consultados por última vez el 28/02/2023.

[14] Publicada en el Diario Oficial de la Federación, el 15 de junio de 2018, disponible en el vínculo electrónico siguiente: https://www.dof.gob.mx/nota_detalle.php?codigo=5526593&fecha=15/06/2018; texto consolidado en formato de documento portable, pdf por sus siglas en inglés, por parte de la Cámara de Diputados del H. Congreso de la Unión, disponible en el vínculo electrónico: https://www.diputados.gob.mx/LeyesBiblio/pdf/LGA.pdf, enlaces consultados por última vez el 28/03/2023.

[15] Publicada en el Diario Oficial de la Federación, el 26 de enero de 2017, disponible en el vínculo electrónico siguiente: http://www.dof.gob.mx/nota_detalle.php?codigo=5469949&fecha=26/01/2017; sin reformas; texto consolidado en formato de documento portable, pdf por sus siglas en inglés, por parte de la Cámara de Diputados del H. Congreso de la Unión, disponible en el vínculo electrónico: http://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPPSO.pdf, enlaces consultados por última vez el 28/02/2023.

[16] Publicados en el Diario Oficial de la Federación el 26 de enero de 2018 disponible en los siguientes vínculos electrónicos: https://www.dof.gob.mx/nota_detalle.php?codigo=5511540&fecha=26/01/2018 y http://inicio.inai.org.mx/AcuerdosDelPleno/ACT-PUB-19-12-2017.10.pdf, última reforma publicada en el Diario Oficial de la Federación el 25 de noviembre de 2020 disponible en los siguientes vínculos electrónicos: https://www.dof.gob.mx/nota_detalle.php?codigo=5605789&fecha=25/11/2020, www.dof.gob.mx/2020/INAI/ACT-PUB-11-11-2020-05.pdf, https://home.inai.org.mx/wp-content/documentos/AcuerdosDelPleno/ACT-PUB-11-11-2020.05.pdf, enlaces consultados por última vez el 28/02/2023.

Se elimina hoja completa, con fundamento en el artículo 110, fracción I de la LFTAIP;Décimo séptimo de los lineamientos Generales en materia de clasificación y desclasificación de la información,así como para la elaboración de versiones públicas, en relación con el artículo 5, fracción VI de la Ley de Seguridad Nacional; 47, Bis 4 de la Ley de Aviación Civil, 46 y 47 de la Ley de Aeropuertos y 152 del Reglamento de Aeropuertos.

Se elimina hoja completa, con fundamento en el artículo 110, fracción I de la LFTAIP;Décimo séptimo de los lineamientos Generales en materia de clasificación y desclasificación de la información,así como para la elaboración de versiones públicas, en relación con el artículo 5, fracción VI de la Ley de Seguridad Nacional; 47, Bis 4 de la Ley de Aviación Civil, 46 y 47 de la Ley de Aeropuertos y 152 del Reglamento de Aeropuertos.

Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales

#	***Requerimiento de INAI-DGNC:***	***Desahogo de requerimiento:***
	administrativas, se considera que el responsable puede estar en presencia de un tratamiento intensivo o relevante de datos personales de carácter general o de manera particular. En ese sentido, se solicita la explicación de por qué se considera que, derivado de la implementación o puesta en operación del ***"Sistema de procesamiento de pasajeros"****, se está en presencia de uno o ambos supuestos mencionados, expresando los motivos que sustenten dicha consideración.*	*conformidad con lo dispuesto por, el Artículo 75. de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados,ya que se cumplen los tres supuestos de tratamiento intensivo de datos, ya que* *I. Existen riesgos inherentes a los datos personales a tratar;* *II. Se traten datos personales sensibles, y* *III. Se efectúen o pretendan efectuar transferencias de datos personales.* *Sobre el particular, el artículo 3, fracción X, de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados,refiere como datos personales los siguientes:* *"Datos personales sensibles: Aquellos que se refieran a la esfera más íntima de su titular, ocuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave paraéste. De manera enunciativa más no limitativa, se consideran sensibles los datos personalesque puedan revelar aspectos como origen racial o étnico, estado de salud presente o futuro,información genética, creencias religiosas, filosóficas y morales, opiniones políticas ypreferencia sexual"* *En este sentido, la utilización de biométricos, y datos como la fotografía enel pasaporteo en la credencial de elector y la nacionalidad, podrían en algunos casos, revelar aspectos como el origen racial y étnico, así como en algunos casos incluso las creencias religiosas.* *Por lo anterior, se considera que el "Sistema de Procesamiento de Pasajeros" realizara tratamiento de datos personales sensibles.*

#	***Requerimiento de INAI-DGNC:***	***Desahogo de requerimiento:***
		Asimismo, el artículo 9 de las Disposiciones Administrativas de Carácter General para la Elaboración, Presentación y Valoración de Evaluaciones de Impacto en la Protección de Datos Personales, cita en las fracciones III y VI, respectivamente: *"Tratar datos personales de grupos vulnerables, atendiendo, de manera enunciativa más no limitativa, a su edad, género, origen étnico o racial; estado de salud; preferencia sexual; nivel de instrucción y condición socioeconómica"* *En el caso que nos ocupa, también del pasaporte, de la credencial de elector, permiten acceso a la edad del pasajero.* *"Realizar un tratamiento frecuente y continúo de grandes volúmenes de datos personales, o bien, llevar a cabo cruces de información con múltiples sistemas o plataformas informáticas;"* *Tal como se desprende de los documentos originales que se entregaron en los anexos de la EIPDP, entregada el 9 de enero del año en curso, son millones de personas las cuales tendrían acceso a los biométricos en caso de estar de acuerdo con las condiciones del aviso de privacidad; aunado al hecho de que existen cruces de información dentro del aplicativo del Sistema de Procesamiento de Pasajeros, a cargo del encargado en diversos procesos, trae consigo que las dos condiciones señaladas en las fracciones III y VI del artículo 9 de las Disposiciones se llevan a cabo, para mayor detalle se expresa lo siguiente:*

Se elimina hoja completa, con fundamento en el artículo 110, fracción I de la LFTAIP;Décimo séptimo de los lineamientos Generales en materia de clasificación y desclasificación de la información,así como para la elaboración de versiones públicas, en relación con el artículo 5, fracción VI de la Ley de Seguridad Nacional; 47, Bis 4 de la Ley de Aviación Civil, 46 y 47 de la Ley de Aeropuertos y 152 del Reglamento de Aeropuertos.

Se elimina hoja completa, con fundamento en el artículo 110, fracción I de la LFTAIP;Décimo séptimo de los lineamientos Generales en materia de clasificación y desclasificación de la información,así como para la elaboración de versiones públicas, en relación con el artículo 5, fracción VI de la Ley de Seguridad Nacional; 47, Bis 4 de la Ley de Aviación Civil, 46 y 47 de la Ley de Aeropuertos y 152 del Reglamento de Aeropuertos.

Se elimina hoja completa, con fundamento en el artículo 110, fracción I de la LFTAIP;Décimo séptimo de los lineamientos Generales en materia de clasificación y desclasificación de la información,así como para la elaboración de versiones públicas, en relación con el artículo 5, fracción VI de la Ley de Seguridad Nacional; 47, Bis 4 de la Ley de Aviación Civil, 46 y 47 de la Ley de Aeropuertos y 152 del Reglamento de Aeropuertos.

Se elimina hoja completa, con fundamento en el artículo 110, fracción I de la LFTAIP;Décimo séptimo de los lineamientos Generales en materia de clasificación y desclasificación de la información,así como para la elaboración de versiones públicas, en relación con el artículo 5, fracción VI de la Ley de Seguridad Nacional; 47, Bis 4 de la Ley de Aviación Civil, 46 y 47 de la Ley de Aeropuertos y 152 del Reglamento de Aeropuertos.

Se elimina hoja completa, con fundamento en el artículo 110, fracción I de la LFTAIP;Décimo séptimo de los lineamientos Generales en materia de clasificación y desclasificación de la información,así como para la elaboración de versiones públicas, en relación con el artículo 5, fracción VI de la Ley de Seguridad Nacional; 47, Bis 4 de la Ley de Aviación Civil, 46 y 47 de la Ley de Aeropuertos y 152 del Reglamento de Aeropuertos.

Se elimina hoja completa, con fundamento en el artículo 110, fracción I de la LFTAIP;Décimo séptimo de los lineamientos Generales en materia de clasificación y desclasificación de la información,así como para la elaboración de versiones públicas, en relación con el artículo 5, fracción VI de la Ley de Seguridad Nacional; 47, Bis 4 de la Ley de Aviación Civil, 46 y 47 de la Ley de Aeropuertos y 152 del Reglamento de Aeropuertos.

Se elimina hoja completa, con fundamento en el artículo 110, fracción I de la LFTAIP;Décimo séptimo de los lineamientos Generales en materia de clasificación y desclasificación de la información,así como para la elaboración de versiones públicas, en relación con el artículo 5, fracción VI de la Ley de Seguridad Nacional; 47, Bis 4 de la Ley de Aviación Civil, 46 y 47 de la Ley de Aeropuertos y 152 del Reglamento de Aeropuertos.

Se elimina hoja completa, con fundamento en el artículo 110, fracción I de la LFTAIP;Décimo séptimo de los lineamientos Generales en materia de clasificación y desclasificación de la información,así como para la elaboración de versiones públicas, en relación con el artículo 5, fracción VI de la Ley de Seguridad Nacional; 47, Bis 4 de la Ley de Aviación Civil, 46 y 47 de la Ley de Aeropuertos y 152 del Reglamento de Aeropuertos.

Se elimina hoja completa, con fundamento en el artículo 110, fracción I de la LFTAIP;Décimo séptimo de los lineamientos Generales en materia de clasificación y desclasificación de la información,así como para la elaboración de versiones públicas, en relación con el artículo 5, fracción VI de la Ley de Seguridad Nacional; 47, Bis 4 de la Ley de Aviación Civil, 46 y 47 de la Ley de Aeropuertos y 152 del Reglamento de Aeropuertos.

Se elimina hoja completa, con fundamento en el artículo 110, fracción I de la LFTAIP;Décimo séptimo de los lineamientos Generales en materia de clasificación y desclasificación de la información,así como para la elaboración de versiones públicas, en relación con el artículo 5, fracción VI de la Ley de Seguridad Nacional; 47, Bis 4 de la Ley de Aviación Civil, 46 y 47 de la Ley de Aeropuertos y 152 del Reglamento de Aeropuertos.

Se elimina hoja completa, con fundamento en el artículo 110, fracción I de la LFTAIP;Décimo séptimo de los lineamientos Generales en materia de clasificación y desclasificación de la información,así como para la elaboración de versiones públicas, en relación con el artículo 5, fracción VI de la Ley de Seguridad Nacional; 47, Bis 4 de la Ley de Aviación Civil, 46 y 47 de la Ley de Aeropuertos y 152 del Reglamento de Aeropuertos.

Se elimina hoja completa, con fundamento en el artículo 110, fracción I de la LFTAIP;Décimo séptimo de los lineamientos Generales en materia de clasificación y desclasificación de la información,así como para la elaboración de versiones públicas, en relación con el artículo 5, fracción VI de la Ley de Seguridad Nacional; 47, Bis 4 de la Ley de Aviación Civil, 46 y 47 de la Ley de Aeropuertos y 152 del Reglamento de Aeropuertos.

Se elimina hoja completa, con fundamento en el artículo 110, fracción I de la LFTAIP;Décimo séptimo de los lineamientos Generales en materia de clasificación y desclasificación de la información,así como para la elaboración de versiones públicas, en relación con el artículo 5, fracción VI de la Ley de Seguridad Nacional; 47, Bis 4 de la Ley de Aviación Civil, 46 y 47 de la Ley de Aeropuertos y 152 del Reglamento de Aeropuertos.

#	Requerimiento de INAI-DGNC:	Desahogo de requerimiento:
3	*En relación con la implementación, y con fundamento en lo dispuesto por los artículos 14, fracción I y 15 fracción IV de las Disposiciones administrativas, se requiere se remita, en su caso, el marco normativo que resulte aplicable como: leyes, lineamientos, manuales, estatutos, protocolos, circulares o cualquier otro instrumento jurídico, indicando los artículos y fracciones aplicables, en el cual se sustente la implementación del "Sistema de Procesamiento de Pasajeros", por el AIFA, es decir, el fundamento legal que motive, conforme a las facultades o atribuciones que la normatividad le confiere al AIFA la implementación del Sistema en cuestión.* *Asimismo, en su caso, se solicita remitir la normatividad nacional e internacional aplicable en materia de tratamiento de datos biométricos que resulte de base para llevar a cabo el tratamiento de datos personales de esta índole.*	*Integración: con el equipamiento de puntos de validación (preseguridad y abordaje) E-Gates GT11 de Vision-Box y la aplicación móvil del AIFA.* *El marco normativo que sustenta la implementación del "Sistema De Procesamiento De Pasajeros", por el AIFA(Anexo 1):* • *Constitución política de los Estados Unidos Mexicanos artículo 6 fracción II y 16. https://www.diputados.gob.mx/LeyesBiblio/pdf/CPEUM.pdf* • *Convenio Internacional en materia de datos personales (108) en materia de datos personales. https://www.clarkemodet.com/news-posts/mexico-y-el-convenio-108-de-europa-sobre-proteccion-de-datos-personales-a-nivel-internacional/#:~:text=El%20Convenio%20108%20tiene%20como,de%20una%20autoridad%20responsable%20de* • *La Adhesión de México al Convenio Internacional en materia de protección de datos personales, firmado el 13 de junio de 2018 de la LGPDPPSO. https://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPPSO.pdf* *1. Programa institucional 2021-2024 de la Empresa de Participación Estatal Mayoritaria Aeropuerto Internacional Felipe Ángeles, S.A. de C.V., https://dof.gob.mx/nota_detalle.php?codigo=5636590&fecha=29/11/2021#gsc.tab=0* ***6.- Objetivos Prioritarios*** ***6.1 Relevancia del Objetivo Prioritario 1.-*** *Contribuir al desarrollo de la industria*

Requerimiento de INAI-DGNC:	***Desahogo de requerimiento:***
	aeroportuaria del País a través de la eficiente administración e los recursos humanos, materiales, financieros y de tecnologías de la Información del Aeropuerto Internacional Felipe Ángeles, en apego a los más altos niveles de valores y normativa establecida por la Administración Pública Federal. *"...Las TIC's en muy poco tiempo han experimentado significativos cambios, con equipos y programas que simplifican los procesos y economizan los recursos; en este contexto, las instalaciones y equipos de la entidad sin duda están en un nivel competitivo y se cuenta con recursos humanos de gran experiencia; sin embargo, se requiere deuna actualización constante y capacitación permanente que acompañe el acelerado cambio de las TIC's.* *El empleo de las TIC's, también requiere de nuevas capacidades y competencias para usar y adaptar tecnologías, para generar y gestionar el conocimiento ysu aplicación ante los cambios vertiginosos, generando nuevos paradigmas que respondan a las necesidades del sector aeroportuario..."* ***6.3 Relevancia del Objetivo Prioritario 3.-*** *Brindar servicios aeroportuarios con calidad ydisponibilidad en beneficio de los clientes y usuarios."...Para la operación del Aeropuerto Internacional "Felipe Ángeles", se espera contar con una infraestructura de comunicación y transporte, para ofrecer un servicio de excelente calidad y que opere de forma exitosa durante el transcurso de los años..."* ***7. Estrategias prioritarias y Acciones puntuales.***

#	*Requerimiento de INAI-DGNC:*	*Desahogo de requerimiento:*
		Estrategia Prioritaria 1.3- *Fomentar la participación de los usuarios de los servicios del AIFA, a través del uso de las TIC's.* ***2. Ley de Aviación Civil*** ***Artículo 47 Bis 4.*** *Los pasajeros deberán:* *I. Brindar al permisionario o concesionario información y datos personales veraces, al momento de la compra del boleto;* *II. Presentar documentos oficiales de identificación, a solicitud del permisionario o concesionario o del personal autorizado del aeropuerto;* *III. Acatar las normas de seguridad y operación aeroportuarias vigentes;* *IV. Ocupar el asiento asignado, a menos que la tripulación por un requerimiento justificado le solicite o le autorice ocupar uno distinto, y* *V. Las demás que establezcan la Ley y demás ordenamientos.* ***3. Ley de Aeropuertos*** ***ARTÍCULO 46.*** *Corresponderá a los concesionarios o permisionarios, conforme a las disposiciones aplicables y con base en el título de concesión o permiso respectivo, asegurar que los aeródromos civiles cuenten con la infraestructura, instalaciones, equipo, señalización, módulo de primeros auxilios y emergencias médicas, servicios y sistemas de organización, adecuados y suficientes para que la operación y atención al usuario se lleve a cabo sobre bases de seguridad, eficiencia y calidad.* ***ARTÍCULO 47.*** *Los concesionarios o permisionarios deberán responsabilizarse*

Requerimiento de INAI-DGNC:	***Desahogo de requerimiento:***
	del control de los accesos y tránsito de personas, vehículos y bienes en zonas restringidas del aeródromo civil, así como de que las áreas cercanas a los equipos de ayuda a la navegación aérea instalados dentro de los mismos, se mantengan libres de obstáculos que puedan afectar su operación. ***4. Reglamento de la Ley de Aeropuertos*** ***ARTÍCULO 152**, fracciones I, II, III y V.* *Tratándose de aeródromos de servicio al público, las medidas de seguridad deberán comprender lo siguiente:* *I. Los dispositivos de protección y control de accesos a las zonas restringida y estéril;* *II. Las medidas de acceso y de control del movimiento de personas y vehículos en las zonas restringidas;* ***5. OACI*** ***Anexo 17** al Convenio sobre Aviación Civil Internacional, Seguridad, Protección de la aviación civil internacional contra los actos de interferencia ilícita.* ***CAPÍTULO 3. ENTRADA Y SALIDA DE PERSONAS Y DE SU EQUIPAJE*** ***C. Seguridad de los documentos de viaje.*** ***3.7** Los Estados contratantes actualizarán regularmente los elementos de seguridad que figuran en las nuevas versiones de sus documentos de viaje, a fin de impedir su uso indebido y facilitar la detección en los casos en que dichos documentos se*

#	Requerimiento de INAI-DGNC:	Desahogo de requerimiento:
		hayan alterado, duplicado o emitido en forma ilegal. ***3.8*** *Los Estados contratantes establecerán controles con respecto a la creación y expedición de los documentos de viaje a fin de protegerse contra el robo de sus inventarios y el apoderamiento indebido de documentos de viaje recientemente emitidos.* ***3.9 Método recomendado.*** *Los Estados contratantes deberían incorporar datos biométricos en sus pasaportes, visados y otros documentos de viaje oficiales de lectura mecánica, utilizando una o más de las técnicas de almacenamiento de datos optativos para suplementar la zona de lectura mecánica, según se especifica en el Doc 9303, Documentos de viaje de lectura mecánica. Los datos requeridos almacenados en un microcircuito integrado son los mismos que se imprimen en la página de datos; o sea, los datos contenidos en la zona de lectura mecánica más la imagen fotográfica digitalizada. Los Estados contratantes que deseen suplementar la imagen facial con otro elemento biométrico en el pasaporte pueden utilizar imágenes de lasimpresiones digitales o del iris. Los Estados contratantes que incorporen datos biométricos en sus pasaportes de lectura mecánica deben almacenar los datos en un microcircuito integrado sin contacto que cumpla con la norma ISO/IEC 14443 y esté programado de conformidad con la estructura lógica de datos establecida por la OACI.* ***I. Inspección de documentos de viaje***

Requerimiento de INAI-DGNC:

Desahogo de requerimiento:

3.35.1 *Las autoridades competentes de cada Estado contratante se incautarán de los documentos de viaje fraudulentos, falsificados o imitados. Las autoridades competentes también se incautarán de los documentos de viaje de una persona que se presenta pretendiendo ser el titular legítimo del documento de viaje. Tales documentos se retirarán de la circulación inmediatamente y se devolverán a las autoridades competentes del Estado que figura como expedidor o a la misión diplomática residente de ese Estado.*

6. LEY DE CIENCIA Y TECNOLOGIA

Capitulo 1

- *Artículo 1: La presente Ley artículo 3 de la Constitución política de los Estados Unidos Mexicanos, y tiene por objetivo: Regular los apoyos que el Gobierno Federal está obligado aotorgar para impulsar, fortalecer, desarrollar y consolidar la investigación científica, el desarrollo tecnológico y la innovación en general en el país.*

Adicionalmente, el fundamento legal que sustenta la implementación del" Sistema De Procesamiento De Pasajeros", por el AIFA, es el siguiente:

Con fecha 15 de octubre del 2021 fue publicado en el Diario Oficial de la Federación el TÍTULO de Concesión que otorga la Secretaría de Comunicaciones y Transportes, a favor de la Empresa de Participación Estatal Mayoritaria Aeropuerto Internacional Felipe Ángeles, S.A. de C.V.

#	***Requerimiento de INAI-DGNC:***	***Desahogo de requerimiento:***
		"CONCESIÓN QUE OTORGA EL GOBIERNO FEDERAL, POR CONDUCTO DE LA SECRETARÍADECOMUNICACIONES Y TRANSPORTES, REPRESENTADA POR SU TITULAR EL ING.JORGE ARGANIS DÍAZ LEAL, AFAVOR DE LA SOCIEDAD DENOMINADA AEROPUERTO INTERNACIONAL FELIPE ÁNGELES, S.A. DE C.V. EMPRESADE PARTICIPACIÓN ESTATAL MAYORITARIA DE NACIONALIDAD MEXICANA, REPRESENTADA POR SU DIRECTORGENERAL EL GENERAL DE BRIGADA D.E.M. RENÉTRUJILLO MIRANDA; A QUIENES EN LO SUCESIVO SE LESDENOMINARÁ LA "SECRETARÍA" Y LA "CONCESIONARIA", RESPECTIVAMENTE. *I. El Plan Nacional de Desarrollo 2019 2024, , publicado en el Diario Oficial de la Federación ("DOF")el 12 de julio de 2019, establece en su Estrategia Nacional de Seguridad Pública entre otros, los siguientes objetivos: garantizar empleo, educación, salud y bienestar mediante la creación depuestos de trabajo, el cumplimiento del derecho de todos los jóvenes del país a la educación superior, la inversión en infraestructura y servicios de salud y por medio de los programas regionales, sectoriales y coyunturales de desarrollo a través del Aeropuerto "Felipe Ángeles" en Santa Lucía. En la Estrategia Política y Gobierno del Plan Nacional de Desarrollo 2019 2024, se prevé garantizar empleo, educación, salud y bienestar mediante la creación de puestos de trabajo, el cumplimiento del derecho de todos los jóvenes del país a la educación*

Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales

Requerimiento de INAI-DGNC:

Desahogo de requerimiento:

superior, la inversión en infraestructura y servicios de salud y por medio de los programas regionales, sectoriales y coyunturales de desarrollo, entre otros, el Aeropuerto "Felipe Ángeles" en Santa Lucía.

V. "LA CONCESIONARIA" es una empresa de participación estatal mayoritaria, cuya estructura accionaria está conformada con un 99% propiedad de la Secretaría de la Defensa Nacional y con un 1% propiedad del Banco Nacional del Ejército, Fuerza Aérea y Armada, S.N.C., tal y como consta en la Resolución por la que se autoriza la constitución de una Empresa de Participación Estatal Mayoritaria denominada Aeropuerto Internacional Felipe Ángeles, S.A. de C.V., misma que estará agrupada en el sector coordinado por la Secretaría de la Defensa Nacional, publicada en el Diario Oficial de la Federación el 14 de diciembre de 2020."

Siendo misión de la Subdirección de sistemas garantizar la infraestructura y los servicios de tecnologías de la información y comunicaciones al Aeropuerto Internacional Felipe Ángeles.
Y atendiendo las funciones del área como:
Supervisar que las comunicaciones, sistemas de operación aeroportuaria, administrativos, financieros y comercias, equipos de cómputo, sistemas de CCTV y control de Acceso, megafonía y Servicios de correo, internet y antivirus operan eficientemente a fin de apoyar la productividad del AIFA.

Se anexa Manual de Organización General – octubre 2021

#	***Requerimiento de INAI-DGNC:***	***Desahogo de requerimiento:***
4	*Con fundamento en el artículo 17 de la Ley General de Datos y artículo 15, fracción IV y XV de las Disposiciones Administrativas, se solicita lo siguiente:* *De las documentales presentadas, específicamente el referente al contrato No. SDN/DN8/AIFA/12916-F7/2021-ITP-043-02 que celebran por una parte, el Gobierno de los Estados Unidos Mexicanos a través de la Secretaría de la Defensa Nacional (SEDENA) y por otra parte las empresas Apollo Communications, S.A. de C.V., Química Apollo S.A. de C.V., Vision-Box Soluções de Visão por Computador, S.A. y Amadeus IT Group, S.A. de C.V. del que derivan en sus anexos, los elementos que componen el aplicativo, se identifica, que éste fue celebrado y signado por SEDENA, por lo tanto, se solicita el instrumento jurídico por el cual, se le otorga al AIFA, como sujeto obligado registrado con la clave 07003 de conformidad con la última actualización del Padrón de Sujetos Obligados del Ámbito Federal[19], en términos de la Ley General de Transparencia y Acceso a la Información Pública, las facultades y atribuciones para llevar a cabo y continuar con lo contratado con dichos proveedores referente al objeto de la presente Evaluación de impacto o en su caso la justificación y motivación del tratamiento del* ***"Sistema de Procesamiento de Pasajeros".***	*A este respecto el día 12 de enero del año en curso la empresa estatal de participación estatal mayoritaria Aeropuerto Internacional Felipe Ángeles S.A de C.V., (AIFA, S.A. de C.V.) entregó a la H. Dirección General a su cargo el documento* ***denominado instrumento jurídico en materia de tratamiento y protección de datos personales del sistema de procesamiento de pasajeros celebrado entre el responsable jurídico (agto. Ings "Felipe ángeles"), el responsable de operación aeroportuaria (AIFA, S.A. DE C.V.)*** *y el encargado (consorcio Apollo Communications S.A. de C.V.), cuya justificación de conformidad a lo establecido en los art. 58, 59, 60, 61, 62, 63 y 64 de la LGPDPPSO y 108 de los lineamientos generales, los cuales expresan que la relación entre el responsable y el encargado deberá estar formalizada mediante contrato o cualquier otro instrumento jurídico que le vincula con el mismo y delimita el ámbito de su actuación para la prestación de un servicio.* *No obstante, a fin de ser más nuevamente, se remite el documento de su interés y se encuentra en el Anexo 4.*
5	*Con fundamento en lo dispuesto por los artículos 18 de la Ley General de Datos, artículos 9 y 10 de los Lineamientos Generales y 14, fracción I 15 fracción VII de las Disposiciones administrativas, se solicita sean especificadas las finalidades generales y especificas del tratamiento de datos personales que se llevará a cabo mediante el* ***"Sistema de Procesamiento de Pasajeros".***	*Asimismo, considerando que, pueden existir en su caso finalidades distintas al tratamiento de datos personales que aquellas que motivaron su tratamiento, se solicita definir aquellas finalidades primarias y secundarias. Por otro lado, se observa que, en la evaluación de impacto presentada, atendiendo a las características y elementos*

[19] Publicado en el Diario Oficial de la Federación el 29 de agosto de 2019, disponible en el vínculo electrónico siguiente: http://www.dof.gob.mx/nota_detalle.php?codigo=5570690&fecha=29/08/2019; última actualización el 01 de agosto de 2022, disponible para su consulta en el vínculo electrónico siguiente: https://home.inai.org.mx/wp-content/documentos/Micrositios/Padron_Sujetos_Obligados.pdf, enlaces consultados por última vez el 28/02/2023.

Se elimina hoja completa, con fundamento en el artículo 110, fracción I de la LFTAIP;Décimo séptimo de los lineamientos Generales en materia de clasificación y desclasificación de la información,así como para la elaboración de versiones públicas, en relación con el artículo 5, fracción VI de la Ley de Seguridad Nacional; 47, Bis 4 de la Ley de Aviación Civil, 46 y 47 de la Ley de Aeropuertos y 152 del Reglamento de Aeropuertos.

#	***Requerimiento de INAI-DGNC:***	***Desahogo de requerimiento:***
		del enrolamiento o registro, durante su evolución, a medida que circula por cada punto de control y hasta su eliminación, luego del abordaje en la aeronave. Permitiéndole al pasajeroemplear su rostro como su identificación durante todo el proceso. Además de la integración con el sistema de uso común propuesto. ***Las finalidades específicas*** *que se encuentran en los avisos de privacidad son consideradas dentro de cada punto de registro y validación siendo las siguientes:* • *Vdesk: realizar el registro biométrico, en sitio y asistido por un agente, en los mostradores convencionales de documentación (Check-in).* • *Quiosco: ofrecer al pasajero la posibilidad de realizar el registro biométrico, en sitio, de manera autónoma, a través de los quioscos de auto-servicio de documentación-check in.* • *App: ofrece al pasajero la posibilidad de realizar un registro o enrolamiento biométrico en cualquier lugar y en cualquier momento, a través de la aplicación móvil del AIFA.* • *Pre-seguridad: llevar a cabo la validación de existencia de un registro biométrico en la base de datos (galería de pre-seguridad) o en su defecto verificar la elegibilidad de acceso de un pasajero mediante el pase de abordar, para permitir el acceso al área de filtros de seguridad.* • *Abordaje: llevar a cabo la validación de existencia de un registro biométrico en la base de datos (galería de abordaje) o en su defecto verificar la elegibilidad de acceso de un pasajero mediante el pase*

#	***Requerimiento de INAI-DGNC:***	***Desahogo de requerimiento:***
		de abordar, para permitir el acceso a la aeronave, enviando un mensaje de confirmación de abordaje al sistema de control de salidas de la aerolínea.
		Las finalidades primarias *por las cuales se recaban datos personalesno conllevan algún tipo de finalidades secundarias, esta es una de las razones por las que se considera que el PDE solo debe conservarse por un periodo de 24 hs.*
		Las finalidades licitas *están expresadas en el punto 3 del presente documento.* *Las figuras de los actores involucrados son las siguientes:*
6	*Con fundamento en el artículo 3, fracción XV, XXVII, XXVIII, XXXII, artículo 65 al 71 de la Ley General de Datos y artículo 15, fracción X y fracción XV de las Disposiciones administrativas, se solicita definir claramente las figuras de los actores involucrados como son: responsable, encargado y en su caso subencargado que participan en el tratamiento de datos personales objeto de esta Evaluación de impacto, así como definir, los procesos, motivos y procedimientos establecidos por los cuáles desempeñaran la figura correspondiente, en su caso, y la forma de obtener los datos personales, es decir, si el AIFA tratará los datos directamente del titular o serán recabados de algún medio diferente, así como las fuentes de su obtención, es decir, de manera directamente de éste (cuando el responsable obtiene directamente del titular los datos personales cuándo éste los proporciona por algún medio que permita su entrega directa; medios electrónicos, ópticos, sonoros, visuales, vía telefónica, Internet o cualquier otra tecnología y/o medio) o indirectamente de éste (cuando no se obtienen de la forma descrita previamente), de conformidad con el artículo 18 y 19 de los Lineamientos Generales.*	***Responsable de Operación Aeroportuaria*** *(Subdir. Sist. AIFA, S.A. de C.V.)proceso Supervisión de Cumplimiento.* ***Responsable jurídico. Agrupamiento de Ingenieros*** ***Encargado:*** *Consorcio Apollocom, AMADEUS, Vision-Box S.A. de C.V.* *En relación al artículo 3 Fracción XV el responsable es el AIFA identificando como encargado del tratamiento de los datos personales al consorcio Apollocom, AMADEUS, Vision-Box S.A. de C.V., fracción XXVII, de quienes se define el nivel de responsabilidad comunicación y remisión es realizada exclusivamente entre el responsable y el encargado dentro del AIFA.* *El encargado será el responsable del tratamiento de los datos personales, por lo*

#	*Requerimiento de INAI-DGNC:*	*Desahogo de requerimiento:*
		que es este quien recibe directamente del titular dicha información. *Definiéndolos como responsables de realizar los procesos y procedimientos de almacenamiento y procesamiento de los datos, soporte en sitio, encargados de atender las fallas en relación con el Hardware y Software del "Sistema de Procesamiento de Pasajeros", con motivo de mantener la funcionalidad del sistema operativo 24/7/365.* *Con fundamento en el Art. 65 se obtendrá el consentimiento expreso del titular a través de los avisos de privacidad que se darán a conocer por medio de los 3 puntos de enrolamiento del sistema.*
7	*Con fundamento en el artículo 86 de la Ley General de Datos, 14, fracción VIII y 15, fracción V y XV de las Disposiciones Administrativas, indicar las categorías de los titulares, distinguiendo aquéllos que pertenezcan a grupos vulnerables, en su caso, en función de su edad; origen étnico o racial; estado de salud; preferencia sexual; nivel instrucción y condición socioeconómica de los cuales se pretende llevar a cabo el tratamiento de datos personales derivado de la implementación del* ***"Sistema de Procesamiento de Pasajeros",*** *además de señalar los mecanismos que se tienen contemplando para procurar su derecho a la protección de datos personales en igualdad de circunstancias.*	*Tal como se señaló en el Inventario de Datos y el Documento de Seguridad, donde se encuentra especificado cuales son los datos sensibles tratados. Se aclara que no hay uso de los datos de estado de salud preferencia sexual; nivel instrucción y condición socioeconómica.* *Se anexa tabla de datos tratados (documento de seguridad, Anexo 6)*

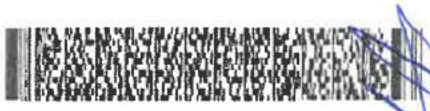
#	***Requerimiento de INAI-DGNC:***	***Desahogo de requerimiento:***
8	*Con fundamento en el articulo 3, fracción X y 8, 9, fracción XI, 14 fracción VIII, 15, fracción VI y XV de las Disposiciones Administrativas, identificar si se considera que los datos biométricos objeto de tratamiento en la implementación del* ***"Sistema de Procesamiento de Pasajeros"****, se consideran datos personales sensibles y en función de qué, explicando las consideraciones que se tengan al respecto.*	*En relación con lo establecido por el Sistema Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales en su Consejo Nacional, en los Lineamientos Generales de clasificación y desclasificación de la información y para la elaboración de versiones públicas, se considera como información confidencial, con fundamento en el numeral Trigésimo octavo lo siguiente* *"Trigésimo octavo. Se considera susceptible de clasificarse como información confidencial:* *Los datos personales, entendidos como cualquier información concerniente a una persona fisica identificada o identificable, en términos de la norma aplicable que, de manera enunciativa mas no limitativa, se pueden identificar de acuerdo con las siguientes categorías:* *I. Datos identificativos: el nombre alias, seudónimo, domicilio, código postal, teléfono particular, sexo, estado civil, teléfono celular, firma, clave de Registro Federal de Contribuyentes (RFC). Clave Única de Registro de Población (CURP), Clave de Elector, Matricula del Servicio Militar Nacional, numero de pasaporte, lugar y fecha de nacimiento, nacionalidad, edad, fotografia, localidad y sección electoral y análogos.* *II. Datos de origen: Origen, etnia, raza, color de piel, color de piel, color de ojos, color y tipo de cabello, estatura, complexión y análogos.* *III. Datos ideológicos: ideologías, creencias, opinión política, afiliación política, opinión*

#	***Requerimiento de INAI-DGNC:***	***Desahogo de requerimiento:***
		pública, afiliación sindical, religión, convicción filosófica y análogos. *IV. Datos sobre la salud: El expediente clínico de cualquier atención médica, historial médico, referencia o descripción de sintomatologías, detección de enfermedades, incapacidades médicas, discapacidades, intervenciones quirúrgicas, vacunas, consumo de estupefacientes, uso de aparatos oftalmológicos, ortopédicos, auditivos, prótesis, estado físico o mental de la persona, así como la información sobre la vida sexual y análogos.* *V. Datos laborales: Numero de seguridad social, documentos de reclutamiento o selección, nombramiento, incidencia, capacitación, actividades extracurriculares, referencias laborales, referencias personales, solicitud de empleo, hoja de servicio y análogos.* *VI. Datos patrimoniales: Bienes muebles e inmuebles de su propiedad, información fiscal, historial crediticio, ingresos y egresos, númerode cuenta bancaria y/o CLABE interbancaria de personas físicas y morales privadas, inversiones, seguros, finanzas, servicios contratados, referencias personales, beneficiarios, dependientes económicos, decisiones patrimoniales y análogos.* *VII. Datos sobre situación jurídica o legal: La información relativa a una persona que se encuentre o haya sido sujeta a un procedimiento administrativo seguido en forma de juicio o jurisdiccional en materia laboral, civil, penal, fiscal, administrativa o*

Requerimiento de INAI-DGNC:	***Desahogo de requerimiento:***
	de cualquier otra rama del Derecho y análogos. *VIII. Datos académicos: Trayectoria educativa, avances de créditos, tipos de exámenes, promedio, calificaciones, títulos, cedula profesional, certificados, reconocimientos y análogos.* *IX. Datos de tránsito y movimientos migratorios: información relativa al tránsito de las personas dentro y fuera del país, así como información migratoria, cedula migratoria, visa, pasaporte.* *X. Datos electrónicos: Firma electrónica, dirección de correo electrónico, código QR.* *XI.* ***Datos biométricos:*** *Huella dactilar, reconocimiento facial, reconocimiento de iris, reconocimiento de la geometría de la mano, reconocimiento vascular, reconocimiento de escritura, reconocimiento de voz, reconocimiento de escritura de teclado y análogos."* *II. La que se entregue con tal carácter por los particulares a los sujetos obligados, siempre y cuando tengan el derecho de entrega con dicho carácter la información, de conformidad con lo dispuesto en las leyes o en los Tratados Internacionales de los que el Estado Mexicanosea parte; y* *III. Los secretos bancarios, fiduciario, industrial, comercial, fiscal, bursátil y postal cuya titularidad corresponde a particulares, sujetos de derecho internacional o a sujetos obligados cuando no involucren el ejercicio de recursos públicos.*

#	***Requerimiento de INAI-DGNC:***	***Desahogo de requerimiento:***
		La información confidencial no estará sujeta a temporalidad alguna y solo podrán tener acceso a ella los titulares de esta, sus representantes y los integrantes de los sujetos obligados facultados para ello. *Para el tratamiento de datos biométricos, los sujetos obligados deberán de implementar los sistemas biométricos que sean necesarios para su debida utilización y protección.* *De conformidad con la reforma la fracción X del artículo 3 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, aprobada por la Cámara de Diputados el pasado 3 de febrero del 2021, para quedar como sigue:* *X. Datos personales sensibles; Aquellos que se refieren a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para este. De manera enunciativa mas no limitativa, se consideran sensibles aquellos datos personales que pueden revelar aspectos como origen racial o étnico, estado de salud presente o futuro, creencias o convicciones religiosas, filosóficas y morales, afiliación sindical, opinión política, información relativa a la preferencia u orientación sexual, información genética o biométrica dirigida a identificar de manera univoca a una persona física.* *Se anexa "Minuta proyecto de decreto", por el que se reforma la fracción X del Articulo 3 de la Ley General de la Protección de Datos Personales en Posesión de Sujetos Obligados(Anexo 7).*

Se elimina hoja completa, con fundamento en el artículo 110, fracción I de la LFTAIP;Décimo séptimo de los lineamientos Generales en materia de clasificación y desclasificación de la información,así como para la elaboración de versiones públicas, en relación con el artículo 5, fracción VI de la Ley de Seguridad Nacional; 47, Bis 4 de la Ley de Aviación Civil, 46 y 47 de la Ley de Aeropuertos y 152 del Reglamento de Aeropuertos.

#	Requerimiento de INAI-DGNC:	Desahogo de requerimiento:
		  *Para mayor detalle, se anexa el documento "Intercambio de datos de información de aviación (AIDX)" y "Bar Coded Boarding Pass"(Anexo 8).*
	*Asimismo, toda vez que se advierte puede haber comunicación de datos personales durante la implementación del **"Sistema de Procesamiento de Pasajeros"**, se requiere mayor información sobre las transferencias y/o remisiones que en su caso se efectúen; identificando los momentos en los que se llevarán a cabo, así como los actores involucrados en este proceso como pueden ser; aerolíneas, sujetos obligados, entre otros.*	*Las transferencias y transmisiones de datos se encuentran definidas en los inventarios de datos que integran la EIPDP presentada a ese instituto el pasado 9 de enero del presente. Asimismo, se comparte nuevamente en formato digital el mencionado inventario.(Anexo 6 "Documentode Seguridad y Diagramas de Flujo")*
10	*En ese sentido, remitir los convenios, contratos o instrumentos jurídicos que definen y regulan dicha relación y por los cuales se establecen dichas comunicaciones de datos personales, en su caso, así como las cláusulas por las cuales se rigen conforme a la normatividad en la materia.* *Con fundamento en lo dispuesto por los artículos 15, fracción IX, X y XV de las Disposiciones administrativas, en cuanto a la confirmación de identidad, se solicita se identifique la forma en cómo se llevará a cabo la confrontación de los datos para la verificación y confirmación de la identidad de los usuarios, considerando las bases de datos que de este procedimiento puedan surgir al tomarse como referencia para dicha comparación a través de los documentos de identificación como puede ser el*	*La forma en que se lleva a cabo la confrontación de los datos para la verificación de identidad de los usuarios se la realiza en la Aplicación Móvil del AIFA, Quiosco de Auto Servicio CUSS, y en el Mostrador convencional CUPPS/Vdesk; y en los procesos de validación de identidad del pasajero, en las puertas de validación de identificación (Pre-Seguridad) y puertas automáticas de abordaje. Para mejor proveer*

Se elimina hoja completa, con fundamento en el artículo 110, fracción I de la LFTAIP;Décimo séptimo de los lineamientos Generales en materia de clasificación y desclasificación de la información,así como para la elaboración de versiones públicas, en relación con el artículo 5, fracción VI de la Ley de Seguridad Nacional; 47, Bis 4 de la Ley de Aviación Civil, 46 y 47 de la Ley de Aeropuertos y 152 del Reglamento de Aeropuertos.

Se elimina hoja completa, con fundamento en el artículo 110, fracción I de la LFTAIP;Décimo séptimo de los lineamientos Generales en materia de clasificación y desclasificación de la información,así como para la elaboración de versiones públicas, en relación con el artículo 5, fracción VI de la Ley de Seguridad Nacional; 47, Bis 4 de la Ley de Aviación Civil, 46 y 47 de la Ley de Aeropuertos y 152 del Reglamento de Aeropuertos.

Se elimina hoja completa, con fundamento en el artículo 110, fracción I de la LFTAIP;Décimo séptimo de los lineamientos Generales en materia de clasificación y desclasificación de la información,así como para la elaboración de versiones públicas, en relación con el artículo 5, fracción VI de la Ley de Seguridad Nacional; 47, Bis 4 de la Ley de Aviación Civil, 46 y 47 de la Ley de Aeropuertos y 152 del Reglamento de Aeropuertos.

#	***Requerimiento de INAI-DGNC:***	***Desahogo de requerimiento:***
	datos personales susceptibles de considerarse sensibles que se puedan contener o visualizar como parte del tratamiento de los datos personales para este objetivo, no puedan dar origen a discriminación por parte de los agentes o personal que realizará la acción descrita.	*i. El programa de Instrucción de Seguridad de la Aviación Civil del Aeropuerto Internacional "Felipe Ángeles", es el documento que establece el contenido de la capacitación a la que se sujeta el personal de la Guardia Nacional que desempeña las funciones de Inspector y Guardia de Seguridad, este incluye el curso* ***"Tronco común",*** *en el que se contempla la información correspondiente a Derechos Humanos, para prevenir la discriminación de los usuarios del AIFA (se anexa contenido del curso).* *5.1.1.6 Contenido del curso* **Tema** / **Inicial (min)** / **Recurrente (min)** Modulo 1 "Concientización en materia de Seguridad de la Aviación Civil" — 01:40 — 00:55 Modulo 2 "Trabajo en el aeropuerto" — 01:30 — 00:45 Modulo 3 "Derechos Humanos y facilitación de los pasajeros" — 02:00 — 01:10 Modulo 4 "Identificación de artefactos explosivos y otros artículos de uso restringido" — 03:30 — 01:50 Modulo 5 "Inspección del edificio2 — 02:00 — 01:00 Modulo 6 "Marco legal y normativo" — 06:00 — 08:30 Total de horas — 16:25 — 08:30 *ii. Los instructores que imparten la capacitación al personal de la Guardia Nacional que se desempeña como Inspectores y Guardias de Seguridad, cuentan con la certificación correspondiente para impartir capacitación en materia de seguridad de la aviación ante la Agencia Federal de Aviación Civil.* *Normatividad* *Las actividades de verificación de identidad de forma manual se aplican de conformidad al contenido de la normatividad emitida por la Agencia Federal de Aviación Civil (CO Sa 17.6/16 "Procedimiento para la inspección de*

#	***Requerimiento de INAI-DGNC:***	***Desahogo de requerimiento:***
		pasajero y equipaje de mano en los aeródromos civiles de servicio al público", se anexa copia), de forma similar al resto de aeropuertos del territorio nacional.
12	*Con fundamento en el artículo 14, fracción V y 20 de las Disposiciones administrativas, se solicita la descripción de los mecanismos o procedimientos por defecto y diseño que la implementación del **"Sistema de Procesamiento de Pasajeros"**, le permitan aplicar de forma efectiva el cumplimiento de los principios, deberes y demás obligaciones previstas en la Ley General de Datos y Lineamientos Generales. Los mecanismos y procedimientos deben ser acompañados con pruebas que demuestren el debido cumplimiento de cada uno, aclarando que no basta el pronunciamiento positivo del cumplimiento, se debe enviar pruebas que acrediten lo manifestado, señalando lo siguiente:* • *De conformidad con el artículo 17 de la Ley General de Datos, en atención al principio de licitud se deberá señalar el marco normativo desde leyes, tratados o acuerdos nacionales e internacionales, reglamentos, lineamientos entre otros; que facultan al sujeto obligado y a la unidad administrativa a tratar los datos personales para cada una de las finalidades, y aquél que regula el tratamiento respectivo de los datos personales bajo su posesión de forma específica, señalando precepto específico y normatividad, es decir, el o los instrumentos jurídicos que otorgan al AIFA la atribución de llevar a cabo la actividad objeto de la Evaluación de impacto.*	*El principio de licitud está agotado en el punto 3 de este documento, ya que en dicho documento se encuentra toda la normatividad que rige actividad del AIFA S.A. de C.V. para estar en posibilidades de efectuar el tratamiento de datos personales en su calidad de responsable de operación aeroportuaria.*
	• *En cuanto al principio de lealtad, el artículo 19 de la Ley General de Datos, contempla el deber del responsable de mostrar el tratamiento apegado a la normatividad y que la obtención del titular no se realizó a través de medios engañosos o fraudulentos, asimismo que se privilegió la protección de los intereses del titular y la expectativa razonable de privacidad; en el que se confirme que*	*Además de lo ya mencionado, en los avisos de privacidad(simple e integral)se ve reflejada la obtención del consentimiento expreso del particular, así como las finalidades por las cuales se recaban los datos, así como las transferencias que para el procesamiento de pasajeros se requieran, lo anterior en cumplimiento a lo que*

#	***Requerimiento de INAI-DGNC:***	***Desahogo de requerimiento:***
	el tratamiento no da lugar a discriminación o trato injusto o arbitrario en contra del titular, por lo cual, deberá señalar las razones que se consideren sustenten el cumplimiento de este principio por parte del responsable.	*dispone el último párrafo del artículo 21 de la LGTAIP, que expresa que tratándose de datos personales sensibles el responsable deberá obtener el consentimiento expreso y por escrito del titular para su tratamiento, a través de mecanismos como el de autenticación que se establezca.* *A mayor abundamiento, el proceso de validación de identidad se realiza de la siguiente manera:* *Paso Uno: será mostrado el aviso de privacidad simplificado en el que también se da a conocer en donde se puede consultar el aviso de privacidad integral, si este aviso no es aceptado por el titular, se finaliza el proceso de enrolamiento.* *Paso Dos: Una vez aceptado el dicho aviso se procede a realizar la validación de identidad 1:1 cruzando los valores de los vectores obtenidos de la imagen del documento de identidad con los vectores de la imagen capturada en tiempo real, la cual permite identificar que efectivamente sea el titular quien está dando la aceptación del aviso de privacidad.* *En caso de no encontrar coincidencias, es finalizado el proceso de enrolamiento y no es almacenado ninguno de los datos leídos.* *En la página web será publicado el procedimiento de enrolamiento para conocimiento de los particulares, como un ejercicio del principio de información. De conformidad con el artículo 25 de la ley general de datos, referente al principio de proporcionalidad, si bien, se identifican los*

Se elimina hoja completa, con fundamento en el artículo 110, fracción I de la LFTAIP;Décimo séptimo de los lineamientos Generales en materia de clasificación y desclasificación de la información,así como para la elaboración de versiones públicas, en relación con el artículo 5, fracción VI de la Ley de Seguridad Nacional; 47, Bis 4 de la Ley de Aviación Civil, 46 y 47 de la Ley de Aeropuertos y 152 del Reglamento de Aeropuertos.

#	***Requerimiento de INAI-DGNC:***	***Desahogo de requerimiento:***
		principio de implementación la Minimización de datos, así como en el propósito delimitado de recolectar datos personales adecuados y relevantes parala finalidad. *Con relación a la "expectativa razonable de privacidad; en el que se confirme que el tratamiento no da lugar a discriminación o trato injusto orbitario en contra del titular, por lo cual, deberá señalar las razones que se consideren sustenta en el cumplimiento de este principio por parte del responsable."* *Se encuentra agotado en el punto inmediato anterior, este incluye el curso* ***"Tronco común"****, en el que se contempla la información correspondiente a Derechos Humanos, para prevenir la discriminación de los usuarios del AIFA.*
	• *De conformidad con los artículos 26, 27 y 28 de la Ley General de Datos, referente al principio de información, si bien, se remiten los avisos de privacidad en sus diversas modalidades (integral y simplificado) y se indica que éstos se podrán a disposición a través de la pantalla, no se indica el tipo de consentimiento requerido en función de los datos personales a tratar ni forma de obtención, por lo que, se solicita indicar con exactitud lo mencionado, además de precisar si existirán medios adicionales al electrónico, como son formatos físicos, ópticos, sonoros, visuales o a través de cualquier otra tecnología que permita su eficaz comunicación; así como si aparecen en el* ***"Sistema de Procesamiento de Pasajeros"****.*	*En la página web será publicado el procedimiento de enrolamiento para conocimiento de los particulares, como un ejercicio del principio de información.* *El tipo de consentimiento es expreso y es recabado directamente del titular a través de medios electrónicos de manera digital al llevar a cabo el proceso de registro biométrico; ya que, para poder realizar el enrolamiento, es requisito aceptar el aviso de privacidad en cualquiera de las tres modalidades de registro (App, Quiosco de Autoservicio y Vdesk) a través de una pantalla táctil. En caso de no ser aceptado, se dará por finalizado el proceso de registro y realizara el abordaje de manera tradicional.*
	• *Con fundamento en los artículos 29 y 30 de la Ley General de Datos, referentes al principio de responsabilidad, se solicita señalar las políticas internas y programas de gestión y tratamiento de*	*Además de contar con las políticas internas y programas de gestión del AIFA, se encuentran disponibles en el apartado virtual https://media-aifa.s3.us-east-*

Se elimina hoja completa, con fundamento en el artículo 110, fracción I de la LFTAIP;Décimo séptimo de los lineamientos Generales en materia de clasificación y desclasificación de la información,así como para la elaboración de versiones públicas, en relación con el artículo 5, fracción VI de la Ley de Seguridad Nacional; 47, Bis 4 de la Ley de Aviación Civil, 46 y 47 de la Ley de Aeropuertos y 152 del Reglamento de Aeropuertos.

Se elimina hoja completa, con fundamento en el artículo 110, fracción I de la LFTAIP;Décimo séptimo de los lineamientos Generales en materia de clasificación y desclasificación de la información,así como para la elaboración de versiones públicas, en relación con el artículo 5, fracción VI de la Ley de Seguridad Nacional; 47, Bis 4 de la Ley de Aviación Civil, 46 y 47 de la Ley de Aeropuertos y 152 del Reglamento de Aeropuertos.

#	***Requerimiento de INAI-DGNC:***	***Desahogo de requerimiento:***
	encontrarán en posesión del responsable", al contemplarse, de conformidad con la Ley General de Datos, el ejercicio de los derechos ARCO y en su caso, el derecho de portabilidad dentro de la protección de datos personales, así como la obligación del responsable de facilitarlo. Asimismo, se solicita conocer los procedimientos internos para asegurar la eficiencia de la gestión de las solicitudes al ejercicio de derechos ARCOP respecto de los datos personales de tratamiento por parte de responsable y los cuales serán sujetos a través del ***"Sistema de Procesamiento de Pasajeros"****.*	*de que el AIFA no cuenta con la posibilidad de hacer un proceso de reversibilidad de los mismos, en virtud de que no cuenta con dichos datos de manera identificable en su repositorio no puede hacer efectivas las solicitudes delos derechos ARCOP de las personas titulares dado que el responsable Operador Aeroportuario no puede identificar al titular de los mismos debido a que los datos se encuentran codificados. Por lo que se vería así la información (imagen código en símbolo del sistema).*  *De acuerdo con el Artículo 23 de la GPDPPSO "cuando los datos personales hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas en los avisos de privacidad y que motivaron su tratamiento conforme a las disposiciones que resulten aplicables, deberán ser suprimidos, previo bloqueo en su caso, y una vez que concluya el plazo de conservación de los mismos".* *Lo anterior atendiendo al criterio de minimización mediante el cual los datos personales estén disponibles durante el tiempo indispensable en el proceso de abordaje y evitar así un riesgo critico en el tratamiento de los mismos.* *Por lo que en la operación inicial del Sistema de Procesamiento de Pasajeros del AIFA el plazo señalado de 24 horas máximo para el borrado de los datos personales cumple con las finalidades que justificaron su tratamiento.*

#	***Requerimiento de INAI-DGNC:***	***Desahogo de requerimiento:***
		El borrado en el plazo mencionado de 24 horas garantizará la correcta funcionalidad del sistema durante los procesos internos de consulta ya que una cantidad alta de registros pudiera resultar en afectaciones al procesamiento de los datos y a la integridad del sistema, aunado a un costo desproporcionado por almacenamiento de datos no inherentes a la finalidad de cada PDE.
	• *Asimismo, se solicita aclarar y proporcionar más información sobre "...una vez que se tengan figuras reales sobre los flujos de datos, el comportamiento del sistema, y para garantizar los derechos ARCO de los titulares se podría analizar, validad y ampliar el periodo de ciclo de vida del tratamiento de los datos personales en el Sistema de Procesamiento de Pasajeros del AIFA", en el mismo sentido que el punto anterior.*	*De acuerdo con la funcionalidad del sistema de procesamiento de pasajeros y al ciclo de vida de los datos tratados, el flujo de los mismos finalizará con la cancelación o supresión de datos personales una vez que pase por las E-Gate de Pre-Seguridad, sus datos se suprimirán de la Galería de Pre-Seguridad. De igual manera, una vez que el pasajero pasa por las E-Gate de Abordaje, sus datos se suprimirán de la Galería de Abordaje y de la base de datos.* *Después de 24 horas posteriores a la fecha de la salida del vuelo, se ejecuta una acción de borrado, de manera automática, de todos los PDE almacenados en las Galerías de la solución biométrica.*
	• *En concordancia con los puntos que anteceden, si bien refiere que "...después de 24 horas posteriores a la fecha de la salida del vuelo, se ejecuta una acción de borrado, de manera automática, de todos los PDE almacenados en las Galerías de la solución biométrica", se solicita señalar con claridad los periodos de conservación de los datos considerando que pueda surgir una solicitud al ejercicio de derechos ARCOP y que, como responsable se establece la obligación en la Ley General de Datos de facilitar dichos derechos a los titulares.*	*De acuerdo con el Artículo 23 de la LGPDPPSO cuando los datos personales hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas en los avisos de privacidad y que motivaron su tratamiento conforme alas disposiciones que resulten aplicables, deberán ser suprimidos, previo bloqueo en su caso, y una vez que concluya el plazo de conservación de los mismos.* *Después de 24 horas posteriores a la fecha de la salida del vuelo, se ejecuta una acción de borrado seguro de manera automática,*

#	***Requerimiento de INAI-DGNC:***	***Desahogo de requerimiento:***
	En ese sentido, se solicita remitir la documentación de los procedimientos para conservación y, en su caso, bloqueo y supresión de los datos personales definiendo el periodo de conservación de los mismos. *Por lo tanto, se sugiere identificar las obligaciones, en su caso, a los que el responsable como sujeto obligado se encuentra constreñido de la conservación y plazos de conservación establecidos de la información.*	*debido a que podrían presentarse los siguientes casos:* o *Que el pasajero no ingrese al área estéril del aeropuerto o no realice el abordaje.* o *Que el pasajero use el procedimiento de pre-seguridad de manera tradicional, con la asistencia de un agente, presentando el pase de abordar de forma física.* o *Que el pasajero use el procedimiento de abordaje tradicional, presentando el pase de abordar de forma física.* o *Que el vuelo sea suspendido.* o *Que exista requerimiento de las autoridades (transporte de drogas ilegales, casos de ebriedad o bajo el influjo de estupefacientes, psicotrópicos o enervantes, otros).* *El borrado seguro consiste en la eliminación de datos de Microsoft Windows del motor de base de datos SQL (DELETE Comando-SQL), que permiten borrar y eliminar de forma segura la información de las bases de datos y dispositivos de almacenamiento.* *De conformidad con el artículo 16 constitucional, una vez recibida una petición por parte de una autoridad judicial, se informara a la misma que el Sistema de Procesamiento de Pasajeros por su naturaleza no tiene la finalidad de aportar elementos para la seguridad aeroportuaria.*
	• *Aunado a lo anterior y, considerando la posible solicitud de acceso a datos personales por parte de una autoridad en materia de aplicación o cumplimiento de la ley. En ese sentido, se solicita aclarar, la forma en que se llevaría a cabo considerando los plazos de conservación de éstos, tomando en cuenta que, como refiere en la Evaluación de impacto a la protección de datos personales, los datos almacenados serían borrados después de 24 horas.* • *De igual forma se solicita remitir las medidas de seguridad implementadas, así como el análisis de brecha a realizar sobre la aplicación móvil de AIFA e indicar que al momento de descargarla se*	*Los permisos requeridos para la descarga de la aplicación son determinados por las tiendas digitales de descarga de aplicaciones, y son estas plataformas las*

Se elimina hoja completa, con fundamento en el artículo 110, fracción I de la LFTAIP;Décimo séptimo de los lineamientos Generales en materia de clasificación y desclasificación de la información,así como para la elaboración de versiones públicas, en relación con el artículo 5, fracción VI de la Ley de Seguridad Nacional; 47, Bis 4 de la Ley de Aviación Civil, 46 y 47 de la Ley de Aeropuertos y 152 del Reglamento de Aeropuertos.

Se elimina hoja completa, con fundamento en el artículo 110, fracción I de la LFTAIP;Décimo séptimo de los lineamientos Generales en materia de clasificación y desclasificación de la información,así como para la elaboración de versiones públicas, en relación con el artículo 5, fracción VI de la Ley de Seguridad Nacional; 47, Bis 4 de la Ley de Aviación Civil, 46 y 47 de la Ley de Aeropuertos y 152 del Reglamento de Aeropuertos.

#	Requerimiento de INAI-DGNC:	Desahogo de requerimiento:
	estos datos personales a través de servicios que éste ofrezca.	*jurídico (agto. Ings. "Felipe ángeles"), el responsable de operación aeroportuaria (AIFA, S.A. DE C.V.) y el encargado (consorcio Apollo Communications S.A. de C.V.),(ver Anexo 4).*
15	*Con fundamento en los artículos 14, fracción I, y 15 fracción XII de las Disposiciones Administrativas, se solicita la siguiente información:* • *A partir de la revisión de la documentación presentada, se observa la falta de documentación y detalle de explicación sobre la interconexión y el flujo de datos para la validación biométrica y no biométrica para el sistema de procesamiento de pasajeros, particularmente se identifican tratamientos no descritos en las etapas denominadas como pre-seguridad y abordaje, en éstas etapas se han identificado subtratamientos que no es posible analizar de la documentación presentada, por ejemplo, de la lectura a las documentales se advierte la generación de las bases de datos identificadas como: galería de pre-seguridad, galería de abordaje y galerías de solución biométrica, mismas que no se encuentran señaladas o descritas como parte integral del sistema de procesamiento, en consecuencia no es posible identificar si estos datos se encuentran almacenados en bases de datos dentro de la arquitectura del AIFA. Adicionalmente, es necesario incluir la descripción detallada sobre la interconexión de los sistemas provistos por externos al AIFA tales como Vision-Box Mobile ID, Vision-Box VDesk, E-GateGT11 y AMADEUS APV, ya que, se identifica que el procesamiento de información ocurre en servicios externos al AIFA que controlan dispositivos en tiempo real, en ese orden, se requiere la aclaración o descripción sobre la no intervención de estos sistemas y dispositivos para los pasajeros que usan la validación no biométrica así como el funcionamiento de los mismos al identificar un*	*La interoperabilidad se encuentra descrita en el punto No. 2 de este documento, adicionalmente se incluyen en el anexo 6 diagramas de flujo de procesamiento de información. En ese orden, al identificar diversos sistemas interoperables, se requieren mayores detalles sobre la interoperabilidad entre los dispositivos de usuarios, sistemas, aplicaciones, hardware y software que intervengan en el proceso de información del sistema de procesamiento de información del AIFA, a fin de identificar las API´s y configuraciones entre los sistemas conectados, conocer los mecanismos de seguridad para el intercambio de información e identificar la eventual recuperación de bases de datos en caso de ocurrir un evento adverso durante el proceso de captura de información. Por otra parte, no fue posible identificar los casos de uso que proporcionen información que ayude a dimensionar los escenarios de funcionamiento de los supuestos de acceso biométrico, es decir, casos de uso para identificar los accesos de usuarios que ya cuentan con personal data en Envelope (PDE) antes de llegar a las zonas de preseguridad, los que generan su PDE asistido o no asistido en áreas de pre seguridad y carga a, así como los casos de uso de acceso no biométrico.*

Se elimina hoja completa, con fundamento en el artículo 110, fracción I de la LFTAIP;Décimo séptimo de los lineamientos Generales en materia de clasificación y desclasificación de la información,así como para la elaboración de versiones públicas, en relación con el artículo 5, fracción VI de la Ley de Seguridad Nacional; 47, Bis 4 de la Ley de Aviación Civil, 46 y 47 de la Ley de Aeropuertos y 152 del Reglamento de Aeropuertos.

Se elimina hoja completa, con fundamento en el artículo 110, fracción I de la LFTAIP;Décimo séptimo de los lineamientos Generales en materia de clasificación y desclasificación de la información,así como para la elaboración de versiones públicas, en relación con el artículo 5, fracción VI de la Ley de Seguridad Nacional; 47, Bis 4 de la Ley de Aviación Civil, 46 y 47 de la Ley de Aeropuertos y 152 del Reglamento de Aeropuertos.

Se elimina hoja completa, con fundamento en el artículo 110, fracción I de la LFTAIP;Décimo séptimo de los lineamientos Generales en materia de clasificación y desclasificación de la información,así como para la elaboración de versiones públicas, en relación con el artículo 5, fracción VI de la Ley de Seguridad Nacional; 47, Bis 4 de la Ley de Aviación Civil, 46 y 47 de la Ley de Aeropuertos y 152 del Reglamento de Aeropuertos.

Se elimina hoja completa, con fundamento en el artículo 110, fracción I de la LFTAIP;Décimo séptimo de los lineamientos Generales en materia de clasificación y desclasificación de la información,así como para la elaboración de versiones públicas, en relación con el artículo 5, fracción VI de la Ley de Seguridad Nacional; 47, Bis 4 de la Ley de Aviación Civil, 46 y 47 de la Ley de Aeropuertos y 152 del Reglamento de Aeropuertos.

Se elimina hoja completa, con fundamento en el artículo 110, fracción I de la LFTAIP;Décimo séptimo de los lineamientos Generales en materia de clasificación y desclasificación de la información,así como para la elaboración de versiones públicas, en relación con el artículo 5, fracción VI de la Ley de Seguridad Nacional; 47, Bis 4 de la Ley de Aviación Civil, 46 y 47 de la Ley de Aeropuertos y 152 del Reglamento de Aeropuertos.

14 de las Disposiciones administrativas, así como, adicionalmente referir las características inherentes a los tratamientos relevantes o intensivos que se presenten en el caso particular.

Lo anterior, bajo la lógica prevista en las Disposiciones administrativas sobre el procedimiento establecido que implica la valoración por parte del Instituto de la evaluación de impacto en la protección de datos personales elaborada y presentada por el sujeto obligado, la cual constituye el punto de partida y marco de referencia para poder llevar a cabo el análisis, dictaminación, y, en su caso la emisión de recomendaciones no vinculantes.

Es decir, el alcance de la revisión a realizar se determina en función de los elementos proporcionados por parte del responsable y del análisis que éste realizó en la evaluación de impacto elaborada, por lo que no se puede sustituir o subsumir el análisis proporcionado por el responsable en su documento, y, por ende, se encuentra circunscrito al marco de referencia provisto por éste. Asimismo, no resulta factible prejuzgar sobre la calidad y completitud de la información proporcionada, por lo que, las conclusiones que deriven del presente documento se encontrarán soportadas en función de lo que se reportó y, en función de ello, cualquier aspecto no señalado, omitido o apreciado de manera diversa, deberá hacerse notar al Instituto a fin de brindar la clarificación correspondiente por los medios que correspondan.

Se debe considerar que las evaluaciones de impacto suponen una herramienta preventiva que permita a los sujetos obligados del tratamiento de datos personales en el sector público, afrontar los nuevos retos en la protección y seguridad de los datos personales que conlleva el uso de nuevas tecnologías y los procesos de digitalización que se están produciendo en el quehacer gubernamental, enfocada en la gestión continua de los riesgos potenciales para los titulares, asociados al tratamiento que se pretenda llevar a cabo.

Asimismo, su elaboración permite la implementación de un esquema de mejora práctica que permite asegurar y acreditar el cumplimiento de los principios, deberes y demás obligaciones establecidas en la Ley General y demás normatividad aplicable, al considerar y evaluar de manera previa la identificación y análisis de potenciales riesgos a los que pueden estar expuestos los titulares y sus datos personales en función de nuevos tratamientos a los que sean sometidos, tomando en consideración el desarrollo tecnológico y las técnicas existentes; la naturaleza, contexto, alcance y finalidades del tratamiento; las atribuciones y facultades del responsable y demás cuestiones que considere convenientes para establecer la adopción de medidas necesarias para reducirlos a un nivel de riesgo aceptable.

Cabe señalar que, en la valoración del tratamiento relevante o intensivo motivo de la evaluación de impacto que nos ocupa, así como de su dictaminación se realizará desde la perspectiva de género,

y un enfoque de derechos humanos, incluyendo el principio de no discriminación, contenidos en la Constitución, con la finalidad de prever recomendaciones y observaciones sobre el tratamiento adecuado de los datos personales del que se podrá, en su caso, eventualmente emitir recomendaciones no vinculantes.

De igual forma, el dictamen emitido no tendrá el efecto de impedir la implementación del Sistema de Procesamiento, que implique el tratamiento intensivo o relevante de datos personales en cuestión, como tampoco validar el presunto cumplimiento de las obligaciones previstas en la Ley General y demás disposiciones aplicables en perjuicio de las atribuciones conferidas al Instituto. Lo anterior, en virtud de que el objeto de este tipo de evaluaciones es orientar a los responsables sobre el fortalecimiento de las obligaciones en la materia mediante la emisión de recomendaciones no vinculantes.

El alcance del presente documento se encuentra limitado a las derivaciones lógicas que surgen del análisis de los documentos presentados, por lo cual, si bien el objeto del presente documento implica el análisis de los tratamientos relevantes o intensivos general y particulares identificados en la Evaluación de impacto, éste se encuentra circunscrito al análisis provisto en la evaluación de impacto en la protección de datos personales del Sistema de Procesamiento.

Finalmente, es importante advertir que el análisis no incluye pruebas de penetración ni peritajes, auditorías, ni peritajes al instrumento normativo y demás mecanismos utilizados en la implementación del Sistema de Procesamiento, por lo que las manifestaciones del Instituto no pueden entenderse como un visto bueno a la implementación de medidas de seguridad, sino que se limitan a realizar recomendaciones y observaciones sobre la seguridad de los datos personales a nivel documental; supuestos de análisis que se encuentran reconocidos de manera expresa en la Ley General y en las Disposiciones administrativas, bajo la lógica no sólo del trámite establecido expresamente para este procedimiento, sino del resultado de la dictaminación, hacia la eventual emisión de recomendaciones no vinculantes.

IV. Descripción del Sistema de Procesamiento de Pasajeros del AIFA, contexto y justificación de la evaluación de impacto.

IV.I Descripción del Sistema de Procesamiento.

De conformidad con lo manifestado en las documentales remitidas por el AIFA, con motivo de la evaluación de impacto antes citada, la información en la respuesta del requerimiento de información adicional y la contenida en los anexos, se informó lo siguiente sobre el Sistema de Procesamiento.

El Sistema de Procesamiento, es un sistema informático a través del cual se hace posible el registro o enrolamiento de pasajeros que confluyen en el AIFA, por medio del cual se recopila, autentica y verifica su información personal y de vuelo, haciendo posible su ingreso a los filtros de seguridad y abordaje de forma rápida y segura, a través del procedimiento no biométrico y procedimiento biométrico, consistentes en:

- **Procedimiento No Biométrico**: el pasajero debe presentar su pase de abordar (BCBP Bar Code Boarding Pass por sus siglas en inglés) en el punto de inspección correspondiente, donde un agente de seguridad confirmará su identidad comparando visualmente los datos de un documento de identificación (autorizada por la aerolínea) y la información de su pase de abordar. Una vez que se ha confirmado la identidad del pasajero, éste podrá acceder a los filtros de seguridad a través de las puertas electrónicas (E-gates), mismas que disponen de un lector de código (QR o Barras) del pase de abordar.

- **Procedimiento Biométrico:** se realiza a través del registro o reconocimiento facial del pasajero, el cual puede efectuarse de tres distintas maneras:
  - En el mostrador convencional de documentación (denominado como CUPPS, como será detallado más adelante), donde será asistido por un agente de la línea aérea (en este proceso, el pasajero deberá tomarse una fotografía de su rostro con el dispositivo V-desk)
  - En un quiosco de autoservicio (conocido como CUSS, como se analizará posteriormente), en donde la cámara de este dispositivo tomará la fotografía; o
  - A través de la App Móvil del AIFA, en la cual el usuario deberá tomarse una fotografía con su teléfono celular). Después de que el pasajero ha realizado el enrolamiento, podrá ingresar directamente a los filtros de seguridad colocándose frente la puerta electrónica.

En este contexto, es dable advertir que, dentro de la Evaluación de impacto presentada, se señala que el procesamiento biométrico no se encuentra configurado para menores de edad, sin especificar las edades comprendidas o bien, hacer alguna referencia en cuanto a adolescentes. En este sentido, se precisa q tratándose de menores de edad se realizará el procedimiento tradicional, es decir, el proceso no biométrico. Así, para el ingreso al área estéril, un agente de seguridad del AIFA realizará la verificación de su identidad y para el proceso de abordaje, un agente de la aerolínea realizará la validación.

En concordancia con lo anterior, se establece que, las personas elegibles para llevar a cabo el enrolamiento y verificación de identidad a través del proceso biométrico, son aquellas personas mayores de edad que pueden realizar un registro biométrico dentro de la solución de procesamiento biométricos de pasajeros. De esta manera, existen algunos requisitos para que un pasajero pueda registrarse biométricamente:

- El pasajero debe proveer su consentimiento para el uso de sus datos personales a través de los avisos de privacidad.
- El pasajero deberá proveer su documento de identidad (Pasaporte electrónico, pasaporte no electrónico o INE, según la fuente de registro biométrico).
- El pasajero deberá estar documentado en un vuelo. Deberá poseer un Pase de Abordar válido.
- Se deberá poder capturar una imagen del rostro (fotografía).
- El pasajero deberá ser mayor de edad (configuración actual de la plataforma vb orchestraTM)

Es importante destacar que, el registro o enrolamiento biométrico, hace posible la generación del sobre de datos del denominado como PDE, consistente en un identificador digital único de cada pasajero, el cual será utilizado y actualizado por la plataforma vb orchestra™ en los diferentes pasos del proceso con el fin de registrar al pasajero en las bases de datos y las galerías biométricas.

Conforme a lo anterior es menester indicar que, el Sistema de Procesamiento involucra la fase de acceso a los filtros de seguridad del AIFA, tomando en consideración que, para que un pasajero pueda tomar un vuelo desde el AIFA, debe contar con un registro de documentación (check-in) con alguna de las aerolíneas que operan en este aeropuerto, ya sea realizándolo directamente en las instalaciones del aeropuerto, o a través de los medios digitales de las aerolíneas, y que una vez que el pasajero obtiene su pase de abordar, tendrá la opción de acceder a los filtros de seguridad a través del registro biométrico o no biométrico, dejándolo a su elección.

En esta tesitura, se advierte que, el registro biométrico para el procesamiento dentro del AIFA es totalmente opcional para el pasajero, por ende, en caso de que el pasajero decida no enrolarse, utilizará el procesamiento o los flujos no biométricos a partir de las puertas de preseguridad y abordaje, supuesto en el que no habrá recolección ni almacenamiento de datos personales a través del PDE.

De esta manera, es dable advertir que, el Sistema de Procesamiento que operará en el AIFA está compuesto, entre otros elementos, por puertas electrónicas (E-Gate) que, junto con la funcionalidad biométrica facial, le proveerán al AIFA, la capacidad de procesar a los pasajeros de manera tradicional, es decir, no biométrica, a través del uso del pase de abordar (BCBP) y de manera biométrica facial, a través de los procesos de registro o enrolamiento e identificación biométrica facial.

Se elimina hoja completa, con fundamento en el artículo 110, fracción I de la LFTAIP;Décimo séptimo de los lineamientos Generales en materia de clasificación y desclasificación de la información,así como para la elaboración de versiones públicas, en relación con el artículo 5, fracción VI de la Ley de Seguridad Nacional; 47, Bis 4 de la Ley de Aviación Civil, 46 y 47 de la Ley de Aeropuertos y 152 del Reglamento de Aeropuertos.

Se elimina hoja completa, con fundamento en el artículo 110, fracción I de la LFTAIP;Décimo séptimo de los lineamientos Generales en materia de clasificación y desclasificación de la información,así como para la elaboración de versiones públicas, en relación con el artículo 5, fracción VI de la Ley de Seguridad Nacional; 47, Bis 4 de la Ley de Aviación Civil, 46 y 47 de la Ley de Aeropuertos y 152 del Reglamento de Aeropuertos.

a. Fase de documentación (check-in).
b. Fase de registro/enrolamiento.
c. Fase de verificación de identidad.

Al respecto, en la presentación de la Evaluación de impacto, el AIFA manifestó como objetivos generales y específicos del Sistema de Procesamiento, los siguientes:

a) Objetivo general

El optimizar el procesamiento de pasajeros, agilizando los procesos de pre-seguridad y abordaje, mediante la implementación de sistemas biométricos y sin contacto, para eficientar el uso de infraestructura del aeropuerto, generar eficiencias operativas para el aeropuerto, las aerolíneas y los operadores aeroportuarios, creando una mejor experiencia para el pasajero.

b) Objetivos específicos

- Beneficios para el pasajero:
  - Experiencia sin contacto.
  - Minimiza el uso papel.
  - Auto-servicio.
  - Reduce el tiempo de procesamiento para pasar a los filtros de pre-seguridad y realizar el embarque a la aeronave de manera rápida y segura.
- Beneficios para la aerolínea:
  - Optimiza el uso de recursos humanos.
  - Reduce el tiempo de documentación y abordaje, acelerando el flujo de salida de pasajeros.
  - Permite la validación automatizada de la identidad del pasajero.
  - Disminuir reclamo de pasajeros por atraso a sus vuelos.
- Beneficios para el aeropuerto:
  - Posiciona al AIFA como un aeropuerto de clase mundial y vanguardista.
  - Acelera los tiempos de procesamiento de pasajeros y reduce el congestionamiento de las áreas críticas (Pre-seguridad y abordaje).
  - Fortalece el proceso de seguridad mediante la identificación de pasajeros que ingresan a la zona de Pre-seguridad y confirmando la validez del pase de abordar con las aerolíneas.
  - Permite contar con información estadística del número de pasajeros que ingresan a los filtros de seguridad y realizan el abordaje mediante el uso de los E-gates (esta información no incluye datos personales).

- Permite desahogar áreas que son críticas: Pre-seguridad y abordaje, en consecuencia, permite a los pasajeros estar en mejor disposición y disponer de más tiempo para consumir alimentos, bienes y servicios en el área comercial del aeropuerto.

Asimismo, en la evaluación de impacto presentada, de manera específica por lo que hace a su anexo "Términos y condiciones", se informó que el Sistema de Procesamiento atiende a las siguientes finalidades general y específicas:

- Finalidad general: se consideran elementos de automatización para el procesamiento de pasajeros y sus bienes, privilegiando la infraestructura de uso común, así como las funcionalidades para crear condiciones "touchless", "paperless", "contactless", en un entorno post Covid, así como, la creación de un entorno de procesamiento automatizado desde el check-in hasta el abordaje mediante el apoyo con tecnologías biométricas en balance con las tradicionales, el Proveedor implementara de la Plataforma Orchestra y los puntos de contacto de identificación biométrica "en movimiento" (onte move) o "pausa y marcha" (Stop and go) de Vision-Box, como el componente principal de Gestión biométrica para el procesamiento de pasajeros dentro del AIFA, integrada al sistema de uso común de Amadeus. La plataforma Orchestra de Vision-Box, junto con los puntos de contacto de identificación biométrica "en movimiento" (on the move) o "pausa y marcha" (Stop and go), serán los responsables por la gestión de la identidad digital del pasajero, a través de un token digital llamado PDE (Passenger Data Envelope), desde su creación, al momento del enrolamiento o registro, durante su evolución, a medida que circula por cada punto de control y hasta su eliminación, luego del abordaje en la aeronave. Permitiéndole al pasajero emplear su rostro como su identificación durante todo el proceso. Además de la integración con el sistema de uso común propuesto.
- Finalidades específicas:
  - Vdesk: realizar el registro biométrico, en sitio y asistido por un agente, en los mostradores convencionales de documentación (Check-in).
  - Quiosco: ofrecer al pasajero la posibilidad de realizar el registro biométrico, en sitio, de manera autónoma, a través de los quioscos de auto-servicio de documentación-check in. App: ofrece al pasajero la posibilidad de realizar un registro o enrolamiento biométrico en cualquier lugar y en cualquier momento, a través de la aplicación móvil del AIFA.
  - Pre-seguridad: llevar a cabo la validación de existencia de un registro biométrico en la base de datos (galería de pre-seguridad) o en su defecto verificar la elegibilidad de acceso de un pasajero mediante el pase de abordar, para permitir el acceso al área de filtros de seguridad.
  - Abordaje: llevar a cabo la validación de existencia de un registro biométrico en la base de datos (galería de abordaje) o en su defecto verificar la elegibilidad de acceso de un

Se elimina hoja completa, con fundamento en el artículo 110, fracción I de la LFTAIP;Décimo séptimo de los lineamientos Generales en materia de clasificación y desclasificación de la información,así como para la elaboración de versiones públicas, en relación con el artículo 5, fracción VI de la Ley de Seguridad Nacional; 47, Bis 4 de la Ley de Aviación Civil, 46 y 47 de la Ley de Aeropuertos y 152 del Reglamento de Aeropuertos.

Las personas elegibles son aquellas personas que pueden realizar un registro biométrico dentro de la solución de procesamiento biométricos de pasajeros.
[...]"

Conforme a lo anterior, es posible advertir que, el Sistema de Procesamiento se definió y quedó configurado para no procesar biométricamente a pasajeros menores de edad, ya que para este sector se utilizará el procedimiento tradicional, es decir, el proceso no biométrico. En tal virtud, todos los pasajeros mayores de edad que cuenten con su pase de abordar y documento de identificación oficial podrían realizar el registro biométrico, si se cuenta con su consentimiento.

Finalmente, por lo que hace a los datos personales que serán objeto de tratamiento a través del Sistema de Procesamiento, es dable advertir que, en la evaluación de impacto presentada, se refiere que los datos personales pueden clasificarse en cuatro categorías, de acuerdo a la criticidad de los mismos por nivel de riesgo inherente, conforme a la Metodología de Análisis de Riesgo BAA, en el ítem 2.1 Clasificación de Datos Personales, documental que al efecto se señaló lo siguiente:

"2. Clasificación de los Datos Personales
El responsable deberá identificar los tipos de Datos Personales que se tratan, la sensibilidad de los mismos y el número de titulares para determinar el valor del riesgo inherente de los datos para un tercero no autorizado.
Los Datos Personales, pueden clasificarse en ***cuatro*** *categorías, de acuerdo a la criticidad de los mismos por el nivel de riesgos inherente:*
• Datos con nivel de riesgo inherente bajo
Esta categoría considera información general concerniente a una persona física identificada o identificable, que no corresponda a la información a la que refieren las otras tres categorías, como por ejemplo datos de identificación y contacto o información académica o laboral, tal como nombre, teléfono, edad, sexo, RFC, CURP, estado civil, dirección de correo electrónico, lugar y fecha de nacimiento, nacionalidad, puesto de trabajo y lugar de trabajo, idioma o lengua, escolaridad, cédula profesional, información migratoria, entre otra información que no refiera a las siguientes tres categorías.
• Datos con nivel de riesgo inherente medio
Esta categoría contempla los datos que permiten conocer la ubicación física de la persona, tales como la dirección física, información relativa al tránsito de las personas dentro y fuera del país, y/o cualquier otro que permita volver identificable a una persona a través de los datos que proporcione alguien más. Por ejemplo: dependientes, beneficiarios, familiares, referencias laborales, referencias personales, etc.
También son datos de riesgo inherente medio aquéllos que permitan inferir el patrimonio de una persona, que incluye entre otros, los saldos bancarios, estados y/o número de cuenta, cuentas de inversión, bienes muebles e inmuebles, información fiscal, historial crediticio, ingresos, egresos, buró de crédito, seguros, afores, fianzas, sueldos y salarios, servicios contratados. Incluye el número de tarjeta bancaria de crédito y/o débito.

Son considerados también, los datos de autenticación con información referente a los usuarios, contraseñas, información biométrica (huellas dactilares, iris, voz, entre otros), firma autógrafa y electrónica, fotografías, identificaciones oficiales, inclusive escaneadas o fotocopiadas y cualquier otro que permita autenticar a una persona.

Dentro de esta categoría se toman en cuenta los datos jurídicos tales como antecedentes penales, amparos, demandas, contratos, litigios y cualquier otro tipo de información relativa a una persona que se encuentre sujeta a un procedimiento administrativo seguido en forma de juicio o jurisdiccional en materia laboral, civil, penal o administrativa.

• Datos con nivel de riesgo inherente alto

Esta categoría de datos contempla a los Datos Personales sensibles, que de acuerdo a la Ley incluyen datos de salud, los cuales se refieren a la información médica donde se documente el estado de salud física y mental, pasado, presente o futuro; información genética; origen racial o étnico, ideología, creencias religiosas, filosóficas y morales, afiliación sindical, opiniones políticas, preferencia sexual, hábitos sexuales y cualquier otro cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para el titular.

•Datos con nivel de riesgo inherente crítico

Los datos de mayor riesgo son los que de acuerdo con su naturaleza derivan en mayor beneficio para un atacante, por ejemplo:

Información adicional de tarjeta bancaria que considera el número de la tarjeta de crédito y/o débito mencionado anteriormente en combinación con cualquier otro dato relacionado o contenido en la misma, por ejemplo, fecha de vencimiento, códigos de seguridad, datos de banda magnética o número de identificación personal (PIN).

Las personas de alto riesgo son aquéllas cuya profesión, oficio o condición están expuestas a una mayor probabilidad de ser atacadas debido al beneficio económico o reputacional que sus datos personales pueden representar para un atacante. Por ejemplo, líderes políticos, religiosos, empresariales, de opinión y cualquier otra persona que sea considerada como personaje público.

Asimismo, se considera a cualquier persona cuya profesión esté relacionada con la impartición de justicia y seguridad nacional.

Tratar datos de personas de alto riesgo involucra que la base de datos contiene nombres de figuras públicas que pueden ser reconocidas a primera vista, así como información personal donde se infiera o se relacione explícitamente con su profesión, puesto o cargo en combinación con datos de identificación como nombre, domicilio, entre otros."

En concordancia con lo anterior, en el anexo del Documento de seguridad a la Evaluación de impacto, se hace referencia al inventario de datos personales que serán tratados a través del Sistema de Procesamiento, representados de la siguiente manera:

Inventario de Datos

Se elimina hoja completa, con fundamento en el artículo 110, fracción I de la LFTAIP;Décimo séptimo de los lineamientos Generales en materia de clasificación y desclasificación de la información,así como para la elaboración de versiones públicas, en relación con el artículo 5, fracción VI de la Ley de Seguridad Nacional; 47, Bis 4 de la Ley de Aviación Civil, 46 y 47 de la Ley de Aeropuertos y 152 del Reglamento de Aeropuertos.

Se elimina hoja completa, con fundamento en el artículo 110, fracción I de la LFTAIP;Décimo séptimo de los lineamientos Generales en materia de clasificación y desclasificación de la información,así como para la elaboración de versiones públicas, en relación con el artículo 5, fracción VI de la Ley de Seguridad Nacional; 47, Bis 4 de la Ley de Aviación Civil, 46 y 47 de la Ley de Aeropuertos y 152 del Reglamento de Aeropuertos.

Se elimina hoja completa, con fundamento en el artículo 110, fracción I de la LFTAIP;Décimo séptimo de los lineamientos Generales en materia de clasificación y desclasificación de la información,así como para la elaboración de versiones públicas, en relación con el artículo 5, fracción VI de la Ley de Seguridad Nacional; 47, Bis 4 de la Ley de Aviación Civil, 46 y 47 de la Ley de Aeropuertos y 152 del Reglamento de Aeropuertos.

Número de Asiento	Número de Asiento	Número de Asiento	X	X
Número de Secuencia	Número de Secuencia	Número de Secuencia	X	X
Estatus del Pasajero	Estatus del Pasajero	Estatus del Pasajero	X	X
Número Serial del Documento	Número Serial del Documento	Número Serial del Documento	X	X
Leg Order	Leg Order	Leg Order	X	X

IV.II. Información obtenida a través de fuentes de acceso público:

Ahora bien, atendiendo a la naturaleza y alcance del dictamen como documento orientador, no vinculante, a efecto de justificar y fortalecer las consideraciones de la presente con relación al análisis y clarificación de aspectos sobre los cuales hacía falta información, fue necesario realizar una consulta de elementos obtenidos de diferentes fuentes de acceso público sobre las empresas involucradas en el tratamiento de datos biométricos, es decir, Vision-Box, Apollocom y Amadeus, a saber:

Vision-Box. De la búsqueda en la página de internet oficial de la empresa[20], se identificó lo siguiente:

- Es una empresa de tecnología multinacional con sede en Lisboa, Portugal, dedicada a mejorar la calidad, la comodidad, la eficiencia y la seguridad en los servicios gubernamentales, los viajes, el control fronterizo y todas las instalaciones inteligentes. Lo hace a través del diseño, el desarrollo y la implementación superiores de soluciones y servicios de gestión de identidad digital integrados y centrados en el usuario **basados en tokens biométricos confiables**.
- Es un socio líder de los aeropuertos, aerolíneas, gobiernos y entidades privadas más prestigiosas con desafíos críticos de seguridad e identificación, ayudándolos a optimizar la identificación y el flujo de viajeros, estableciendo **procesos confiables de registro, verificación y autenticación de identidad biométrica, y permitiendo transacciones de datos multidireccionales para transformar la información sin procesar en inteligencia comercial procesable**.
- Dentro de sus soluciones se encuentra **VB Orquesta**, que es una plataforma de toma de decisiones y gestión centralizada 4.0 de múltiples partes interesadas de Vision-Box, que

[20] Vision-box, disponible en el vínculo electrónico: https://www.vision-box.com/ consultado por última vez el 28/02/2023.

conecta toda la seguridad virtual y física y la infraestructura de datos en tiempo real. Al **unir el flujo de información entre los puntos biométricos y los flujos de datos detallados de múltiples fuentes**, la suite de orquestación permite una poderosa estructura de información para la toma de decisiones. Esa estructura está orientada a analizar y descifrar el flujo estructural, la capacidad y los problemas de seguridad de los viajeros, así como a desarrollar relaciones cercanas con las partes interesadas a través de un compromiso colaborativo y personalizado.

- VB Orquesta se basa en los **principios de privacidad por diseño**, lo que garantiza una distribución de información segmentada confiable, la integridad de los datos y la seguridad y privacidad de los datos personales. Esto es posible utilizando una **estructura de libro mayor distribuida híbrida: vb trustchain™,** la arquitectura de cadena de bloques de Vision-Box™, basada en 16 años de gestión de identidades en un mundo digital.

Apollocom. De la búsqueda en la página de internet oficial de la empresa[21], se identificó lo siguiente:

- Es una empresa mexicana con 10 años de experiencia en el mercado nacional y reconocimiento a nivel internacional, que diseña e implementa soluciones en el ámbito de Telecomunicaciones, Automatización y Control, Capacidades MAC, Telemetría y Ciberseguridad Industrial, así como Servicios de Mantenimiento y Administrados, enfocados principalmente a la industria de Energía, Petróleo y Gas.
- Entre las soluciones previstas por Apollo, se encuentran: Telecomunicaciones, Automatización y Control, Capacidades MAC, Telemetría y Ciberseguridad Industrial.
- En cuanto a la contribución de Apollo al AIFA, se incluyen: **Puertas biométricas para la verificación automática de documentos, Abordaje automático Self-Boarding Gate, Registro biométrico en mostradores, Aplicación móvil desarrollada por Apollocom**, que incluye un mapa táctil responsivo a los gestos del teléfono celular.

Amadeus. De la búsqueda en la página de internet oficial de la empresa[22], se identificó lo siguiente:

- Es una empresa de tecnología de viajes con sede en Madrid, España, con soluciones críticas que ayudan a las **aerolíneas y aeropuertos**, hoteles y ferrocarriles, motores de búsqueda, agencias de viajes, operadores turísticos y otros actores de viajes a ejecutar sus operaciones y mejorar la experiencia de viaje.
- Respecto a las soluciones para aeropuertos, su tecnología aeroportuaria brinda la agilidad y adaptabilidad para responder a situaciones cambiantes. Con vuelos, pasajeros y equipaje para

[21] Apollocom, disponible en el vínculo electrónico: https://www.apollocom.com.mx/ consultado por última vez el 28/02/2023.
[22] Amadeus, disponible en el vínculo electrónico: https://amadeus.com/es/tema/servicios-en-la-nube consultado por última vez el 28/02/2023.

administrar, tiene una visibilidad clara de cada actividad de respuesta y toma decisiones informadas, gracias a la información en tiempo real compartida entre los socios y sistemas del aeropuerto.

- En particular, para aeropuertos se ha desarrollado una **solución biométrica** totalmente integrada para que la experiencia del pasajero puede automatizarse utilizando la biometría. Las soluciones de Amadeus ofrecen a los aeropuertos el software y hardware que necesitan en varios puntos de contacto con **dispositivos biométricos avanzados de captura de imágenes integrados en quioscos, unidades Auto Bag Drop (ABD) o suministrados como Smart Biopods en otros puntos de contacto como puertas de embarque o preseguridad**.
- En relación con sus **servicios de cómputo en la nube**, 2014 lanzaron Amadeus Cloud Services (ACS), una plataforma de aplicaciones de próxima generación, respaldada por un proyecto de código abierto que han desarrollado con la colaboración de RedHat en OpenShift Enterprise. **Amadeus Cloud Services** es una combinación de software, herramientas y prácticas, que proporciona un marco potente y flexible para la implementación masiva y la **distribución de operaciones de tráfico de datos y transacciones a gran escala**. Su software en la nube depende de un sistema de distribución global (GDS) y consigue que hacer frente a la demanda sea un proceso ininterrumpido y más rápido.

Dicha información se retoma a manera de estricta referencia para el análisis que se realiza en el apartado correspondiente del presente documento sobre cómputo en la nube.

V. Marco normativo aplicable a las evaluaciones de impacto en la protección de datos personales.

Los artículos 3, fracción XVI, 74, 75, 76, 77 y 78 de la Ley General, los artículos 1, 6, 7, 8, 9, 10, 14, 23, 27, 28, 29 y 30 de las Disposiciones administrativas, las cuales disponen que la Ley General tiene por objeto establecer las bases, principios y procedimientos para garantizar el derecho que tiene toda persona a la protección de sus datos personales en posesión de cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos y fideicomisos y fondos públicos en los tres órdenes de gobierno, destacando que dicho ordenamiento resulta directamente aplicable en el ámbito federal.

Específicamente, una evaluación de impacto en la protección de datos personales es un documento mediante el cual cualquier responsable que pretenda poner en operación o modificar políticas públicas, programas, sistemas o plataformas informáticas, aplicaciones electrónicas o

cualquier otra tecnología que implique un tratamiento intensivo o relevante de datos personales, valora los impactos reales de dicho tratamiento de datos personales a efecto de identificar y mitigar posibles riesgos relacionados con el cumplimiento de los principios, deberes y derechos previstos en la normativa aplicable.

Ahora bien, el responsable estará en presencia de un tratamiento intensivo o relevante de datos personales cuando concurran las siguientes condiciones:

- Existan riesgos inherentes a los datos personales a tratar.
- Se traten datos personales sensibles a los que se refiere el artículo 3, fracción X de la Ley General.
- Se efectúen o pretendan efectuar transferencias de datos personales a las que se refiere el artículo 3, fracción XXXII de la Ley General.

Asimismo, el responsable estará en presencia de tratamientos intensivos o relevantes de datos personales específicos cuando pretenda realizar alguna de las siguientes acciones:

- Cambiar la o las finalidades que justificaron el origen de determinado tratamiento de datos personales, de tal manera que pudiera presentarse una incompatibilidad entre las finalidades de origen con las nuevas finalidades, al ser estas últimas más intrusivas para los titulares.
- Evaluar, monitorear, predecir, describir, clasificar o categorizar la conducta o aspectos análogos de los titulares, a través de la elaboración de perfiles determinados para cualquier finalidad, destinados a producir efectos jurídicos que los vinculen o afecten de manera significativa, especialmente, cuando a partir de dicho tratamiento se establezcan o pudieran establecerse diferencias de trato o un trato discriminatorio económico, social, político, racial, sexual o de cualquier otro tipo que pudiera afectar la dignidad o integridad personal de los titulares.
- Tratar datos personales de grupos vulnerables atendiendo, de manera enunciativa más no limitativa, a su edad; género; origen étnico o racial; estado de salud; preferencia sexual; nivel de instrucción y condición socioeconómica.
- Crear bases de datos respecto de un número elevado de titulares de tal manera que se produzca una acumulación no intencional de una gran cantidad de datos personales respecto de los mismos.
- Incluir o agregar nuevas categorías de datos personales a las bases de datos ya existentes y en posesión del responsable, de tal forma que, en caso de presentarse una vulneración a la seguridad pudiera derivarse una afectación a la esfera personal de los titulares.
- Realizar un tratamiento frecuente y continúo de grandes volúmenes de datos personales, o bien, llevar a cabo cruces de información con múltiples sistemas o plataformas informáticas.
- Utilizar tecnologías con sistemas de vigilancia; aeronaves o aparatos no tripulados; minería de datos; biometría; Internet de las cosas; geolocalización; técnicas analíticas; radiofrecuencia

o cualquier otra que pueda desarrollarse en el futuro y que implique un tratamiento de datos personales a gran escala.

- Permitir el acceso de terceros a una gran cantidad de datos personales que anteriormente no tenían acceso, ya sea, entregándolos, recibiéndolos y/o poniéndolos a su disposición en cualquier forma.
- Realizar transferencias internacionales de datos personales a países que no cuenten en su derecho interno con garantías suficientes y equivalentes para asegurar la debida protección de los datos personales, conforme al sistema jurídico mexicano en la materia.
- Revertir la disociación de datos personales para la consecución de finalidades determinadas, especialmente si éstas son de carácter intrusivo o invasivo al titular, entre otros.
- Tratar datos personales sensibles con la finalidad de efectuar un tratamiento sistemático y masivo de los mismos.
- Realizar una evaluación sistemática y exhaustiva de aspectos propios de las personas físicas que se base en un tratamiento automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para éstas o que les afecten significativamente de modo similar.
- Realizar un tratamiento a gran escala de datos personales sensibles o datos personales relativos a condenas e infracciones penales.
- La observación sistemática a gran escala de una zona de acceso público.

Es por ello, que, cuando el responsable pretenda poner en operación o modificar políticas públicas, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que, a su juicio y de conformidad con la Ley General y las Disposiciones administrativas, impliquen un tratamiento intensivo o relevante de datos personales está obligado a presentar una evaluación de impacto en la protección de datos personales ante el Instituto, al menos, con treinta días hábiles de anterioridad a la fecha en que se pretenda poner en operación o modificar la política pública, sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología.

Una vez presentada la evaluación de impacto en la protección de datos personales conforme a lo anteriormente descrito, el Instituto está obligado a valorar la misma tomando en consideración lo siguiente:

- Los objetivos generales y específicos que persigue la política pública, programa, sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología que implique un tratamiento intensivo o relevante de datos personales.
- Las razones o motivos que justifican la puesta en operación o modificación de la política pública, programa, sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología que implique un tratamiento intensivo o relevante de datos personales, en función de las atribuciones o facultades del responsable que la normatividad aplicable le confiera.

- Las categorías de titulares, distinguiendo aquéllos que pertenezcan a grupos vulnerables en función de su edad; género; origen étnico o racial; estado de salud; preferencia sexual; nivel de instrucción y condición socioeconómica.
- Los datos personales tratados y su volumen.
- Las finalidades del tratamiento intensivo o relevante de datos personales.
- Las transferencias, nacionales o internacionales, de datos personales que, en su caso, pretendan efectuarse con la puesta en operación o modificación de la política pública, programa, sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología que implique un tratamiento intensivo o relevante de datos personales.
- La tecnología utilizada para efectuar el tratamiento intensivo o relevante de datos personales.
- Las medidas de seguridad de carácter administrativo, físico y técnico que se pretenden adoptar.
- Los posibles riesgos y amenazas, así como el daño o consecuencias que pudieran producirse o presentarse si llegasen a materializarse con la puesta en operación o modificación de la política pública, programa, sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología que implique un tratamiento intensivo o relevante de datos personales.
- Las medidas y controles concretos que el responsable adoptará para eliminar, mitigar, transferir o retener los riesgos identificados.
- Los mecanismos o procedimientos que adoptará el responsable para que la política pública, programa, sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología que implique un tratamiento intensivo o relevante de datos personales cumpla, desde el diseño y por defecto, con las obligaciones previstas en la Ley General y demás disposiciones aplicables.
- La opinión técnica del oficial de protección de datos personales respecto del tratamiento intensivo o relevante de datos personales que implique la política pública, programa, sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología, en su caso.
- Cualquier otra información que considere pertinente atendiendo a las circunstancias del caso en particular.

Para tal efecto, el Instituto está obligado a emitir un dictamen, dentro de los treinta días hábiles posteriores al día siguiente de la presentación de la evaluación de impacto en la protección de datos personales, determinando que:

- La política pública, programa, sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología que implique un tratamiento intensivo o relevante de datos personales cumple con lo dispuesto en la Ley General y demás disposiciones aplicables, y, por lo tanto, no será necesario emitir recomendaciones no vinculantes al respecto, o
- La política pública, programa, sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología que implique un tratamiento intensivo o relevante de datos

personales no cumple con lo dispuesto en la Ley General y demás normatividad aplicable, y, por lo tanto, será necesario emitir recomendaciones no vinculantes al respecto.

Cabe señalar, que el dictamen emitido por el Instituto no tendrá el efecto de impedir la puesta en operación o modificación de la política pública, programa, sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología que implique el tratamiento intensivo o relevante de datos personales en cuestión, como tampoco validar el presunto cumplimiento de las obligaciones previstas en la Ley General y demás disposiciones aplicables en perjuicio de las atribuciones conferidas al Instituto. Lo anterior, en virtud de que el objeto de este tipo de evaluaciones es orientar a los responsables sobre el fortalecimiento y mejor cumplimiento de las obligaciones en la materia mediante la emisión de recomendaciones no vinculantes.

VI. Análisis del tratamiento de datos personales que conllevará el Sistema de Procesamiento de Pasajeros del AIFA

Establecido el marco de contexto de la procedencia y tramitación de las Evaluaciones de impacto en la protección de datos personales, es posible advertir que, en términos de lo dispuesto por los artículos 3, fracción XVI, 74, 75 y 76 de la Ley General, 120 de los Lineamientos generales, y, 8 y 9 de las Disposiciones administrativas, la obligación de elaboración y presentación de dicho documento se genera a partir de los siguientes supuestos:

- Puesta en operación o modificación, es decir, la implementación o algún ajuste de un supuesto particular.
- Políticas públicas, programas, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología.
- Implique el tratamiento intensivo o relevante de datos personales; de carácter general, particular, o ambos.

- En este sentido, en la evaluación de impacto se señala que, para la implementación del Sistema de Procesamiento, el AIFA tiene entre sus facultades la de asegurar que los aeródromos civiles cuenten con la infraestructura, instalaciones, equipo, señalización, módulo de primeros auxilios y emergencias médicas, servicios y sistemas de organización, adecuados y suficientes para que la operación y atención al usuario se lleve a cabo sobre bases de seguridad, eficiencia y calidad. Por lo cual, el AIFA desarrolló el Sistema de Procesamiento, en ejercicio de las facultades previstas en los artículos 47 Bis 4 de la Ley de Aviación Civil[23]:

[23] Disponible en el vínculo electrónico siguiente: https://www.diputados.gob.mx/LeyesBiblio/pdf/25_200521.pdf; enlace consultado por última vez el 28/02/2023.

46 y 47 de la Ley de Aeropuertos[24]; 152, fracciones I, II, III y V del Reglamento de la Ley de Aeropuertos; y Anexo 17 al Convenio sobre Aviación Civil Internacional, Seguridad, Protección de la aviación civil internacional contra los actos de interferencia ilícita.

En este sentido, de conformidad con lo señalado en la evaluación de impacto presentada por el AIFA, se observa que el Sistema de Procesamiento fue implementado para la *"Adquisición, Suministro, Instalación, Comisionamiento y Puesta en Operación de Sistemas de Seguridad de la Aviación, Operación Aeroportuaria, Procesamiento del Pasajero, Infraestructuras de Telecomunicaciones, Ciberseguridad y Soporte al Pasajero, para la Ciudad Aeroportuaria (AIFA)"* y su plan de trabajo proyectado para la implementación de este sistema."

En esta tesitura, es dable advertir que, el Sistema de Procesamiento hará posible la realización de un procesamiento automatizado de pasajeros a través de su registro o enrolamiento en el que se recopilarán y validarán sus datos personales y de vuelo, el cual podrá llevarse a cabo por medio del procedimiento no biométrico mediante la exhibición del pase de abordar o, bien, mediante el procedimiento biométrico, realizado mediante el reconocimiento facial y la consecuente generación del PDE.

Bajo este tenor, se precisa que, conforme al desahogo de requerimiento de información adicional presentado por el AIFA, se hace referencia al concepto de sistema definiéndolo como el *"Dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, cuya función, o la de alguno de sus elementos, sea el tratamiento automatizado de datos en ejecución de un programa."* Por ende, de conformidad con lo señalado, se considera al Sistema de Procesamiento como un sistema informático, cuya interoperabilidad se integra por los sistemas CUPPS/Vdesk, CUSS/E-gate así como de la Aplicación Móvil del AIFA, mismos que involucran el tratamiento de datos personales y, que a su vez, se integran por determinada infraestructura, sistemas o plataformas.

En esta consonancia, como ya fue advertido, los procesos, fases o actividades operativas del Sistema de Procesamiento que involucren el tratamiento de datos personales, se pueden realizar por medio de tres vías consistentes en: la aplicación móvil del AIFA, quisco de documentación (CUSS) (Modo Auto-Servicio) y mostrador de documentación convencional (CUPPS/V-desk) (Modo Asistido); información que, para su fácil su identificación, se representa de manera gráfica de la forma siguiente:

[24] Disponible en el vínculo electrónico siguiente: https://www.diputados.gob.mx/LeyesBiblio/pdf/15_200521.pdf; enlace consultado por última vez el 28/02/2023.

Fase de Enrolamiento	Fase de Verificación (Pre-seguridad)	Fase de Verificación (Abordaje)
Vía la aplicación móvil (Modo Auto-Servicio)	Vía E-Gates de Pre-seguridad	Vía E-Gates de abordaje
Vía el quiosco de documentación (CUSS) (Modo Auto-Servicio)		
Vía el mostrador de documentación convencional (CUPPS/V-desk) (Modo Asistido)		

De esta manera, se advierte que el Sistema de Procesamiento es un sistema informático de control que será implementado por primera vez por el AIFA con el objetivo, de entre otros, de optimizar el procesamiento de pasajeros, agilizando los procesos de pre-seguridad y abordaje, generar eficiencias operativas para el aeropuerto, las aerolíneas y los operadores aeroportuarios, creando una mejor experiencia para el pasajero.

En esta tesitura, de conformidad con lo dispuesto por los artículos 74 de la Ley General, 120 de los Lineamientos generales, y 10 de las Disposiciones administrativas, el responsable que pretenda poner en operación o modificar una política pública, programa, sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología que, a su juicio, implique un tratamiento intensivo o relevante de datos personales deberá elaborar y presentar ante el Instituto o los organismos garantes una evaluación de impacto en la protección de datos personales de conformidad con los citados ordenamientos.

Por lo anterior y considerando a todo sistema informático como el conjunto de partes identificadas como dispositivos esencialmente electrónicos (*hardware*) programas (*software*) y recursos humanos (*humanware*) que funcionan relacionándose entre sí; la implementación del Sistema de Procesamiento pudiera constituir la puesta en operación de un sistema implementado por el AIFA para automatizar el proceso de enrolamiento y verificación de identidad de pasajeros a través del tratamiento de datos personales, por medio de procesos biométricos y no biométricos, mediante la interacción de sistemas, plataformas y participación del personal del aeropuerto en mostradores, que hacen posible el intercambio de información a través de su operación; encuadrando en el supuesto previsto por artículos 74 de la Ley General, 120 de los Lineamientos generales, y 10 de las Disposiciones administrativas.

De esta manera, es dable confirmar que el desarrollo del Sistema de Procesamiento actualiza por sí misma dos de las condiciones para estar en la obligación de elaborar y presentar una evaluación de impacto establecida en los artículos 74 de la Ley General, 120 de los Lineamientos generales; y 10 de las Disposiciones administrativas; en virtud de que, en el ejercicio de sus atribuciones, el AIFA pretende implementar el Sistema de Procesamiento, es decir, la puesta en operación de un sistema. Una vez precisado lo anterior, es importante analizar si los supuestos anteriores implican un tratamiento relevante o intensivo de datos personales, por lo cual se realizan una serie de consideraciones.

Atendiendo a los supuestos previstos por los artículos 75 y 76 de la Ley General y 8 y 9 de las Disposiciones administrativas, se advierte que, en la elaboración y presentación de una evaluación de impacto, se debe considerar en el análisis realizado, tanto las hipótesis que constituyen un tratamiento relevante o intensivo de carácter general, como los diversos tratamientos relevantes o intensivos de carácter particular, a fin de desarrollar los elementos a que hace referencia el artículo 14 de las Disposiciones administrativas, en congruencia con el cumplimiento de criterios relativos a la observancia de principios, deberes y derechos previstos por la Ley General y los Lineamientos generales.

En ese sentido, el objeto del presente Dictamen se encuentra relacionado con el análisis de los supuestos de tratamiento relevante o intensivo de carácter general y/o particular, para lo cual, en lo que hace al primer supuesto, es decir, respecto al tratamiento relevante o intensivo de carácter general, los artículos 75 de la Ley General y 8 de las Disposiciones administrativas establecen los supuestos que deben concurrir para considerar a un tratamiento de datos personales con dicha connotación, a saber:

- Cuando existan riesgos inherentes a los datos personales a tratar, entendidos como el valor potencial cuantitativo o cualitativo que pudieran tener éstos para una tercera persona no autorizada para su posesión o uso en función de la sensibilidad de los datos personales; las categorías de titulares; el volumen total de los datos personales tratados; la cantidad de datos personales que se tratan por cada titular; la intensidad o frecuencia del tratamiento, o bien, la realización de cruces de datos personales con múltiples sistemas o plataformas informáticas.
- Se traten datos personales sensibles que refieran a la esfera más íntima de su titular o cuya utilización indebida pueda dar origen a discriminación o conllevar un grave riesgo 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.

- Se efectúen o pretendan efectuar transferencias de datos personales, entendidas como cualquier comunicación de datos personales, dentro o fuera del territorio mexicano, realizada a persona distinta del titular, responsable o encargado, considerando con especial énfasis, de manera enunciativa más no limitativa, las finalidades que motivan éstas y su periodicidad prevista; las categorías de titulares; la categoría y sensibilidad de los datos personales transferidos; el carácter nacional y/o internacional de los destinatarios o terceros receptores y la tecnología utilizada para la realización de éstas.

En primer punto es importante analizar el tratamiento de datos personales que se lleve cabo a partir de la puesta en operación del Sistema de Procesamiento y determinar los supuestos normativos que se cumplen respecto a si se trata de un tratamiento intensivo o relevante ya sea de carácter general y/o particular.

Una vez precisado lo anterior, cabe traer a colación lo establecido en los artículos 3, fracción IX de la Ley General y 4 de los Lineamientos generales definen como **dato personal** a cualquier información concerniente a una persona física identificada o identificable, la cual puede estar expresada en forma numérica, alfabética, gráfica, alfanumérica, fotográfica, acústica o de cualquier otro tipo. Se considera que una persona física es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información.

En este tenor, cualquier información concerniente a una persona física que la identifica o la haga identificable, expresada en forma numérica, gráfica, fotográfica, alfabética, alfanumérica, acústica o de cualquier otro tipo, tiene la connotación de dato personal.

Por su parte, los artículos 3, fracción IX de la Ley General y 4 de los Lineamientos generales definen los parámetros objetivos para definir un dato personal:

- Cualquier información, por lo que, los datos personales pueden estar expresados en forma numérica, alfabética, gráfica, alfanumérica, fotográfica, acústica o de cualquier otro tipo.
- Concerniente a una persona física, concepto normativo en el marco del derecho civil aplicable al ámbito de aplicación.
- Identificada o identificable, considerando que una persona física es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información.

Así, con la finalidad de identificar la información que es susceptible de considerarse como un dato personal, se considera pertinente llevar a cabo un análisis de los elementos contenidos en dicho concepto, el cual es relativo a *"cualquier información concerniente a una persona física identificada o identificable"*.

En este sentido, el primer componente de la definición relativo a *"cualquier información"*, obliga a hacer una interpretación amplia, independientemente de la naturaleza o del contenido de la información y del soporte técnico en que se presente. Eso significa que tanto la información objetiva, por ejemplo, la presencia de determinada sustancia en la sangre, como la subjetiva de una persona física, por ejemplo, la relacionada con opiniones, cualquiera que sea su amplitud y con independencia del soporte técnico que la contenga puede ser considerada como dato personal.

El segundo componente *"concerniente"* es crucial en la determinación del alcance sustantivo del concepto, especialmente en relación con objetos y nuevas tecnologías. En este sentido, este segundo componente se materializa a través de la existencia de un elemento de contenido, finalidad o resultado, los cuales deben de considerarse como condiciones alternativas y no acumulativas:

- Contenido: se actualiza cuando la información se refiere o versa sobre una persona física, por ejemplo, los resultados de análisis médicos se refieren claramente a un paciente.
- Finalidad: se actualiza cuando los datos personales se utilizan o es probable que se utilicen, teniendo en cuanta todas las circunstancias que rodean el caso concreto, con la finalidad de evaluar, tratar de manera o influir en la situación o el comportamiento de una persona física.
- Resultado: se refiere a que el uso de cierta información repercuta en los derechos e intereses de determinada persona física. Así, basta con que la persona física pueda ser tratada de forma diferente por otras personas como consecuencia del tratamiento de sus datos personales.

El tercer componente *"persona física"* se centra en el requisito de que lo datos personales se refieran a seres humanos, así como el componente normativo contenido en las disposiciones en materia civil.

El cuarto componente *"identificada o identificable"* implica las condiciones que deben de darse para poder considerar a una persona como identificable, especialmente en los medios que pueden ser razonablemente utilizados para identificar a esta. Así, la identificación de una persona física implica la existencia de uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social que la distingan dentro de un grupo de personas.

A partir de lo anterior, con base en lo manifestado en la evaluación de impacto, respuesta al requerimiento de información adicional y anexos, se advirtió que los datos personales que serán objeto de tratamiento en el marco de la implementación del Sistema de Procesamiento son los siguientes:

- **Quioscos de documentación (CUSS)**
  - ❖ **Datos del quiosco del AIFA**
    - o Id Cámara

- Nombre del dispositivo
- Tipo de dispositivo
- Nombre del aeropuerto
- Numero de Terminal
- Código de aerolínea
- Vendedor
- Horario
- Datos del documento del pasajero (Pasaporte electrónico)
- Nombre completo
- Fecha de nacimiento
- Tipo de documento
- Número de documento
- País de emisión de documento
- Fecha de expiración del documento
- País de Nacionalidad
- Género

❖ **Datos del Pase de Abordar**

- Tipo de Código de Barra
- Formato de Código
- Indicador de Ticket Electrónico
- RAW
- Nombre del Pasajero
- Código PNR
- Aeropuerto de Origen
- Aeropuerto de Destino
- Código del Carrier
- Número de Vuelo
- Fecha del Vuelo
- Código de Compartimiento
- Número de Asiento
- Número de Secuencia
- Estatus del Pasajero
- Número Serial del Documento
- Leg Order

- **Mostradores de documentación (Vdesk)**
  - ❖ **Datos del mostrador del AIFA**
    - Nombre del dispositivo (VDESK)

- Tipo de Dispositivo
- Nombre del aeropuerto
- Número de Terminal
- Código de Aerolínea
- Vendedor
- Horario

❖ **Datos del documento del pasajero (INE)**

- Nombre completo
- Numero de Documento
- País de Nacionalidad
- Fecha de Validez
- Genero

❖ **Datos del documento del pasajero (Pasaporte no electrónico)**

- Nombre completo
- Numero de documento
- País de emisión
- Fecha de Validez del documento
- Fecha de nacimiento.
- Nacionalidad
- Genero

❖ Datos del documento del pasajero (Pasaporte electrónico)

- Numero de pasaporte
- Nombre completo
- Fecha de nacimiento
- País de emisión
- Fecha de validez del documento
- Nacionalidad
- Genero
- Biometría facial
- Biometría facial (vectores)

❖ **Datos del Pase de Abordar**

- Tipo de Código de Barra
- Formato de Código
- Indicador de Ticket Electrónico
- RAW
- Nombre del Pasajero
- Código PNR
- Aeropuerto de Origen

- Aeropuerto de Destino
- Código del Carrier
- Número de Vuelo
- Fecha del Vuelo
- Código de Compartimiento
- Número de Asiento
- Número de Secuencia
- Estatus del Pasajero
- Número Serial del Documento
- Leg Order

- **Aplicación móvil AIFA**
  - **Datos del documento del pasajero (Pasaporte Electrónico)**
  - Nombre completo
  - Fecha de nacimiento
  - País de Nacionalidad
  - Tipo de Documento
  - Número de documento
  - País de emisión de documento
  - Fecha de expiración del documento
  - Género
  - Foto del chip del pasaporte
  - Foto capturada por el dispositivo móvil (vector)
  - **Datos del Pase de Abordar**
  - Tipo de Código de Barra
  - Formato de Código
  - Indicador de Ticket Electrónico
  - RAW
  - Nombre del Pasajero
  - Código PNR
  - Aeropuerto de Origen
  - Aeropuerto de Destino
  - Código del Carrier
  - Número de Vuelo
  - Fecha del Vuelo
  - Código de Compartimiento
  - Número de Asiento
  - Número de Secuencia

- Estatus del Pasajero
- Número Serial del Documento
- Leg Order

De lo anterior, es posible advertir que la información antes referida se constituye como datos personales al actualizar el supuesto normativo establecido en el artículo 3, fracción IX, de la Ley General, al constituir información concerniente a una persona física identificada o identificable toda vez que refiere a información de personas físicas en su carácter de pasajeros que utilizan el AIFA, que las identifica o las hace identificables.

Por su parte, los artículos 1 y 3, fracción XXVIII de la Ley General y 3 de los Lineamientos generales, disponen que cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos, del orden federal, adquiere el carácter de responsable cuando decide sobre determinado tratamiento de datos personales.

De esta manera, la característica principal del responsable del sector público es el poder de decisión que ostenta sobre determinado tratamiento de datos personales, poder que incluye la definición del alcance, contenido, medios, fines y demás cuestiones relacionadas con el tratamiento de datos personales que pretende efectuar, como podría ser, de manera enunciativa mas no limitativa:

- Las finalidades concretas que motivan el tratamiento de los datos personales y que estén relacionadas con las atribuciones que la normatividad aplicable le confiera.
- Los datos personales por tratar.
- Las categorías de titulares involucrados.
- Las comunicaciones de datos personales que, en su caso, se efectúen.
- La tecnología utilizada para llevar a cabo el tratamiento de los datos personales.

Por lo tanto, resulta importante señalar que, a consideración de esta unidad administrativa, la actividad que realiza el AIFA a través de la implementación del Sistema de Procesamiento, dirigido a automatizar el proceso de enrolamiento y verificación de identidad de los pasajeros, le atribuye el carácter de responsable en términos de los artículos 1, párrafos segundo y quinto, y 3, fracción XXVIII de la Ley General, al advertirse que lleva a cabo el tratamiento de datos personales.

Esto es así ya que, tomando en consideración que, en términos del artículo 3, fracción XXXIII de la Ley General, por tratamiento de datos personales se entiende 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, por lo que, de conformidad con antes mencionado, el AIFA, como Empresa de Participación Estatal Mayoritaria tiene por objeto, entre otros, llevar a cabo todas las acciones necesarias para administrar, operar, explotar y construir el Aeropuerto Internacional Felipe Ángeles, entre ellas, permitir el flujo ininterrumpido para el acceso de los pasajeros para pasar a los filtros de pre-seguridad y realizar el embarque a la aeronave de manera rápida y segura, por lo que es quien decide la implementación del Sistema de Procesamiento como medio para el tratamiento de los datos personales, los sistemas de almacenamiento y los fines por los cuales se utilizan, de acuerdo a sus atribuciones.

Por tanto, el AIFA es responsable tanto de la implementación del Sistema de Procesamiento; así como de decidir y llevar a cabo todas las operaciones que involucra su funcionamiento y que son aplicadas a los datos personales, operaciones relativas a su obtención, su uso, registro, conservación, utilización, comunicación, almacenamiento, manejo, aprovechamiento y transferencia de los datos personales concernientes a la automatización del enrolamiento y verificación de identidad de los pasajeros a través del procedimiento biométrico y no biométrico.

Asimismo, es menester señalar que el AIFA, en términos del artículo 1, párrafos segundo y quinto de la Ley General, cumple con el supuesto de ser considerado como sujeto obligado, aunado a que se encuentra reconocido con tal carácter con la clave 07003 de la: "*Actualización del Padrón de Sujetos Obligados del Ámbito Federal, en términos de la Ley General de Transparencia y Acceso a la información Pública*"[25], el cual resulta aplicable en materia de protección de datos personales en términos del "*ACUERDO mediante el cual se aprueba que el padrón de sujetos obligados del ámbito federal, en términos de la Ley General de Transparencia y Acceso a la Información Pública y sus respectivas actualizaciones llevadas a cabo por la Secretaría de Acceso a la Información, se utilice como referencia directa del catálogo de sujetos obligados en el ámbito federal para efectos de lo dispuesto en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados*"[26], por lo tanto, le corresponde tratar los datos personales en su posesión conforme a las reglas previstas en la Ley General, los Lineamientos generales y demás normatividad que resulte en la materia, en su carácter de responsable federal.

En consideración a lo antes expuesto, se advierte que, al actualizarse la figura de tratamiento de datos personales, es procedente que esta unidad administrativa proceda a calificar, para efectos de la valoración de la evaluación de impacto, el carácter relevante o intensivo de carácter general y/o particular.

---

[25] Disponible en el siguiente vínculo electrónico: https://home.inai.org.mx/wp-content/documentos/Micrositios/Padron_Sujetos_Obligados.pdf última actualización de fecha 11 de enero de 2023, enlace consultado por última vez el 28/02/2023.

[26] Publicado en el DOF el 29 de agosto de 2019, disponible en el siguiente vínculo electrónico: http://www.dof.gob.mx/nota_detalle.php?codigo=5570690&fecha=29/08/2019, enlace consultado por última vez el 28/02/2023.

Riesgos inherentes a los datos personales a tratar.

Una vez precisado lo anterior, con relación al primer requisito para considerar que cierto tratamiento de datos personales tiene la connotación de relevante o intensivo en términos de los artículos 75, fracción I, de la Ley General y 8, fracción I de las Disposiciones administrativas, es decir, cuando existan riesgos inherentes a los datos personales, conviene señalar que en todo tratamiento de datos personales siempre existirán riesgos por el valor potencial cuantitativo o cualitativo que pudieran tener éstos para una tercera persona no autorizada para su posesión o uso en función de la sensibilidad de los datos personales; las categorías de titulares; el volumen total de los datos personales tratados; la cantidad de datos personales que se tratan por cada titular; la intensidad o frecuencia del tratamiento, o bien, la realización de cruces de datos personales con múltiples sistemas o plataformas informáticas.

Tan es así, que conforme a los artículos 31 y 32 de la Ley General y 55 y 60 de los Lineamientos generales el responsable está obligado a implementar y mantener medidas de seguridad de carácter físico, técnico y administrativo que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o uso, acceso o tratamiento no autorizado, considerando los riesgos inherentes y asociados a los datos personales.

Para lo cual, el responsable está obligado a llevar a cabo un análisis de riesgos de los datos personales tratados considerando los requerimientos regulatorios, códigos de conducta o mejores prácticas de un sector específico; el valor de los datos personales de acuerdo con su clasificación previamente definida y su ciclo de vida; el valor y exposición de los activos involucrados en el tratamiento de los datos personales; las consecuencias negativas para los titulares que pudieran derivar de una vulneración de seguridad ocurrida; la sensibilidad de los datos personales; el desarrollo tecnológico; las posibles consecuencias de una vulneración para los titulares; las trasferencias de datos personales que se realicen; el número de titulares; las vulneraciones previas ocurridas, entre otros factores.

Al respecto, en la evaluación de impacto, se señaló lo siguiente:

> *"[…]*
> *Los datos personales pueden clasificarse en cuatro categorías, de acuerdo a la criticidad de los mismos por nivel de riesgo inherente, conforme a la Metodología de Análisis de Riesgo BAA, en el ítem 2.1 Clasificación de Datos Personales*
> *[…]"*

En esta tesitura, cabe señalar que en anexo denominado "Análisis de Riesgos para Datos Personales", se refiere que, en la Clasificación de los Datos Personales, se deberá identificar los tipos de datos personales que se tratan, la sensibilidad de los mismos y el número de titulares para

determinar el valor del riesgo inherente de los datos para un tercero no autorizado. Así, se señala que los datos personales, pueden clasificarse en cuatro categorías, de acuerdo a la criticidad de los mismos clasificados en bajo, medio, alto y crítico.

En este contexto, se señala que, el nivel de riesgo por tipo de dato es igual al beneficio que representa la información para un atacante, y para calcularlo se requieren dos elementos principalmente:

- El nivel de riesgo inherente de cada tipo de dato que se trate (sensibilidad de los datos).
- Calcular el volumen de los titulares, cuantificando el número de personas de las que se traten datos personales.

Lo anterior, se representó de manera gráfica de la siguiente forma:

Tipo de Dato	Nivel de Riesgo Inherente
N/A	Crítico
• País de Nacionalidad • Género • Fotografía capturada por el Quiosco (vector) • Fotografía capturada por el V-Desk (vector) • Foto capturada por el dispositivo móvil (vector) • Foto del chip del pasaporte	Alto
• Número de documento • Aeropuerto de Origen • Aeropuerto de Destino	Medio
• Nombre del dispositivo • Tipo de Dispositivo • Nombre del aeropuerto • Número de Terminal • Código de Aerolínea • Vendedor • Horario • Id de la cámara • Nombre completo • Fecha de nacimiento • Tipo de Documento • País de emisión de documento • Fecha de expiración del documento (validez) • Tipo de Código de Barra • Formato de Código • Indicador de Ticket Electrónico • RAW • Nombre del Pasajero • Código PNR • Código del Carrier • Número de Vuelo • Fecha del Vuelo • Código de Compartimiento • Número de Asiento • Número de Secuencia • Estatus del Pasajero • Número Serial del Documento • Leg Order	Bajo

De igual forma se informó en dicho documental se señala que llevó a cabo el análisis de riesgos conforme al Metodología BAA (Beneficio, Accesibilidad y Anonimidad para el atacante).

En este sentido, se identificaron una serie de riesgos tecnológicos, físicos y administrativos, así como una ponderación cuantitativa y/o cualitativa de la probabilidad de que los riesgos identificados se materialicen.

De lo anterior, se advierte que la implementación de la PBI actualiza la primera condición para considerar a un tratamiento de datos personales con el carácter de intensivo o relevante de carácter general previsto en los artículos 75, fracción I de la Ley General y 8, fracción I de las Disposiciones administrativas, toda vez que, derivado del análisis de riesgos realizado por el AIFA se advirtió que existen riesgos inherentes a los datos personales a tratar en función del tipo de datos personales que se traten y del volumen de los titulares; situación que serán analizados particularmente en el apartado siguiente.

Datos personales sensibles

Asimismo, con relación al segundo requisito para considerar que cierto tratamiento de datos personales tiene la connotación de relevante o intensivo en términos de los artículos 75, fracción II de la Ley General y 8, fracción II de las Disposiciones administrativas, la cual implica que se traten datos personales sensibles, en primer término, resulta importante traer a colación lo referido en el artículo 3, fracción X de la Ley General, el cual a la letra señala lo siguiente:

> *"**Artículo 3.** Para los efectos de la presente Ley se entenderá por:*
> *[…]*
> ***X. 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;*
> *[…]"*

Por lo anterior, se puede determinar que un dato personal adquiere categoría de sensible en cualquiera de los siguientes supuestos:

a) Que se refieran a la esfera más íntima de su titular;
b) Que su utilización indebida pueda dar origen a discriminación;
c) Que su utilización indebida conlleve un riesgo grave para su titular;
d) Datos personales que puedan revelar aspectos como origen racial o étnico;
e) Datos personales que puedan revelar aspectos como estado de salud presente o futuro;

f) Datos personales que puedan revelar aspectos como información genética;
g) Datos personales que puedan revelar aspectos como creencias religiosas, filosóficas y morales;
h) Datos personales que puedan revelar aspectos como opiniones políticas; y/o,
i) Datos personales que puedan revelar aspectos como preferencia sexual.

Es de precisar que la Ley General, establece una lista enunciativa más no limitativa de este tipo de datos personales, lo cual no excluye que en atención del contexto y de las circunstancias particulares de cierto tratamiento, un dato personal pueda ser considerado como sensible partiendo de la premisa que éstos podrían afectar la esfera más íntima de su titular o cuya utilización indebida podría dar origen a discriminación o conllevar un grave riesgo para éste.

De esta manera, hacer referencia al tratamiento de datos personales sensibles implica una categoría especial de tratamiento que comprende diversos supuestos que en el ámbito de sujetos obligados son enunciativos, es decir, que no se limitan a los supuestos determinados de manera expresa en dicha disposición.

Ahora bien, por lo que hace a la Evaluación de impacto presentada por el AIFA, se refirió lo siguiente:

> *"En los Inventarios de Datos Personales se encuentra:*
> *1. La categoría de los Datos (sensibles o no sensibles) por sistema.*
> *Con fundamento En el Art. 3 de la Ley General De Protección De Datos Personales En Posesión De Sujetos Obligados refiere como datos sensible: 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.*
> *...*
> *Se consideró como datos sensibles la fotografía, vectores (fotografía), nacionalidad y género, debido a que podrían relacionarse con aspectos como origen, origen racial o étnico, y su utilización indebida podría dar origen a discriminación.*
> *[...]"*

Por su parte, en la respuesta al requerimiento de información adicional, se informó lo siguiente:

> *"[...]*
> *En este sentido, la utilización de biométricos, y datos como la fotografía en el pasaporte o en la credencial de elector y la nacionalidad, podrían en algunos casos, revelar aspectos como el origen racial y étnico, así como en algunos casos incluso las creencias religiosas. Por lo*

Se elimina hoja completa, con fundamento en el artículo 110, fracción I de la LFTAIP;Décimo séptimo de los lineamientos Generales en materia de clasificación y desclasificación de la información,así como para la elaboración de versiones públicas, en relación con el artículo 5, fracción VI de la Ley de Seguridad Nacional; 47, Bis 4 de la Ley de Aviación Civil, 46 y 47 de la Ley de Aeropuertos y 152 del Reglamento de Aeropuertos.

Se elimina hoja completa, con fundamento en el artículo 110, fracción I de la LFTAIP;Décimo séptimo de los lineamientos Generales en materia de clasificación y desclasificación de la información,así como para la elaboración de versiones públicas, en relación con el artículo 5, fracción VI de la Ley de Seguridad Nacional; 47, Bis 4 de la Ley de Aviación Civil, 46 y 47 de la Ley de Aeropuertos y 152 del Reglamento de Aeropuertos.

Se elimina hoja completa, con fundamento en el artículo 110, fracción I de la LFTAIP;Décimo séptimo de los lineamientos Generales en materia de clasificación y desclasificación de la información,así como para la elaboración de versiones públicas, en relación con el artículo 5, fracción VI de la Ley de Seguridad Nacional; 47, Bis 4 de la Ley de Aviación Civil, 46 y 47 de la Ley de Aeropuertos y 152 del Reglamento de Aeropuertos.

Conforme a lo anterior y con base en las manifestaciones realizadas, se cuenta con elementos para determinar que el tratamiento de datos personales que se efectuará en el marco de la implementación del Sistema de Procesamiento tiene carácter de tratamiento intensivo o relevante de carácter general, esto es, conforme a la hipótesis prevista en los artículos 75 de la Ley General y 8 de las Disposiciones administrativas. Esto es así ya que la determinación de un tratamiento intensivo o relevante de carácter general conlleva forzosamente el cumplimiento de tres condiciones:

1. La existencia de riesgos inherentes a los datos personales que serán tratados dado su impacto y posibilidad de que éstos ocurran.
2. Se tratan datos personales biométricos sensibles a los que se refiere el artículo 3, fracción X de la Ley General.
3. Se realiza una comunicación de datos personales actualizando la realización de transferencias a las que refiere el artículo 3, fracción XXXII de la Ley General.

De las cuales en el caso en concreto se actualizan cada una de ellas, es decir, la existencia de riesgos inherentes a los datos personales, el tratamiento de datos personales sensibles y la transferencia de datos personales.

Ahora bien, a fin de continuar con los supuestos para la existencia de tratamientos relevantes o intensivos, y con base en los elementos que se tienen a la vista para la emisión del presente dictamen, se señala que de acuerdo con los artículos 76 de la Ley General y 9 de las Disposiciones administrativas prevén, de manera enunciativa más no limitativa, una serie de tratamientos intensivos o relevantes de datos personales de manera particular, mismos que se actualizan cuando ocurra alguno de los siguientes supuestos:

- Cambiar la o las finalidades que justificaron el origen de determinado tratamiento de datos personales, de tal manera que pudiera presentarse una incompatibilidad entre las finalidades de origen con las nuevas finalidades, al ser estas últimas más intrusivas para los titulares.
- Evaluar, monitorear, predecir, describir, clasificar o categorizar la conducta o aspectos análogos de los titulares, a través de la elaboración de perfiles determinados para cualquier finalidad, destinados a producir efectos jurídicos que los vinculen o afecten de manera significativa, especialmente, cuando a partir de dicho tratamiento se establezcan o pudieran establecerse diferencias de trato o un trato discriminatorio económico, social, político, racial, sexual o de cualquier otro tipo que pudiera afectar la dignidad o integridad personal de los titulares.
- Tratar datos personales de grupos vulnerables atendiendo, de manera enunciativa más no limitativa, a su edad; género; origen étnico o racial; estado de salud; preferencia sexual; nivel de instrucción y condición socioeconómica.

- Crear bases de datos respecto de un número elevado de titulares de tal manera que se produzca una acumulación no intencional de una gran cantidad de datos personales respecto de estos.
- Incluir o agregar nuevas categorías de datos personales a las bases de datos ya existentes y en posesión del responsable, de tal forma que, en caso de presentarse una vulneración a la seguridad pudiera derivarse una afectación a la esfera personal de los titulares.
- Realizar un tratamiento frecuente y continuo de grandes volúmenes de datos personales, o bien, llevar a cabo cruces de información con múltiples sistemas o plataformas informáticas.
- Utilizar tecnologías con sistemas de vigilancia; aeronaves o aparatos no tripulados; minería de datos; biometría; Internet de las cosas; geolocalización; técnicas analíticas; radiofrecuencia o cualquier otra que pueda desarrollarse en el futuro y que implique un tratamiento de datos personales a gran escala.
- Realizar transferencias internacionales de datos personales a países que no cuenten en su derecho interno con garantías suficientes y equivalentes para asegurar la debida protección de los datos personales, conforme al sistema jurídico mexicano en la materia.
- Revertir la disociación de datos personales para la consecución de finalidades determinadas, especialmente si éstas son de carácter intrusivo o invasivo al titular, entre otros.
- Tratar datos personales sensibles con la finalidad de efectuar un tratamiento sistemático y masivo de los mismos.
- Realizar una evaluación sistemática y exhaustiva de aspectos propios de las personas físicas que se base en un tratamiento automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para éstas o que les afecten significativamente de modo similar.
- Realizar un tratamiento a gran escala de datos personales sensibles o datos personales relativos a condenas e infracciones penales.
- La observación sistemática a gran escala de una zona de acceso público.

Al respecto, en la evaluación de impacto el AIFA informó que le son aplicables las causales establecidas en el artículo 9, fracciones III y VI referentes a:

- Tratar datos personales de grupos vulnerables atendiendo, de manera enunciativa más no limitativa, a su edad; género; origen étnico o racial; estado de salud; preferencia sexual; nivel de instrucción y condición socioeconómica.
- Realizar un tratamiento frecuente y continuo de grandes volúmenes de datos personales, o bien, llevar a cabo cruces de información con múltiples sistemas o plataformas informáticas.

Respecto al supuesto señalado en la fracción III del numeral 9 de la Disposiciones Administrativas que prevé:

"III. Tratar datos personales de grupos vulnerables atendiendo, de manera enunciativa mas no limitativa, a su edad; género; origen étnico o racial; estado de salud; preferencia sexual; nivel de instrucción y condición socioeconómica;"

En este sentido, el AIFA informó en la evaluación de impacto respecto a los datos personales pertenecientes a grupos vulnerables, lo siguiente:

"V. Categorías de los titulares.
El sistema se definió y quedó configurado para no procesar biométricamente a pasajeros menores de edad. Para menores de edad se realizará el procedimiento tradicional (proceso no biométrico). Para el ingreso al área estéril, un agente de seguridad del AIFA realizará la verificación de su identidad. Para el proceso de abordaje, un agente de la aerolínea realizará la validación.
Todos los pasajeros mayores de edad que cuenten con su pase de abordar y documento de identificación oficial podrían realizar el registro biométrico, si se cuenta con su consentimiento.
El sistema no discrimina, porque no está configurado para clasificar o identificar a un pasajero ya sea por origen étnico o racial; género; estado de salud; preferencia sexual; nivel de instrucción; condición socioeconómica; ni limitaciones físicas."

[Énfasis añadido]

Por su parte, en el desahogo del requerimiento de información adicional, se manifestó:

"Sobre el particular, el artículo 3, fracción X, de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, refiere como datos personales los siguientes:
"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"
En este sentido, la utilización de biométricos, y ***datos como la fotografía en el pasaporte o en la credencial de elector y la nacionalidad, podrían en algunos casos, revelar aspectos como el origen racial y étnico, así como en algunos casos incluso las creencias religiosas****. Por lo anterior, se considera que el "Sistema de Procesamiento de Pasajeros" realizara tratamiento de datos personales sensibles.*
Asimismo, el artículo 9 de las Disposiciones Administrativas de Carácter General para la Elaboración, Presentación y Valoración de Evaluaciones de Impacto en la Protección de Datos Personales, cita en las fracciones III y VI, respectivamente:
"Tratar datos personales de grupos vulnerables atendiendo, de manera enunciativa mas no limitativa, a su edad; género; origen étnico o racial; estado de salud; preferencia sexual; nivel de instrucción y condición socioeconómica"
En el caso que nos ocupa, también del pasaporte, de la credencial de elector permiten acceso a la edad del pasajero

"Realizar un tratamiento frecuente y continúo de grandes volúmenes de datos personales, o bien, llevar a cabo cruces de información con múltiples sistemas o plataformas informáticas;"
Tal como se desprende de los documentos originales que se entregaron en los anexos de la EIPDP, entregada el 9 de enero del año en curso, son millones de personas las cuales tendrían acceso a los biométricos en caso de estar de acuerdo con las condiciones del aviso de privacidad; aunado al hecho de que existen cruces de información dentro del aplicativo del Sistema de Procesamiento de Pasajeros, a cargo del encargado en diversos procesos, trae consigo que las dos condiciones señaladas en las fracciones III y VI del artículo 9 de las Disposiciones se llevan a cabo, para mayor detalle se expresa lo siguiente: Se está en presencia de un tratamiento intensivo o relevante de datos personales de carácter general derivado del hecho de llevar a cabo cruces de información entre los sistemas ACUS y APV de AMADEUS y la plataforma Orchestra VB. Adicionalmente, se considera un tratamiento frecuente y continuo de grandes volúmenes de datos personales, debido al número de pasajeros de salida por
Tal como se señaló en el Inventario de Datos y el Documento de Seguridad, donde se encuentra especificado cuales son los datos sensibles tratados. Se aclara que no hay uso de los datos de estado de salud preferencia sexual; nivel instrucción y condición socioeconómica
[...]

[Énfasis añadido]

Por lo anterior, se advierte que diversos datos personales de los titulares recabados por medio del Sistema de Procesamiento permitirían determinar su situación de vulnerabilidad en función de su origen étnico o nacional, idioma o lengua, religión, edad, género, preferencia u orientación sexual, identidad de género, condición de discapacidad, así como cualesquiera otras circunstancias diferenciadoras que requiera de una atención especializada.

En este sentido, es importante precisar que, los datos personales objeto de tratamiento, especificados en el inventario presentado, refieren a datos personales obtenidos a través del proceso biométrico mediante los Quioscos de documentación (CUSS), Mostradores de documentación (Vdesk) y Aplicación móvil del AIFA.

En este sentido, cabe reiterar el artículo 5, fracción VI de la Ley General de Desarrollo Social[28], establece una definición sobre qué grupos son considerados vulnerables, conforme a lo siguiente:

*"**Artículo 5**. Para los efectos de esta Ley se entiende por:*
[...]
***VI.** Grupos sociales en situación de vulnerabilidad: Aquellos núcleos de población y personas que por diferentes factores o la combinación de ellos, enfrentan situaciones de riesgo o*

[28]Publicada en el DOF el 20 de enero de 2004, disponible para ser consultada en el vínculo electrónico siguiente: https://www.dof.gob.mx/nota_detalle.php?codigo=676752&fecha=20/01/2004; última reforma publicada en el DOF el 11 de mayo de 2022, disponible en el vínculo electrónico siguiente: https://dof.gob.mx/nota_detalle.php?codigo=5651685&fecha=11/05/2022#gsc.tab=0 , enlace consultado por última vez el 28/02/2023.

discriminación que les impiden alcanzar mejores niveles de vida y, por lo tanto, requieren de la atención e inversión del Gobierno para lograr su bienestar;
[...]"

Por su parte, el artículo 4, de la Ley de Asistencia Social[29] establece lo siguiente:
***"Artículo 3.-** Para los efectos de esta Ley, se entiende por asistencia social el conjunto de acciones tendientes a modificar y mejorar las circunstancias de carácter social que impiden el desarrollo integral del individuo, así como la protección física, mental y social de personas en estado de necesidad, indefensión desventaja física y mental, hasta lograr su incorporación a una vida plena y productiva.*

***Artículo 4.-** Tienen derecho a la asistencia social los individuos y familias que por sus condiciones físicas, mentales, jurídicas, económicas o sociales, requieran de servicios especializados para su protección y su plena integración al bienestar.*

Con base en lo anterior, son sujetos de la asistencia social, preferentemente:
I. Todas las niñas, niños y adolescentes, en especial aquellos que se encuentren en situación de riesgo o afectados [...]
[...]
II. Las mujeres: [...]
[...]
III. Indígenas migrantes, desplazados o en situación vulnerable;
IV. Migrantes;
V. Personas adultas mayores: [...]
[...]
VI. Personas con algún tipo de discapacidad o necesidades especiales;
VII. Dependientes de personas privadas de su libertad, de desaparecidos, de enfermos terminales, de alcohólicos o de fármaco dependientes
VIII. Víctimas de la comisión de delitos;
IX. Indigentes;
X. Alcohólicos y fármaco dependientes;
XI. Coadyuvar en asistencia a las personas afectadas por desastres naturales, y
XII. Los demás sujetos considerados en otras disposiciones jurídicas aplicables."

---

[29] Publicados en el DOF el 15 de abril de 2016; disponible en el vínculo electrónico siguiente: http://dof.gob.mx/nota_detalle.php?codigo=662330&fecha=02/09/2004, última reforma publicada en el DOF el 20 de mayo de 2021, disponible en el vínculo electrónico siguiente: http://dof.gob.mx/nota_detalle.php?codigo=5618885&fecha=20/05/2021 ; texto consolidado por la Cámara de Diputados del H. Congreso de la Unión en formato de documento portable, denominado como pdf por sus siglas en inglés, incorporando las diversas reformas de dicho ordenamiento jurídico en el sitio siguiente: http://www.diputados.gob.mx/LeyesBiblio/pdf/1_110321.pdf; enlaces consultados por última ocasión el 26/03/2021, http://www.diputados.gob.mx/LeyesBiblio/pdf/270_200521.pdf texto consolidado por la Cámara de Diputados del H. Congreso de la Unión en formato de documento portable, denominado como pdf por sus siglas en inglés, incorporando las diversas reformas de dicho ordenamiento jurídico en el sitio siguiente: http://www.diputados.gob.mx/LeyesBiblio/pdf/270_200521.pdf; enlaces consultados por última vez el 28/02/2023.

De las disposiciones antes citadas se desprende que, se entiende por grupos sociales en situación de vulnerabilidad o vulnerables como aquellos núcleos de personas que a raíz de diversos factores o la combinación de ellos enfrentan situaciones de riesgo o discriminación lo cual les impide mejores condiciones de vida y requieren atención del Gobierno.

En este sentido, entre los grupos sociales que requieren atención del gobierno a través de asistencia social, entendida como el conjunto de acciones tendientes a modificar y mejorar las circunstancias de carácter social que impidan el desarrollo integral del individuo, así como la protección física, mental y social de personas en estado de necesidad, indefensión desventaja física y mental, se encuentran todas las niñas, niños y adolescentes, mujeres y personas con algún tipo de discapacidad.

Aunado a lo anterior, el Consejo Nacional de Evaluación de la Política de Desarrollo Social, establece un listado enunciativo de grupos vulnerables históricamente discriminados a los jóvenes, niñas, niños y adolescentes, mujeres, adultos mayores, personas con discapacidad y la población indígena, así como los migrantes y los jornaleros agrícolas.[30]

Es preciso señalar lo establecido en los artículos 5 Ley General de los Derechos de Niñas, Niños y Adolescentes

> *"**Artículo 5.** Son niñas y niños los menores de doce años, y adolescentes las personas de entre doce años cumplidos y menos de dieciocho años de edad. Para efectos de los tratados internacionales y la mayoría de edad, son niños los menores de dieciocho años de edad.*

Asimismo, cabe traer a colación lo establecido por el Comité de los Derechos del Niño de la Organización de las Naciones Unidas en su Observación General Nº 13 (2011): Derecho del niño a no ser objeto de ninguna forma de violencia (CRC/C/GC/13)[31] en el que se indica que: "*A nivel universal se consideran vulnerables todos los niños hasta los 18 años de edad, porque no ha concluido aún su crecimiento y desarrollo neurológico, psicológico, social y físico. Los lactantes y los niños pequeños son los más vulnerables debido a la inmadurez de su cerebro, todavía en desarrollo, y a su completa dependencia de los adultos*".

Por su parte, la CoIDH, ha sostenido que: "*Las medidas especiales de protección que el Estado debe adoptar se basan en el hecho de que las niñas, niños y adolescentes se consideran más vulnerables a violaciones de derechos humanos, lo que además estará determinado por distintos*

---

[30] Información disponible en el siguiente vínculo electrónico: https://www.coneval.org.mx/Evaluacion/IEPSM/Documents/CPP_2021/Info_Vulnerables_COVID.pdf enlace consultado por última vez el 28/02/2023.

[31] Información disponible en el siguiente vínculo electrónico: https://www.bienestaryproteccioninfantil.es/imagenes/tablaContenidos03SubSec/G1142390.pdf, enlace consultado por última vez el 28/02/2023.

factores, como la edad, las condiciones particulares de cada uno, su grado de desarrollo y madurez, entre otros."[32]

Por lo anterior, es preciso advertir que las niñas y niños, son aquellas personas menores de 12 años y los adolescentes refieren a las personas de entre 12 años cumplidos y menos de 18 años de edad. Este tipo de grupo poblacional que integran las niñas, niños y adolescentes, de acuerdo con las disposiciones antes referidas del marco normativo mexicano, así como el internacional, se consideran vulnerables ya que enfrentan situaciones de riesgo, discriminación y violación a sus derechos humanos, en general o en contextos particulares, determinado por distintos factores, como lo es la edad, las condiciones particulares de cada uno, su grado de desarrollo y madurez toda vez que no ha concluido aún su crecimiento y desarrollo neurológico, psicológico, social y físico.

En este sentido, dentro de lo señalado en la evaluación de impacto, se advierte que, el Sistema de Procesamiento, se configuró para no procesar biométricamente a pasajeros menores de edad. Así, se señala que, para menores de edad, se realizará el procedimiento tradicional, es decir, el proceso no biométrico, refiriendo que, para el ingreso al área estéril, un agente de seguridad del AIFA realizará la verificación de su identidad y que, para el proceso de abordaje, un agente de la aerolínea realizará la validación. Una vez precisado lo anterior, no es posible apreciar mayor información al respecto, así como referencia alguna a adolescentes.

Por lo tanto, es posible advertir que, dentro del Sistema de Procesamiento, específicamente por lo que hace al proceso no biométrico, pueden encontrarse menores de edad, es decir, personas de tres años a dieciocho años formando parte del grupo de población de niñas, niños y adolescentes los cuales, son reconocidos como grupos vulnerables en atención a su edad, las condiciones particulares de cada uno, su grado de desarrollo y madurez toda vez que no ha concluido aún su crecimiento y desarrollo neurológico, psicológico, social y físico.

Ahora bien, por lo que hace a la categoría de titulares en función de su origen étnico o racial que pudiera derivar de los datos sociodemográficos recabados sobre entidad, municipio y localidad de nacimiento, domicilio y lengua indígena que habla; datos del contexto social, es preciso reiterar el análisis antes realizado sobre el origen étnico o racial como información sensible perteneciente a la esfera más íntima de sus titulares, es preciso señalar lo siguiente:

---

[32] Corte IDH. Caso V.R.P., V.P.C. y otros vs. Nicaragua. Excepciones Preliminares, Fondo, Reparaciones y Costas. Sentencia de 8 de marzo de 2018. Serie C No. 350, párrafo 156. Disponible en: https://www.corteidh.or.cr/docs/casos/articulos/seriec_350_esp.pdf, enlace consultado por última vez el 28/02/2023.

De acuerdo con la CEPAL, una etnia refiere a "*un grupo humano que comparte una cultura, una historia y costumbres, y cuyos miembros están unidos por una conciencia de identidad.*" En este sentido señala que una etnia implica un grupo étnico, el cual define como "*una comunidad que no solo comparte una ascendencia común sino además costumbres, un territorio, creencias, una cosmovisión, un idioma o dialecto y una aproximación simbólica al mundo semejante, y estos elementos compartidos le permiten tanto identificarse a sí mismo como ser identificado por los demás*" [33].

De igual forma, CEPAL ha señalado que, dentro del concepto de grupo étnico, "*se alberga dentro de sí, según los contextos y circunstancias, ideas como la de pueblo, nación, nacionalidad, tribu o comunidad*" por ejemplo los pueblos indígenas.

En este sentido, la Organización de las Naciones Unidas[34] ha señalado la existencia de múltiples violaciones de los derechos civiles, políticos, económicos, sociales y culturales basados en la discriminación, el racismo y la exclusión por motivos, entre otros, de raza y origen nacional o étnico. Por su parte, la Oficina del Alto Comisionada de los Derechos Humanos de la ONU[35], ha señalado que las minorías nacionales, étnicas, religiosas o lingüísticas muy a menudo, se enfrentan a múltiples formas de discriminación que se traducen en marginación y exclusión.

Aunado a lo anterior, el Consejo Nacional para Prevenir la Discriminación (CONAPRED)[36] ha señalado que las personas que conforman las comunidades indígenas enfrenten una exclusión histórica en ámbitos como la salud, la educación, la justicia y el empleo, así como en el goce de sus derechos humanos; *"los prejuicios y estereotipos que asocian a estas comunidades con la pobreza o con la falta de disposición y capacidad para trabajar han reforzado esta exclusión, tanto en lo público como en lo privado."*

En este sentido, es dable advertir que la pertenencia a un grupo étnico o racial, por ejemplo, a un pueblo o comunidad indígena, constituye un factor de vulnerabilidad dado que este tipo de grupos humanos son grupos poblacionales que se enfrentan a múltiples formas de discriminación que se traducen en marginación y exclusión, así como en violación a sus derechos humanos.

---

[33] Información disponible en el vínculo electrónico siguiente: https://repositorio.cepal.org/bitstream/handle/11362/1446/3/S2011512_es.pdf , enlace consultado por última vez el 28/02/2023.
[34] Información disponible en el vínculo electrónico siguiente: https://www.un.org/es/fight-racism/vulnerable-groups/minorities, enlace consultado por última vez el 28/02/2023.
[35] Información disponible en el vínculo electrónico siguiente: https://www.ohchr.org/SP/Issues/Minorities/Pages/MinoritiesIndex.aspx, enlace consultado por última vez el 28/02/2023.
[36] Información disponible en el vínculo electrónico siguiente: http://www.conapred.org.mx/userfiles/files/Ficha%20Pindingenas.pdf, enlace consultado por última vez el 28/02/2023.

Por lo tanto, los titulares de los datos personales que serán objeto del tratamiento pertenecen a un grupo étnico o racial, como lo puede ser una comunidad indígena, forman parte de un grupo vulnerable en función de su origen étnico-racial dadas las dificultades que enfrentan las personas estos atributos en su inserción social y las circunstancias de discriminación y violación a sus derechos humanos.

Con relación al dato sobre género, es preciso reiterar lo establecido en el análisis respecto al tratamiento de datos personales sensibles, específicamente al carácter de sensible del dato de sexo.

Con respecto a los datos de discapacidad es importante señalar lo establecido en el artículo 2, fracción XXVII de la Ley de Inclusión, el cual dice a la letra lo siguiente:

> *"**Artículo 2.** Para los efectos de esta Ley se entenderá por:*
> *I. a XIV*
> *XV. **Persona con discapacidad:** Toda persona que por razón congénita o adquirida presenta una o más deficiencias de carácter físico, mental, intelectual o sensorial, ya sea permanente o temporal y que al interactuar con las barreras que le impone el entorno social, pueda impedir su inclusión plena y efectiva, en igualdad de condiciones con los demás;*
> *[…]"*

Una persona con discapacidad es la que presenta, por una razón congénita o adquirida, una limitación o deficiencia física, mental, intelectual o sensorial, transitoria o permanente, que le impide desarrollar sus actividades en la forma que se considera normal para un ser humano, con las barreras que le impone el entorno social.

Por otro lado, la Convención sobre los Derechos de las Personas con Discapacidad[37] reconoce que la discapacidad es:

> *"e) Reconociendo que la discapacidad es un concepto que evoluciona y que resulta de la interacción entre las personas con deficiencias y las barreras debidas a la actitud y al entorno que evitan su participación plena y efectiva en la sociedad, en igualdad de condiciones con las demás,*
> *[…]*
> *k) Observando con preocupación que, pese a estos diversos instrumentos y actividades, las personas con discapacidad siguen encontrando barreras para participar en igualdad de condiciones con las demás en la vida social y que se siguen vulnerando sus derechos humanos en todas las partes del mundo, […]"*

[37] Convención disponible en el vínculo electrónico siguiente: https://www.un.org/esa/socdev/enable/documents/tccconvs.pdf , enlace consultado por última vez el 28/02/2023.

Por su parte, la Comisión Nacional de Derechos Humanos[38] coloca a las personas con discapacidad en *"condiciones de mayor vulnerabilidad al enfrentarse a barreras físicas, institucionales, de información, de actitud y de comunicación, legitimadas por la sociedad"*, lo que las excluye frecuentemente de una participación activa en la sociedad y del reconocimiento pleno de sus derechos humanos, ya que "*se considera, equivocadamente, que no pueden llevar a cabo las mismas actividades, en igualdad de condiciones que el resto de las personas*".

Por lo anterior, es dable advertir que la discapacidad es esta interacción de una persona que, por razón congénita o adquirida, presenta una o más deficiencias de carácter físico, mental, intelectual o sensorial, permanente o temporal con las barreras impuestas, con el entorno social que impiden su inclusión plena y efectiva en la sociedad en igualdad de condiciones con los demás.

Por lo cual, las personas con discapacidad constituyen grupos poblacionales en condición de mayor vulnerabilidad al enfrentarse a diversas barreras u obstáculos tanto de carácter físico, institucional, de acceso a servicios, de actitud y de comunicación, así como en su participación activa y en igualdad de condiciones con las demás en la vida social lo cual vulnera sus derechos humanos.

Por lo tanto, los titulares de los datos personales objeto de tratamiento a través del Sistema de Procesamiento que presenten alguna posible discapacidad, no sólo constituyen un grupo vulnerable dado el factor de su condición, sino que también se sobreponen distintas dimensiones de vulnerabilidad más allá de la edad, por ejemplo, el estado de salud, presente y futuro, en caso de tener alguna discapacidad la pertenencia étnica, el género, la raza, el origen étnico o la religión.

Con relación al idioma o lenguaje de acuerdo con el artículo 2 de la Ley General de los Derechos Lingüísticos de los Pueblos Indígenas[39], las lenguas indígenas son *aquellas que proceden de los pueblos existentes en el territorio nacional antes del establecimiento del Estado Mexicano, además de aquellas provenientes de otros pueblos indoamericanos, igualmente preexistentes que se han arraigado en el territorio nacional con posterioridad y que se reconocen por poseer un conjunto ordenado y sistemático de formas orales funcionales y simbólicas de comunicación.*

---

[38] Información disponible en el vínculo electrónico siguiente: http://informe.cndh.org.mx/menu.aspx?id=10039#ida10846, enlace consultado por última vez el 28/02/2023.

[39] Publicados en el DOF el 13 de marzo de 2003; disponible en el vínculo electrónico siguiente: http://www.dof.gob.mx/nota_detalle.php?codigo=698625&fecha=13/03/2003 última reforma publicada en el DOF el 20 de junio de 2018, disponible en el vínculo electrónico siguiente: http://dof.gob.mx/nota_detalle.php?codigo=5527037&fecha=20/06/2018, texto consolidado por la Cámara de Diputados del H. Congreso de la Unión en formato de documento portable, denominado como pdf por sus siglas en inglés, incorporando las diversas reformas de dicho ordenamiento jurídico en el sitio siguiente: http://www.diputados.gob.mx/LeyesBiblio/pdf/257_200618.pdf; enlaces consultados por última vez el 28/02/2023.

De acuerdo con el documento curricular para la elaboración de los programas de estudio de las lenguas indígenas emitido por la Secretaría de Educación Pública en el año 2013, ésta *se refiere a un "nombre genérico para referirse a los idiomas indígenas que se hablan en el territorio nacional"*[40] mismas que son 70 lenguas pertenecientes a" diez *familias o troncos lingüísticos con características fonológicas, morfológicas, sintácticas y semánticas tan distintas entre sí"*, en México existen prejuicios en torno a la identidad indígena lo que provoca que existan discriminación a los hablantes de dichas lenguas, inclusive ésta ha contribuido a la extinción de las lenguas originaria[41] por lo que al ser una información que permita discriminan al titular de dicho dato, éste encuentra en la categoría de sensible.

La Convención sobre la Eliminación de toda forma de Discriminación Racial[42] del que México forma parte, en el artículo 1, párrafo primero, define como discriminación racial a:

> *"[...]* ***toda distinción, exclusión, restricción o preferencia basada*** *en motivos de* ***raza, color, linaje u origen nacional o étnico*** *que tenga por objeto o resultado anular o menoscabar el reconocimiento, goce o ejercicio, en condiciones de igualdad, de los derechos humanos y las libertades fundamentales en las esferas política, económica, social, cultural o en cualquier otra esfera de la vida pública."*
>
> ***[Énfasis añadido]***

De esa misma forma, el artículo 1, último párrafo de la Constitución manifiesta que:

> "*Queda* ***prohibida toda discriminación motivada por origen étnico o nacional, el género, la edad, las discapacidades, la condición social, las condiciones de salud, la religión, las opiniones, las preferencias sexuales, el estado civil o cualquier otra*** *que atente contra la dignidad humana y tenga por objeto anular o menoscabar los derechos y libertades de las personas"*
>
> ***[Énfasis añadido]***

Ahora bien, en cuanto a los datos personales referentes a la raza, color linaje, origen nacional o étnico de una persona es un dato personal que puede conllevar a una persona a ser objeto de discriminación y, por tanto, razón suficiente para que existan normatividades que señalen de forma específica la prohibición de discriminación con base en éstos, lo que nos permite concluir que

---

[40] Documento disponible en el siguiente vínculo electrónico: https://educacionbasica.sep.gob.mx/multimedia/RSC/BASICA/Documento/201611/201611-3-RSC-FPozv0Ni9x-parametros_curriculares.pdf, enlace consultado por última vez el 28/02/2023.

[41] Noticia disponible en el siguiente vínculo electrónico: https://www.eluniversal.com.mx/articulo/cultura/2015/10/22/discriminacion-obstaculo-para-rescatar-lenguas-indigenas, enlace consultado por última vez el 28/02/2023.

[42] Documento disponible en el vínculo electrónico siguiente: https://www.cndh.org.mx/DocTR/2016/JUR/A70/01/JUR-20170331-II11.pdf, enlace consultado por última vez el 28/02/2023.

estamos ante datos personales que determinan a las personas titulares a formar parte de un grupo de alta vulnerabilidad ante los riesgos a los que se enfrentan.

En virtud de lo anterior, es preciso señalar que efectivamente dichos grupos de personas configuran un grupo social en condición de vulnerabilidad pues enfrentan situaciones de riesgo o discriminación debido a su condición y contexto con motivo del delito de desaparición que les impiden alcanzar mejores niveles de vida y bienestar integral y que, por lo tanto, requieren de atención por parte del Estado para su atención y bienestar.

Por lo que, se determina que la implementación del Sistema de Procesamiento actualiza el supuesto de un tratamiento intensivo o relevante de datos personales en función del artículo 9, fracción III de las Disposiciones administrativas, relativo al tratamiento de datos personales de grupos vulnerables, de conformidad con el análisis y descripción realizado previamente.

Ahora, bien por lo que concierne a la fracción VI del artículo 9 de las Disposiciones administrativas referente a realizar un tratamiento frecuente y continúo de grandes volúmenes de datos personales; se señala qué se entiende por "frecuente" y "continuo". De acuerdo con la Real Academia Española, se advierte lo siguiente:

> ***"continuo[43]:***
> *1. adj. Que dura, obra, se hace o se extiende sin interrupción.*
> *[…]*
> ***3.** adj. Constante y perseverante en alguna acción.*
> *[…]"*
>
> ***"frecuente[44]:***
> ***1.** adj. Repetido a menudo."*

Por lo tanto, un tratamiento de datos personales frecuente y continuo, consiste en un tratamiento que se realiza sin interrupción, de manera constante y se repite a menudo; en ese sentido, en la evaluación de impacto, el AIFA señaló que el tiempo de duración del Sistema de Procesamiento, tendrá un servicio de soporte y mantenimiento hasta el 21 de marzo 2024.

Una vez precisado lo anterior, tomando en consideración lo mencionado en el apartado de consideraciones preliminares, en la puesta en operación del Sistema de Procesamiento se contempla la realización de cruces de información de este con múltiples sistemas o plataformas

---

[43] Diccionario de la Real Academia Española; disponible en el vínculo siguiente: https://dle.rae.es/continuo?m=form, enlace consultado por última vez el 28/02/2023.

[44] Diccionario de la Real Academia Española; disponible en el vínculo siguiente: https://dle.rae.es/frecuente?m=form , enlace consultado por última vez el 28/02/2023.

competentes para intercambiar datos relacionados con el enrolamiento y verificación de identidad de pasajeros.

Por lo que se considera que se actualiza el supuesto establecido en la fracción VI del artículo 9 de las Disposiciones administrativas, pues implica la realización de un tratamiento frecuente y continúo de grandes volúmenes de datos personales, así como el llevar a cabo cruces de información con múltiples sistemas o plataformas informáticas.

Por otro lado, como bien se señaló, la puesta en operación del Sistema de Procesamiento conlleva el tratamiento de datos personales sensibles con la finalidad de efectuar un tratamiento sistemático a través de dicho sistema con la interoperabilidad de diversos sistemas y plataformas que convergen entre sí para poder llevar a cabo el enrolamiento y verificación de la identidad de los pasajeros, así como la generación del PDE, en los supuestos de procesamiento biométrico.

Al respecto, conviene traer a colación, a manera de referencia, que el GT29 en sus *Directrices sobre la evaluación de impacto relativa a la protección de datos (EIPD) y para determinar si el tratamiento «entraña probablemente un alto riesgo» a efectos del Reglamento (UE) 2016/679*[45], interpreta el término "sistemático" con uno o más de los siguientes significados:

- Que se produce de acuerdo con un sistema.
- Preestablecido, organizado o metódico.
- Que tiene lugar como parte de un plan general de recogida de datos.
- Llevado a cabo como parte de una estrategia.

En una primera instancia y tomando en consideración la operación del Sistema de Procesamiento antes analizada, éste pudiera conllevar para su funcionamiento una serie de sistemas que lo conformarán de acuerdo a las finalidades que se persigan cuya implementación es parte del plan general de recolectar, organizar, agregar, analizar y procesar los datos personales en el marco de la estrategia tecnológica que permita unificar y definir una metodología estandarizada de información para homologar y garantizar la interoperabilidad, disponibilidad y consistencia de los datos relativos a personas que llevan a cabo su enrolamiento y verificación de identidad a través del Sistema de Procesamiento.

En esta circunstancia, se determina la actualización del artículo 9, fracción XI de las Disposiciones administrativas en virtud de que se tratarán datos personales sensibles con la finalidad de efectuar un tratamiento sistemático a través de los sistemas que pudieran interactuar el Sistema de Procesamiento, así como un tratamiento masivo de los mismos.

---

[45] Ibidem.

Finalmente, por lo que hace al supuesto contenido en el primer extremo del artículo 9, fracción XIII de las Disposiciones administrativas relativo a realizar un tratamiento a gran escala de datos personales sensibles, se considera necesario volver a retomar como referencia el GT29, el cual recomienda que para determinar que se está ante un tratamiento de datos a gran escala, es necesario tomar en consideración los siguientes factores:

- El número de interesados afectados, bien como cifra concreta o como proporción de la población correspondiente;
- El volumen de datos o la variedad de elementos de datos que son objeto de tratamiento;
- La duración, o permanencia, de la actividad de tratamiento de datos;
- El alcance geográfico de la actividad de tratamiento.

En este sentido y tomando en consideración el caso concreto, se tiene que, en su primera fase, el AIFA tendrá una capacidad para atender una demanda de 19.5 millones de pasajeros y 470 mil toneladas de carga aérea anuales. Cuando alcance su última fase de construcción proyectada para el año 2050, este aeropuerto moverá a 85 millones de pasajeros y. En este sentido, es posible inferir que la cantidad de datos constituye un gran volumen de información.

Por lo tanto, y conforme a lo antes expuesto, se advierte el cumplimiento de la primera condición del artículo 9, fracción XIII toda vez que en primera instancia se tratarán datos personales de carácter sensible tratamiento a realizar a gran escala pues persigue tratar una cantidad considerable de datos personales, a nivel nacional, de un gran número de interesados, lo cual pudiera afectar a un gran número de interesados y entrañar probablemente un alto riesgo del tratamiento.

Aunado a los supuestos manifestados por el responsable, es posible advertir que también se actualizan los supuestos vertidos en el artículo 9, fracciones IV, V y VII, es decir:

- Crear bases de datos concernientes a un número elevado de titulares, aun cuando dichas bases no estén sujetas a criterios determinados en cuanto a su creación o estructura, de tal manera que se produzca la acumulación no intencional de una gran cantidad de datos personales respecto de los mismos.
- Incluir o agregar nuevas categorías de datos personales a las bases de datos ya existentes y en posesión del responsable, de tal forma que, en caso de presentarse una vulneración de seguridad por la cantidad de información contenida en ellas, pudiera derivarse una afectación a la esfera personal de los titulares, sus derechos o libertades.
- Utilizar tecnologías con sistemas de vigilancia; aeronaves o aparatos no tripulados; minería de datos; biometría; Internet de las cosas; geolocalización; técnicas analíticas; radiofrecuencia o cualquier otra que pueda desarrollarse en el futuro y que implique un tratamiento de datos personales a gran escala.

Lo anterior es así, ya que, en el primer supuesto, se advierte que los datos personales que conforman el PDE serán almacenados en la plataforma vb Orchestra y en bases de datos internas del AIFA, lo cual implica la creación de bases de datos concernientes a un número elevado de titulares considerando el número antes referido de titulares por el AIFA.

De igual forma, en el supuesto sobre incluir o agregar nuevas categorías de datos personales a las bases de datos ya existentes, se advierte que se agregarán los datos biométricos a las bases de datos del AIFA, lo cual implica una nueva categoría de datos.

Ahora bien, por lo que hace a utilizar tecnologías de biometría, el responsable señala justamente que una de las finalidades principales es establecer un Sistema de procesamiento que permita el enrolamiento biométrico tanto en el módulo CUSS, como en el quiosco de servicios y en la app. Por lo cual se está ante un tratamiento de datos personales en el que se usará tecnología biométrica.

Por las razones antes expuestas, se determina que la puesta en operación del Sistema de procesamiento es susceptible de configurarse como un tratamiento de datos personales relevante o intensivo de carácter particular, en términos de lo previsto en los artículos, 76 de la Ley General y 9 fracciones III, IV, V, VI, VII, XI de las Disposiciones administrativas que se refieren a las siguientes condiciones:

- Tratar datos personales de grupos vulnerables atendiendo, de manera enunciativa mas no limitativa, a su edad; género; origen étnico o racial; estado de salud; preferencia sexual; nivel de instrucción y condición socioeconómica.
- Crear bases de datos concernientes a un número elevado de titulares, aun cuando dichas bases no estén sujetas a criterios determinados en cuanto a su creación o estructura, de tal manera que se produzca la acumulación no intencional de una gran cantidad de datos personales respecto de los mismos.
- Incluir o agregar nuevas categorías de datos personales a las bases de datos ya existentes y en posesión del responsable, de tal forma que, en caso de presentarse una vulneración de seguridad por la cantidad de información contenida en ellas, pudiera derivarse una afectación a la esfera personal de los titulares, sus derechos o libertades.
- Realizar un tratamiento frecuente y continúo de grandes volúmenes de datos personales, o bien, llevar a cabo cruces de información con múltiples sistemas o plataformas informáticas.
- Utilizar tecnologías de biometría.
- Tratar datos personales sensibles con la finalidad de efectuar un tratamiento sistemático y masivo de los mismos.

Por lo tanto, es posible advertir que la puesta en operación del Sistema de Procesamiento reúne las características previstas para la procedencia de la elaboración y presentación de una evaluación de impacto en la protección de datos personales, atendiendo a lo siguiente:

- Constituye una puesta en operación de una política pública que implica un tratamiento de datos personales.
- Dicho tratamiento se realiza a través de una herramienta tecnológica, esto es del Sistema de procesamiento.
- Implica un tratamiento relevante o intensivo de carácter general y particular.

VII. Identificación, análisis y gestión de los riesgos para la protección de los datos personales en el Sistema de Procesamiento

Al respecto, la Ley General menciona que:

> *"**Artículo 33.** Para establecer y mantener las medidas de seguridad para la protección de los datos personales, el responsable deberá realizar, al menos, las siguientes actividades interrelacionadas:*
> *[...]*
> *III. Elaborar un inventario de datos personales y de los sistemas de tratamiento;*
> *IV. Realizar un análisis de riesgo de los datos personales, considerando las amenazas y vulnerabilidades existentes para los datos personales y los recursos involucrados en su tratamiento, como pueden ser, de manera enunciativa más no limitativa, hardware, software, personal del responsable, entre otros;*
> *V. Realizar un análisis de brecha, comparando las medidas de seguridad existentes contra las faltantes en la organización del responsable;*
> *VI. Elaborar un plan de trabajo para la implementación de las medidas de seguridad faltantes, así como las medidas para el cumplimiento cotidiano de las políticas de gestión y tratamiento de los datos personales;*
> *[...]".*

De conformidad con lo dispuesto en el artículo 33 fracciones III y IV de la Ley General, para establecer y mantener las medidas de seguridad para la protección de los datos personales el responsable debe elaborar un inventario de datos personales y de los sistemas de tratamiento, así como, realizar un análisis de riesgo de los datos personales, considerando las amenazas y vulnerabilidades existentes para los datos personales y los recursos involucrados en su tratamiento, como pueden ser, de manera enunciativa más no limitativa, hardware, software, personal del responsable, entre otros; así como otras actividades interrelacionadas.

Adicionalmente, los Lineamientos generales señalan que:

> ***"Análisis de riesgos***

Artículo 60. *Para dar cumplimiento al artículo 33, fracción IV de la Ley General, el responsable deberá realizar un análisis de riesgos de los datos personales tratados considerando lo siguiente:*

I. Los requerimientos regulatorios, códigos de conducta o mejores prácticas de un sector específico;
II. El valor de los datos personales de acuerdo a su clasificación previamente definida y su ciclo de vida;
III. El valor y exposición de los activos involucrados en el tratamiento de los datos personales;
IV. Las consecuencias negativas para los titulares que pudieran derivar de una vulneración de seguridad ocurrida, y
V. Los factores previstos en el artículo 32 de la Ley General.

Análisis de brecha

Artículo 61*. Con relación al artículo 33, fracción V de la Ley General, para la realización del análisis de brecha el responsable deberá considerar lo siguiente:*

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

Plan de trabajo

Artículo 62. *De conformidad con lo dispuesto en el artículo 33, fracción VI de la Ley General, el responsable deberá elaborar un plan de trabajo que defina las acciones a implementar de acuerdo con el resultado del análisis de riesgos y del análisis de brecha, priorizando las medidas de seguridad más relevantes e inmediatas a establecer.*
Lo anterior, considerando los recursos designados; el personal interno y externo en su organización y las fechas compromiso para la implementación de las medidas de seguridad nuevas o faltantes."

Por su parte, el artículo 19 de las Disposiciones administrativas señala que:

*"**Artículo 19.** En la evaluación de impacto en la protección de datos personales, el responsable deberá incluir la gestión de riesgos que tenga por objeto identificar y analizar los posibles riesgos y amenazas, así como los daños o consecuencias que pudieran producirse o presentarse si llegasen a materializarse con la puesta en operación o modificación de la política pública, programa, sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología que implique un tratamiento intensivo o relevante de datos personales.*

El responsable deberá presentar un plan general para gestionar los riesgos identificados, en el que se mencione, al menos, lo siguiente:

I. La identificación y descripción específica de los riesgos administrativos, físicos o tecnológicos que podrían presentarse con la puesta en operación o modificación de la política pública, programa, sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología que implique un tratamiento intensivo o relevante de datos personales;
II. La ponderación cuantitativa y/o cualitativa de la probabilidad de que los riesgos identificados sucedan, así como su nivel de impacto en los titulares en lo que respecta al tratamiento de sus datos personales, y
III. Las medidas y controles concretos que el responsable adoptará para eliminar, mitigar, transferir o retener los riesgos detectados, de tal manera que no tengan un impacto en la esfera de los titulares, en lo que respecta al tratamiento de sus datos personales."

De las disposiciones anteriores se advierte que el responsable está obligado a realizar un análisis de riesgo de los datos personales y los recursos involucrados en su tratamiento, considerando: (I) los requerimientos regulatorios, códigos de conducta o mejores prácticas de un sector específico; (II) el valor de los datos personales de acuerdo con la clasificación previamente definida y su ciclo de vida; (III) el valor y exposición de los activos involucrados en el tratamiento de los datos personales; (IV) las consecuencias negativas para los titulares que pudieran derivar de una vulneración de seguridad ocurrida, y (V) los factores previstos en el artículo 32 de la Ley General.

Al respecto, en el documento denominado "ANÁLISIS DE RIESGOS PARA DATOS PERSONALES" se manifestó lo siguiente:

Se elimina hoja completa, con fundamento en el artículo 110, fracción I de la LFTAIP;Décimo séptimo de los lineamientos Generales en materia de clasificación y desclasificación de la información,así como para la elaboración de versiones públicas, en relación con el artículo 5, fracción VI de la Ley de Seguridad Nacional; 47, Bis 4 de la Ley de Aviación Civil, 46 y 47 de la Ley de Aeropuertos y 152 del Reglamento de Aeropuertos.

Se elimina hoja completa, con fundamento en el artículo 110, fracción I de la LFTAIP;Décimo séptimo de los lineamientos Generales en materia de clasificación y desclasificación de la información,así como para la elaboración de versiones públicas, en relación con el artículo 5, fracción VI de la Ley de Seguridad Nacional; 47, Bis 4 de la Ley de Aviación Civil, 46 y 47 de la Ley de Aeropuertos y 152 del Reglamento de Aeropuertos.

Se elimina hoja completa, con fundamento en el artículo 110, fracción I de la LFTAIP;Décimo séptimo de los lineamientos Generales en materia de clasificación y desclasificación de la información,así como para la elaboración de versiones públicas, en relación con el artículo 5, fracción VI de la Ley de Seguridad Nacional; 47, Bis 4 de la Ley de Aviación Civil, 46 y 47 de la Ley de Aeropuertos y 152 del Reglamento de Aeropuertos.

Se elimina hoja completa, con fundamento en el artículo 110, fracción I de la LFTAIP;Décimo séptimo de los lineamientos Generales en materia de clasificación y desclasificación de la información,así como para la elaboración de versiones públicas, en relación con el artículo 5, fracción VI de la Ley de Seguridad Nacional; 47, Bis 4 de la Ley de Aviación Civil, 46 y 47 de la Ley de Aeropuertos y 152 del Reglamento de Aeropuertos.

Se elimina hoja completa, con fundamento en el artículo 110, fracción I de la LFTAIP;Décimo séptimo de los lineamientos Generales en materia de clasificación y desclasificación de la información,así como para la elaboración de versiones públicas, en relación con el artículo 5, fracción VI de la Ley de Seguridad Nacional; 47, Bis 4 de la Ley de Aviación Civil, 46 y 47 de la Ley de Aeropuertos y 152 del Reglamento de Aeropuertos.

Se elimina hoja completa, con fundamento en el artículo 110, fracción I de la LFTAIP;Décimo séptimo de los lineamientos Generales en materia de clasificación y desclasificación de la información,así como para la elaboración de versiones públicas, en relación con el artículo 5, fracción VI de la Ley de Seguridad Nacional; 47, Bis 4 de la Ley de Aviación Civil, 46 y 47 de la Ley de Aeropuertos y 152 del Reglamento de Aeropuertos.

Se elimina hoja completa, con fundamento en el artículo 110, fracción I de la LFTAIP;Décimo séptimo de los lineamientos Generales en materia de clasificación y desclasificación de la información,así como para la elaboración de versiones públicas, en relación con el artículo 5, fracción VI de la Ley de Seguridad Nacional; 47, Bis 4 de la Ley de Aviación Civil, 46 y 47 de la Ley de Aeropuertos y 152 del Reglamento de Aeropuertos.

Se elimina hoja completa, con fundamento en el artículo 110, fracción I de la LFTAIP;Décimo séptimo de los lineamientos Generales en materia de clasificación y desclasificación de la información,así como para la elaboración de versiones públicas, en relación con el artículo 5, fracción VI de la Ley de Seguridad Nacional; 47, Bis 4 de la Ley de Aviación Civil, 46 y 47 de la Ley de Aeropuertos y 152 del Reglamento de Aeropuertos.

Se elimina hoja completa, con fundamento en el artículo 110, fracción I de la LFTAIP;Décimo séptimo de los lineamientos Generales en materia de clasificación y desclasificación de la información,así como para la elaboración de versiones públicas, en relación con el artículo 5, fracción VI de la Ley de Seguridad Nacional; 47, Bis 4 de la Ley de Aviación Civil, 46 y 47 de la Ley de Aeropuertos y 152 del Reglamento de Aeropuertos.

Se elimina hoja completa, con fundamento en el artículo 110, fracción I de la LFTAIP;Décimo séptimo de los lineamientos Generales en materia de clasificación y desclasificación de la información,así como para la elaboración de versiones públicas, en relación con el artículo 5, fracción VI de la Ley de Seguridad Nacional; 47, Bis 4 de la Ley de Aviación Civil, 46 y 47 de la Ley de Aeropuertos y 152 del Reglamento de Aeropuertos.

Se elimina hoja completa, con fundamento en el artículo 110, fracción I de la LFTAIP;Décimo séptimo de los lineamientos Generales en materia de clasificación y desclasificación de la información,así como para la elaboración de versiones públicas, en relación con el artículo 5, fracción VI de la Ley de Seguridad Nacional; 47, Bis 4 de la Ley de Aviación Civil, 46 y 47 de la Ley de Aeropuertos y 152 del Reglamento de Aeropuertos.

Se elimina hoja completa, con fundamento en el artículo 110, fracción I de la LFTAIP;Décimo séptimo de los lineamientos Generales en materia de clasificación y desclasificación de la información,así como para la elaboración de versiones públicas, en relación con el artículo 5, fracción VI de la Ley de Seguridad Nacional; 47, Bis 4 de la Ley de Aviación Civil, 46 y 47 de la Ley de Aeropuertos y 152 del Reglamento de Aeropuertos.

Se elimina hoja completa, con fundamento en el artículo 110, fracción I de la LFTAIP;Décimo séptimo de los lineamientos Generales en materia de clasificación y desclasificación de la información,así como para la elaboración de versiones públicas, en relación con el artículo 5, fracción VI de la Ley de Seguridad Nacional; 47, Bis 4 de la Ley de Aviación Civil, 46 y 47 de la Ley de Aeropuertos y 152 del Reglamento de Aeropuertos.

Se elimina hoja completa, con fundamento en el artículo 110, fracción I de la LFTAIP;Décimo séptimo de los lineamientos Generales en materia de clasificación y desclasificación de la información,así como para la elaboración de versiones públicas, en relación con el artículo 5, fracción VI de la Ley de Seguridad Nacional; 47, Bis 4 de la Ley de Aviación Civil, 46 y 47 de la Ley de Aeropuertos y 152 del Reglamento de Aeropuertos.

Se elimina hoja completa, con fundamento en el artículo 110, fracción I de la LFTAIP;Décimo séptimo de los lineamientos Generales en materia de clasificación y desclasificación de la información,así como para la elaboración de versiones públicas, en relación con el artículo 5, fracción VI de la Ley de Seguridad Nacional; 47, Bis 4 de la Ley de Aviación Civil, 46 y 47 de la Ley de Aeropuertos y 152 del Reglamento de Aeropuertos.

Se elimina hoja completa, con fundamento en el artículo 110, fracción I de la LFTAIP;Décimo séptimo de los lineamientos Generales en materia de clasificación y desclasificación de la información,así como para la elaboración de versiones públicas, en relación con el artículo 5, fracción VI de la Ley de Seguridad Nacional; 47, Bis 4 de la Ley de Aviación Civil, 46 y 47 de la Ley de Aeropuertos y 152 del Reglamento de Aeropuertos.

Se elimina hoja completa, con fundamento en el artículo 110, fracción I de la LFTAIP;Décimo séptimo de los lineamientos Generales en materia de clasificación y desclasificación de la información,así como para la elaboración de versiones públicas, en relación con el artículo 5, fracción VI de la Ley de Seguridad Nacional; 47, Bis 4 de la Ley de Aviación Civil, 46 y 47 de la Ley de Aeropuertos y 152 del Reglamento de Aeropuertos.

Se elimina hoja completa, con fundamento en el artículo 110, fracción I de la LFTAIP;Décimo séptimo de los lineamientos Generales en materia de clasificación y desclasificación de la información,así como para la elaboración de versiones públicas, en relación con el artículo 5, fracción VI de la Ley de Seguridad Nacional; 47, Bis 4 de la Ley de Aviación Civil, 46 y 47 de la Ley de Aeropuertos y 152 del Reglamento de Aeropuertos.

Se elimina hoja completa, con fundamento en el artículo 110, fracción I de la LFTAIP;Décimo séptimo de los lineamientos Generales en materia de clasificación y desclasificación de la información,así como para la elaboración de versiones públicas, en relación con el artículo 5, fracción VI de la Ley de Seguridad Nacional; 47, Bis 4 de la Ley de Aviación Civil, 46 y 47 de la Ley de Aeropuertos y 152 del Reglamento de Aeropuertos.

Al ser parte del objeto de creación del AIFA tener a su cargo un aeropuerto, es importante considerar el contenido conducente de la Concesión del AIFA en los siguientes términos:

"[...]

1.1 Definiciones. Para efectos de la presente concesión, se entenderá por:

Aeropuerto: *El aeródromo civil según se define en la fracción VI del artículo 2 de la Ley de Aeropuertos, cuyas características se encuentran descritas en la condición 2.2 del presente título de Concesión.*

[...]

Concesionaria: *AEROPUERTO INTERNACIONAL FELIPE ÁNGELES, S.A. DE C.V., una sociedad constituida conforme a las leyes mexicanas que, al momento del otorgamiento de esta Concesión, es una empresa estatal mayoritaria del Gobierno Federal.*

[...]

Capítulo II

Objeto, Alcances y Régimen Inmobiliario

2.1 Objeto de la Concesión: El presente título tiene por objeto otorgar a "LA CONCESIONARIA":

2.1.1 Una Concesión para construir, administrar, operar y explotar el Aeropuerto.

[...]

2.4 Servicios: "LA CONCESIONARIA", por sí misma o por conducto de terceros, prestará los servicios aeroportuarios, complementarios y comerciales de manera permanente, uniforme, regular y no discriminatoria, a todos los usuarios del Aeropuerto, incluidos los concesionarios y los permisionarios del servicio de transporte aéreo regular nacional, no regular nacional, privado comercial y privado no comercial que así lo requieran.

En caso de que el Aeropuerto sea declarado y habilitado como internacional, "LA CONCESIONARIA", adicionalmente a lo anterior, podrá prestar los servicios aeroportuarios a los concesionarios y los permisionarios del servicio de transporte aéreo internacional regular y no regular.

"LA CONCESIONARIA" en todo momento, tendrá la responsabilidad frente a "LA SECRETARÍA", a fin de que los Servicios se presten en términos de la legislación aplicable y de este título de Concesión.

Asimismo, "LA CONCESIONARIA" será responsable de que el Aeropuerto cuente con los servicios aeroportuarios y complementarios que se requieran, de acuerdo a su clasificación, clave de referencia y categoría.

2.4.1 Servicios Complementarios: Para la prestación de los servicios complementarios, "LA CONCESIONARIA" deberá observar lo dispuesto en los artículos 57, 58 y demás relativos de la Ley y del Reglamento.

"LA CONCESIONARIA" podrá prestar los servicios complementarios directamente, siempre que lo realice en forma eficiente, equitativa y no discriminatoria, frente a los concesionarios o permisionarios del servicio de transporte aéreo u otros terceros prestadores de estos servicios en el Aeropuerto.

"LA CONCESIONARIA" estará obligada a identificar y registrar, de manera independiente, las operaciones, los costos e ingresos relacionados con los servicios complementarios que preste.

En todo caso, "LA CONCESIONARIA" deberá llevar a cabo los actos necesarios a efecto de contar con opciones competitivas para la prestación de cada uno de los servicios complementarios.

"LA CONCESIONARIA" únicamente podrá limitar el número de prestadores de servicios complementarios por razones de disponibilidad de espacio, eficiencia operativa y seguridad, lo anterior después de escuchar la opinión del Comité de Operación y Horarios del Aeropuerto, y previa aprobación de "LA SECRETARÍA".

El Comité de Operación y Horarios del Aeropuerto se integrará conforme a lo dispuesto en el artículo 61 de la Ley, los relativos del Reglamento, y conforme a lo estipulado en la condición 7.3 del presente título.

En los supuestos en que "LA CONCESIONARIA" limite el número de prestadores de servicios complementarios conforme al párrafo anterior, los contratos necesarios para permitir que los concesionarios y permisionarios del transporte aéreo o terceros ajenos a éstos presten los servicios complementarios que sean requeridos en el Aeropuerto, serán adjudicados a favor de aquellas personas que ofrezcan las mejores condiciones para una operación eficiente y segura del Aeropuerto, así como la mejor calidad y precio para los usuarios. "LA CONCESIONARIA", con la participación de los concesionarios y permisionarios del servicio de transporte aéreo, establecerá los criterios, las reglas generales para las adjudicaciones, y en su caso, los procedimientos de los concursos y llevará a cabo los mismos.

En caso de que "LA CONCESIONARIA" contravenga lo señalado en la presente condición, "LA SECRETARÍA" podrá ordenarle que deje de prestar los servicios complementarios, sin perjuicio de lo establecido en el artículo 58 de la Ley.

2.4.2 Servicios de Combustible: De conformidad con la legislación aplicable, los servicios que a continuación se indican de manera enunciativa más no limitativa, consistentes en el transporte, almacenamiento, distribución, suministro, succión o expendio de combustible a los operadores, concesionarios y permisionarios del servicio de transporte aéreo, usuarios del Aeropuerto a que se refiere la presente condición podrán ser prestados por terceros.

"LA CONCESIONARIA" deberá tomar las medidas necesarias para que dichos servicios se presten de forma segura y eficiente.

"LA CONCESIONARIA" celebrará los contratos necesarios en los que se establecerán los términos y condiciones para que dichos servicios se presten de manera segura y eficiente, precisando la contraprestación y forma de pago correspondiente para "LA CONCESIONARIA", por el acceso y el uso de sus instalaciones para la prestación del servicio de combustible en el Aeropuerto.

Asimismo, "LA CONCESIONARIA" deberá adecuar sus programas al crecimiento y necesidades del Aeropuerto. "LA CONCESIONARIA" y el tercero que preste el servicio al que se alude en la presente condición, serán responsables de cualquier daño que ocasione la prestación del servicio de combustible.

Todos los conflictos que surjan con motivo de la prestación de los servicios de combustible serán resueltos por aquellas autoridades competentes de conformidad con la normatividad aplicable.

2.4.3 Servicios Comerciales: Los servicios comerciales en el Aeropuerto podrán ser prestados directamente por "LA CONCESIONARIA" o por terceros que contrate la misma, mediante el arrendamiento de áreas, en términos de los artículos 48, fracción III, de la Ley, y 65 del Reglamento, incluyendo, sin limitar: áreas para comercios, restaurantes, arrendamiento de vehículos, publicidad, correo, casas de cambio, bancos y hoteles. En ningún caso la prestación de servicios comerciales debe constituir un obstáculo para la prestación de servicios aeroportuarios y complementarios, ni podrá poner en peligro la seguridad del Aeropuerto o la operación de las aeronaves. En caso de que esto ocurra, "LA SECRETARÍA" ordenará las adecuaciones necesarias. Las áreas que se destinen a la prestación de servicios comerciales serán descritas en el Programa Maestro de Desarrollo y para modificarlas se requerirá la previa autorización de "LA SECRETARÍA".

Asimismo, "LA CONCESIONARIA" y/o terceros que contrate la misma deberán cumplir con lo dispuesto en la condición 2.3.2 del presente título.

2.4.4 Responsabilidad. "LA CONCESIONARIA" responderá directamente ante "LA SECRETARÍA", del cumplimento de las obligaciones asumidas bajo esta Concesión, inclusive de aquellas que se deriven de la celebración de contratos con terceros, así como de los daños que, con motivo de la administración, operación, explotación y, en su caso, construcción, se causen a los Bienes Concesionados y a terceros usuarios del Aeropuerto.

[...]"

Por lo expuesto, se desprende que el AIFA tiene a su cargo los siguientes servicios derivados de la concesión que le fue otorgada para construir, administrar, operar y explotar el aeropuerto:

- El AIFA prestará por sí misma o por conducto de terceros, los servicios aeroportuarios, complementarios y comerciales de manera permanente, uniforme, regular y no discriminatoria, a todos los usuarios del aeropuerto, incluidos los concesionarios y los permisionarios del servicio de transporte aéreo regular nacional, no regular nacional, privado comercial y privado no comercial que así lo requieran.
- En caso de que el Aeropuerto sea declarado y habilitado como internacional, el AIFA podrá prestar, adicionalmente a lo anterior, los servicios aeroportuarios a los concesionarios y los permisionarios del servicio de transporte aéreo internacional regular y no regular.
- **El AIFA en todo momento, tendrá la responsabilidad frente a la Secretaría de Infraestructura, Comunicaciones y Transportes, a fin de que los Servicios se presten en términos de la legislación aplicable y de la Concesión del Aeropuerto.**
- El AIFA será responsable de que el aeropuerto cuente con los servicios aeroportuarios y complementarios que se requieran, de acuerdo con su clasificación, clave de referencia y categoría.

- El AIFA podrá prestar los servicios complementarios directamente, siempre que lo realice en forma eficiente, equitativa y no discriminatoria, frente a los concesionarios o permisionarios del servicio de transporte aéreo u otros terceros prestadores de estos servicios en el Aeropuerto.
- El AIFA estará obligada a identificar y registrar, de manera independiente, las operaciones, los costos e ingresos relacionados con los servicios complementarios que preste.
- En todo caso, el AIFA deberá llevar a cabo los actos necesarios a efecto de contar con opciones competitivas para la prestación de cada uno de los servicios complementarios.
- El AIFA únicamente podrá limitar el número de prestadores de servicios complementarios por razones de disponibilidad de espacio, eficiencia operativa y seguridad, lo anterior después de escuchar la opinión del Comité de Operación y Horarios del Aeropuerto, y previa aprobación de la Secretaría de Comunicaciones y Transportes.
- Deberá integrar el Comité de Operación y Horarios del Aeropuerto.
- En aquellos casos en que el AIFA limite el número de prestadores de servicios complementarios conforme al párrafo anterior, los contratos necesarios para permitir que los concesionarios y permisionarios del transporte aéreo o terceros ajenos a éstos presten los servicios complementarios que sean requeridos en el Aeropuerto, serán adjudicados a favor de aquellas personas que ofrezcan las mejores condiciones para una operación eficiente y segura del Aeropuerto, así como la mejor calidad y precio para los usuarios.
- El AIFA, con la participación de los concesionarios y permisionarios del servicio de transporte aéreo, establecerá los criterios, las reglas generales para las adjudicaciones, y en su caso, los procedimientos de los concursos y llevará a cabo los mismos.
- El AIFA podrá, de manera enunciativa más no limitativa, prestar los servicios de transporte, almacenamiento, distribución, suministro, succión o expendio de combustible a los operadores, concesionarios y permisionarios del servicio de transporte aéreo, usuarios del Aeropuerto a que se refiere la presente condición podrán ser prestados por terceros, de forma segura y eficiente.
- **Para la prestación de ese servicio, el AIFA celebrará los contratos necesarios en los que se establecerán los términos y condiciones para que dichos servicios se presten de manera segura y eficiente, precisando la contraprestación y forma de pago correspondiente por el acceso y el uso de sus instalaciones para la prestación del servicio de combustible en el Aeropuerto, pero en materia de daños que ocasione la prestación del servicio de combustible, serán responsables.**
- Todos los conflictos que surjan con motivo de la prestación de los servicios de combustible serán resueltos por aquellas autoridades competentes de conformidad con la normatividad aplicable.
- Que, para el caso de los servicios comerciales, estos podrán ser prestados directamente por el AIFA o por terceros que contrate la misma, mediante el arrendamiento de áreas, incluyendo,

sin limitar: áreas para comercios, restaurantes, arrendamiento de vehículos, publicidad, correo, casas de cambio, bancos y hoteles.

- En ningún caso la prestación de servicios comerciales debe constituir un obstáculo para la prestación de servicios aeroportuarios y complementarios, ni podrá poner en peligro la seguridad del Aeropuerto o la operación de las aeronaves, ya que en caso de que esto ocurra, la Secretaría de Infraestructura, Comunicaciones y Transportes ordenará las adecuaciones necesarias.

Ahora bien, el artículo 8 de la Ley General prevé que la aplicación e interpretación se realizará conforme a lo dispuesto en la Constitución, los Tratados Internacionales de los que el Estado mexicano sea parte, así como las resoluciones y sentencias vinculantes que emitan los órganos nacionales e internacionales especializados, favoreciendo en todo tiempo el derecho a la privacidad, la protección de datos personales y a las personas la protección más amplia. Y en el caso de la interpretación, se pueden tomar en cuenta los criterios, determinaciones y opiniones de los organismos nacionales e internacionales, en materia de protección de datos personales.

En el caso de la interpretación, dicho precepto permite efectuarla conforme al a lo dispuesto en la Constitución, los Tratados Internacionales de los que el Estado mexicano sea parte, así como las resoluciones y sentencias vinculantes que emitan los órganos nacionales e internacionales especializados, así como podrá complementarse lo previsto en criterios, determinaciones y opiniones de los organismos nacionales e internacionales, en materia de protección de datos personales.

Atento a esa regla, y para puntualizar los alcances del principio de licitud, se tiene que el Convenio 108, referente al principio que nos ocupa, señala lo siguiente:

> *"[…]*
> *Artículo 2 - Definiciones*
> *Para los efectos del presente Convenio:*
> *a. "datos de carácter personal" significa cualquier información relativa a una persona física identificada o identificable ("persona concernida");*
> *[…]*
> *c. "tratamiento automatizado" incluye las operaciones que a continuación se indican efectuadas en su totalidad o en parte con ayuda de procedimientos automatizados: registro de datos, aplicación a esos datos de operaciones lógicas y/o aritméticas, su modificación, borrado, extracción o difusión;*
> *[…]*
> *Artículo 3 - Ámbito de aplicación*
> *1. Las Partes se comprometen a aplicar el presente Convenio a los ficheros y a los tratamientos automatizados de datos de carácter personal en los sectores público y privado.*

[...]
Artículo 5 - Calidad de los datos
Los datos de carácter personal que sean objeto de tratamiento automatizado:
a. se obtendrán y tratarán justa y legalmente;
[...]
Artículo 6 - Categorías particulares de datos
Los datos de carácter personal que revelen el origen racial, las opiniones políticas, las creencias religiosas u otras convicciones, así como los datos de carácter personal relativos a la salud o a la vida sexual, no podrán tratarse automáticamente a menos que la legislación interna prevea garantías apropiadas. La misma norma regirá en el caso de datos de carácter personal referentes a sentencias penales.
[...]
Artículo 9 - Excepciones y restricciones
[...]
2. Será posible una excepción a lo dispuesto en los artículos 5, 6 y 8 del presente Convenio cuando tal excepción, prevista por la legislación de la Parte, constituya una medida necesaria en una sociedad democrática para:
a. la protección de la seguridad del Estado, de la seguridad pública, para los intereses monetarios del Estado o para la represión de infracciones penales;
b. la protección de la persona concernida y de los derechos y libertades de otras personas.
[...]"

Sobre el principio que nos ocupa, el instrumento normativo en estudio prevé que los estados parte se comprometen para aplicarlo a los ficheros y a los tratamientos automatizados de datos de carácter personal en los sectores público y privado, esto al considerar que los datos de carácter personal que sean objeto de tratamiento automatizado se obtendrán y tratarán justa y legalmente.

Igualmente, se establece que los datos de carácter personal que revelen el origen racial, las opiniones políticas, las creencias religiosas u otras convicciones, así como los datos de carácter personal relativos a la salud o a la vida sexual, no podrán tratarse automáticamente a menos que la legislación interna prevea garantías apropiadas. La misma norma regirá en el caso de datos de carácter personal referentes a sentencias penales.

Desde ese instrumento normativo, se advierte una previsión sobre el tratamiento de los datos personales es que este debe ser justo y legal, así como para el caso de los datos personales sensibles señala puntualmente que estos no deben ser objeto de tratamientos automatizados, esto es, no deben ser sometidos al registro de datos, aplicación a esos datos de operaciones lógicas y/o aritméticas, su modificación, borrado, extracción o difusión. Sin embargo, es excepción a esa regla que la legislación interna prevea garantías apropiadas para esos tratamientos.

Dicha excepción debe descansar, al menos, en los siguientes supuestos:

- La protección de la seguridad del Estado, de la seguridad pública, para los intereses monetarios del Estado o para la represión de infracciones penales,
- La protección de la persona concernida y de los derechos y libertades de otras personas.

En ese sentido, se advierte que en el Convenio 108 se establecen las condiciones bajo las cuales pueden tratarse datos personales de carácter sensible, pero estas deben estar establecidas en la normatividad bajo los parámetros de protección de la seguridad del estado, la seguridad pública, los intereses monetarios, la represión de infracciones penales o la protección de la persona concernida y de los derechos y libertades de otras personas.

Sin embargo, este Instituto considera que es posible ampliar aún más los alcances de la interpretación del principio que nos ocupa, por medio de dos determinaciones adoptadas en materia de protección de datos personales que, si bien no tienen el carácter de resolución adoptada por un Tribunal o un tratado internacional en materia del derecho humano a la protección de datos personales, son útiles para ampliar el análisis sobre el principio que nos ocupa.

Así, los "Principios actualizados del Comité Jurídico Interamericano sobre la privacidad y la protección de datos personales"[46], establecen sobre las excepciones del seguimiento de los principios, lo subsecuente:

> *"[…]*
> *PRINCIPIO DOCE:*
> *EXCEPCIONES*
> *Cualquier excepción a alguno de estos Principios debería estar prevista de manera expresa y específica en la legislación nacional, ser puesta en conocimiento del público y limitarse únicamente a motivos relacionados con la soberanía nacional, la seguridad nacional, la seguridad pública, la protección de la salud pública, el combate a la criminalidad, el cumplimiento de normativas u otras prerrogativas de orden público o el interés público.*
> *[…]"*

Si bien dicho instrumento no es de carácter vinculante al tratarse de un documento emitido por el Comité Jurídico Interamericano, que es un cuerpo consultivo de la Organización de los Estados Americanos (OEA), en asuntos jurídicos encargado de promover el desarrollo progresivo y la codificación del derecho internacional y de estudiar la posibilidad de uniformar las legislaciones de los países del Continente[47], se trata de un instrumento orientador para establecer los alcances del principio de licitud.

---

[46] Disponible en el vínculo https://www.oas.org/es/sla/cji/docs/CJI-doc_638-21.pdf, consultado por última vez el 28/02/2023.
[47] Disponible en el vínculo https://www.oas.org/es/sla/cji/, consultado por última vez el 28/02/2023.

Lo anterior es importante, ya que las excepciones al seguimiento de los principios deben estar establecida en la Ley, pero dicha reserva de Ley debe ser puesta en conocimiento del público y limitarse únicamente a motivos relacionados con la soberanía nacional, seguridad nacional, seguridad pública, protección de la salud pública, combate a la criminalidad, cumplimiento de normativas u otras prerrogativas de orden público o interés público, esto es, no basta con que la excepción se encuentre en la Ley, pues debe responder a la protección de ciertos bienes jurídicos concretos, como lo son: soberanía nacional, seguridad nacional, seguridad pública, protección de la salud pública, combate a la criminalidad, cumplimiento de normativas u otras prerrogativas de orden público o el interés público.

En esa misma línea, los Estándares de Protección de Datos Personales[48] amplían las previsiones sobre el principio de licitud en relación con las limitaciones del tratamiento:

> *"[…]*
> *6.1. La legislación nacional de los Estados Iberoamericanos aplicable en la materia podrá limitar el derecho a la protección de datos para salvaguardar la seguridad nacional, la seguridad pública, la protección de la salud pública, la protección de los derechos y las libertades de terceros, así como por cuestiones de interés público.*
> *6.2. Las limitaciones y restricciones serán reconocidas de manera expresa en ley, con el propósito de brindar certeza suficiente a los titulares acerca de la naturaleza y alcances de la medida.*
> *6.3. Cualquier ley que tenga como propósito limitar el derecho a la protección de datos personales contendrá, como mínimo, disposiciones relativas a:*
> *a. La finalidad del tratamiento.*
> *b. Las categorías de datos personales de que se trate.*
> *c. El alcance de las limitaciones establecidas.*
> *d. Las garantías adecuadas para evitar accesos o transferencias ilícitas o desproporcionadas.*
> *e. La determinación del responsable o responsables.*
> *f. Los plazos de conservación de los datos personales.*
> *g. Los posibles riesgos para los derechos y libertades de los titulares.*
> *h. El derecho de los titulares a ser informados sobre la limitación, salvo que resulte perjudicial o incompatible a los fines de ésta.*
> *6.4. Las leyes serán las necesarias, adecuadas y proporcionales en una sociedad democrática, y deberán respetar los derechos y las libertades fundamentales de los titulares.*
> *[…]*
> *14. Principio de licitud*
> *14.1. El responsable tratará los datos personales en su posesión con estricto apego y cumplimiento de lo dispuesto por el derecho interno del Estado Iberoamericano que resulte aplicable, el derecho internacional y los derechos y libertades de las personas.*

[48] Disponibles para su consulta en https://www.redipd.org/sites/default/files/inline-files/Estandares_Esp_Con_logo_RIPD.pdf, consultados por última vez el 28/02/2023.

14.2. El tratamiento de datos personales que realicen las autoridades públicas se sujetará a las facultades o atribuciones que el derecho interno del Estado Iberoamericano de que se trate les confiera expresamente, además de lo previsto en el numeral anterior de los presentes Estándares.
[…]"

Los estándares que nos ocupan establecen que el principio de licitud comprende que el responsable tratará los datos personales en su posesión con estricto apego y cumplimiento de lo dispuesto por el derecho interno el derecho internacional y los derechos y libertades de las personas. Sobre las entidades estatales, puntualiza que se sujetará a las facultades o atribuciones que el derecho interno del Estado Iberoamericano de que se trate les confiera expresamente.

Sobre este punto, resulta ilustrativo que en la Guía para el tratamiento de datos biométricos[49]se vincula el uso de datos biométricos con el principio en estudio, de la siguiente manera:

"[…]
De conformidad con este principio, los datos personales deberán tratarse con apego y cumplimiento a lo dispuesto por la legislación mexicana y el derecho internacional.
En el caso de los sujetos obligados, de manera adicional, el tratamiento de los datos personales que éstos realicen deberá sujetarse a las facultades o atribuciones que la normativa aplicable les confiera.
[…]
Recomendaciones específicas para el principio de licitud en el tratamiento de datos biométricos
• Conocer la normatividad que en lo específico regula y aplica a la actividad en la que son tratados los datos biométricos, a fin de verificar que la misma prevea el uso de este tipo de datos y en qué términos lo hace, o bien, que la misma no lo prohíba.
• Revisar las atribuciones que facultan al sujeto obligado para tratar datos biométricos, o bien, en el caso de los responsables del sector privado, analizar si el uso de los datos biométricos está debidamente justificado según la finalidad de la que se trate.
[…]"

Fundamento jurídico del tratamiento de datos señalados por el AIFA.

De forma previa al análisis del tratamiento que pretende efectuar el AIFA respecto al Sistema de Procesamiento, es oportuno recordar que en el artículo 1, párrafo segundo, de la Constitución Política de los Estados Unidos Mexicanos establece que las normas relativas a los derechos humanos se interpretarán de conformidad con dicho ordenamiento y con los tratados internacionales de la materia favoreciendo en todo tiempo a las personas la protección más amplia.

[49] Disponible para su consulta en el vínculo: https://home.inai.org.mx/wp-content/documentos/DocumentosSectorPublico/GuiaDatosBiometricos_Web_Links.pdf, consultado por última vez el 28/02/2023.

En el diverso 133, se estableció que la Constitución, las leyes del Congreso de la Unión que emanen de ella y todos los tratados que estén de acuerdo con la misma, celebrados y que se celebren por el Presidente de la República, con aprobación del Senado, serán la Ley Suprema de toda la Unión.

Por su parte, en el artículo 8 de la Ley General se prevé que para su aplicación e interpretación se realizará conforme a lo dispuesto en la Constitución Política de los Estados Unidos Mexicanos, los Tratados Internacionales de los que el Estado mexicano sea parte, así como las resoluciones y sentencias vinculantes que emitan los órganos nacionales e internacionales especializados, favoreciendo en todo tiempo el derecho a la privacidad, la protección de datos personales y a las personas la protección más amplia. Para el caso de la interpretación, se podrán tomar en cuenta los criterios, determinaciones y opiniones de los organismos nacionales e internacionales, en materia de protección de datos personales.

En suma, este Instituto advierte que para la correcta identificación del tratamiento de datos personales efectuado a nivel normativo se debe atender no únicamente a las normas de derecho interno, también debe considerarse aquellas normas de derecho internacional que regulen esa actuación, pues al tratarse de un derecho humano, la aplicación e interpretación debe ser integral y garantizando a las personas la protección más amplia.

Establecido lo anterior, es importante traer a colación lo manifestado respecto de este principio en la Evaluación de Impacto presentada por el AIFA, en la cual fue señalado lo siguiente:

> *"[…]*
> ***IV. Fundamento legal del sistema.***
> *El fundamento legal para que el AIFA implemente el uso de los sistemas biométricos es:*
> ***1. Programa Institucional 2021-2024 de la Empresa de Participación Estatal Mayoritaria Aeropuerto Internacional Felipe Ángeles, S.A. de C.V.,*** *https://dof.gob.mx/nota_detalle.php?codigo=5636590&fecha=29/11/2021#gsc.t ab=0 6.-* ***Objetivos Prioritarios***
> ***6.1 Relevancia del Objetivo Prioritario 1.-*** *Contribuir al desarrollo de la industria aeroportuaria del País a través de la eficiente administración de los recursos humanos, materiales, financieros y de tecnologías de la Información del Aeropuerto Internacional Felipe Ángeles, en apego a los más altos niveles de valores y normativa establecida por la Administración Pública Federal.*
> *"… Las TIC's en muy poco tiempo han experimentado significativos cambios, con equipos y programas que simplifican los procesos y economizan los recursos; en este contexto, las instalaciones y equipos de la entidad sin duda están en un nivel competitivo y se cuenta con*

recursos humanos de gran experiencia; sin embargo, se requiere de una actualización constante y capacitación permanente que acompañe el acelerado cambio de las TIC's.
El empleo de las TIC's, también requiere de nuevas capacidades y competencias para usar y adaptar tecnologías, para generar y gestionar el conocimiento y su aplicación ante los cambios vertiginosos, generando nuevos paradigmas que respondan a las necesidades del sector aeroportuario..."
6.3 Relevancia del Objetivo Prioritario 3.- *Brindar servicios aeroportuarios con calidad y disponibilidad en beneficio de los clientes y usuarios. "...Para la operación del Aeropuerto Internacional "Felipe Ángeles", se espera contar con una infraestructura de comunicación y transporte, para ofrecer un servicio de excelente calidad y que opere de forma exitosa durante el transcurso de los años..."*
7.- Estrategias prioritarias y Acciones puntuales.
Estrategia Prioritaria 1.3.- *Fomentar la participación de los usuarios de los servicios del AIFA., a través del uso de las TIC's.*
2. Artículo 74 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados Cuando el responsable pretenda poner en operación o modificar políticas públicas, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que a sus juicio y de conformidad con esta ley impliquen el tratamiento intensivo o relevante de datos personales deberá realizar una evaluación de impacto en la protección de datos personales y presentarla ante el Instituto o los organismos garantes según corresponda los cuales podrán emitir recomendaciones no vinculantes especializadas en la materia de datos personales.
3. Ley de Aviación Civil
Artículo 47 Bis 4. *Los pasajeros deberán:*
I. Brindar al permisionario o concesionario información y datos personales veraces, al momento de la compra del boleto;
II. Presentar documentos oficiales de identificación, a solicitud del permisionario o concesionario o del personal autorizado del aeropuerto;
III. Acatar las normas de seguridad y operación aeroportuarias vigentes;
IV. Ocupar el asiento asignado, a menos que la tripulación por un requerimiento justificado le solicite o le autorice ocupar uno distinto, y
V. Las demás que establezcan la Ley y demás ordenamientos.
4. Ley de Aeropuertos.
ARTICULO 46. *Corresponderá a los concesionarios o permisionarios, conforme a las disposiciones aplicables y con base en el título de concesión o permiso respectivo, asegurar que los aeródromos civiles cuenten con la infraestructura, instalaciones, equipo, señalización, módulo de primeros auxilios y emergencias médicas, servicios y sistemas de organización, adecuados y suficientes para que la operación y atención al usuario se lleve a cabo sobre bases de seguridad, eficiencia y calidad.*
ARTICULO 47. *Los concesionarios o permisionarios deberán responsabilizarse del control de los accesos y tránsito de personas, vehículos y bienes en zonas restringidas del aeródromo civil, así como de que las áreas cercanas a los equipos de ayuda a la navegación aérea*

instalados dentro de los mismos, se mantengan libres de obstáculos que puedan afectar su operación.

5. Reglamento de la Ley de Aeropuertos

ARTÍCULO 152. *fracciones I, II, III y V. Tratándose de aeródromos de servicio al público, las medidas de seguridad deberán comprender lo siguiente:*

I. Los dispositivos de protección y control de accesos a las zonas restringida y estéril;

II. Las medidas de acceso y de control del movimiento de personas y vehículos en las zonas restringidas;

6. OACI

Anexo 17 *al Convenio sobre Aviación Civil Internacional, Seguridad, Protección de la aviación civil internacional contra los actos de interferencia ilícita.*

CAPÍTULO 3. ENTRADA Y SALIDA DE PERSONAS Y DE SU EQUIPAJE

C. Seguridad de los documentos de viaje.

3.7 *Los Estados contratantes actualizarán regularmente los elementos de seguridad que figuran en las nuevas versiones de sus documentos de viaje, a fin de impedir su uso indebido y facilitar la detección en los casos en que dichos documentos se hayan alterado, duplicado o emitido en forma ilegal.*

3.8 *Los Estados contratantes establecerán controles con respecto a la creación y expedición de los documentos de viaje a fin de protegerse contra el robo de sus inventarios y el apoderamiento indebido de documentos de viaje recientemente emitidos.*

3.9 Método recomendado. *Los Estados contratantes deberían incorporar datos biométricos en sus pasaportes, visados y otros documentos de viaje oficiales de lectura mecánica, utilizando una o más de las técnicas de almacenamiento de datos optativos para suplementar la zona de lectura mecánica, según se especifica en el Doc 9303, Documentos de viaje de lectura mecánica. Los datos requeridos almacenados en un microcircuito integrado son los mismos que se imprimen en la página de datos; o sea, los datos contenidos en la zona de lectura mecánica más la imagen fotográfica digitalizada. Los Estados contratantes que deseen suplementar la imagen facial con otro elemento biométrico en el pasaporte pueden utilizar imágenes de las impresiones digitales o del iris. Los Estados contratantes que incorporen datos biométricos en sus pasaportes de lectura mecánica deben almacenar los datos en un microcircuito integrado sin contacto que cumpla con la norma ISO/IEC 14443 y esté programado de conformidad con la estructura lógica de datos establecida por la OACI.*

I. Inspección de documentos de viaje

3.35.1 *Las autoridades competentes de cada Estado contratante se incautarán de los documentos de viaje fraudulentos, falsificados o imitados. Las autoridades competentes también se incautarán de los documentos de viaje de una persona que se presenta pretendiendo ser el titular legítimo del documento de viaje. Tales documentos se retirarán de la circulación inmediatamente y se devolverán a las autoridades competentes del Estado que figura como expedidor o a la misión diplomática residente de ese Estado.*

7. Política *Se han establecido Políticas Internas de la Subdirección de Sistemas y para el Sistema de Procesamiento de Pasajeros. Actualmente no existe un presupuesto en específico asignado para este fin."*

En concordancia con lo anterior, es menester indicar que, en el desahogo del requerimiento de información adicional respecto al cumplimiento de este principio, específicamente por lo que hace a los puntos 3 y 12, se refirió lo siguiente:

"3. […]

El marco normativo que sustenta la implementación de "Sistema De Procesamiento De Pasajeros", por el AIFA (Anexo 1)

• Constitución política de los Estados Unidos Mexicanos artículos 6 fracción II y 16. https://www.diputados.gob.mx/LeyesBiblio/pdf/CPEUM.pdf

• Convenio Internacional en materia de datos personales (108) en materia de datos personales. https://www.clarkemodet.com/news-posts/mexicoy-el-convenio-108-de-europa-sobre-proteccion-de-datos-personales-anivelinternacional/#:~:text=El%20Convenio%20108%20tiene%20como,de%20una%20autoridad%20responsable%20de

• La Adhesión de México al Convenio Internacional en materia de protección de datos personales, firmado el 13 de junio 2018 de la LGPDPPSO. https://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPPSO.pdf

1. Programa Institucional 2021-2024 de la Empresa de Participación Estatal Mayoritaria Aeropuerto Internacional Felipe Ángeles, S.A. de C.V., *https://dof.gob.mx/nota_detalle.php?codigo=5636590&fecha=29/11/2021#gsc.t ab=0 6.-* ***Objetivos Prioritarios***

6.1 Relevancia del Objetivo Prioritario 1.- *Contribuir al desarrollo de la industria aeroportuaria del País a través de la eficiente administración de los recursos humanos, materiales, financieros y de tecnologías de la Información del Aeropuerto Internacional Felipe Ángeles, en apego a los más altos niveles de valores y normativa establecida por la Administración Pública Federal.*

[…] Las TIC's en muy poco tiempo han experimentado significativos cambios, con equipos y programas que simplifican los procesos y economizan los recursos; en este contexto, las instalaciones y equipos de la entidad sin duda están en un nivel competitivo y se cuenta con recursos humanos de gran experiencia; sin embargo, se requiere de una actualización constante y capacitación permanente que acompañe el acelerado cambio de las TIC's.

El empleo de las TIC's, también requiere de nuevas capacidades y competencias para usar y adaptar tecnologías, para generar y gestionar el conocimiento y su aplicación ante los cambios vertiginosos, generando nuevos paradigmas que respondan a las necesidades del sector aeroportuario..."

6.3 Relevancia del Objetivo Prioritario 3.- *Brindar servicios aeroportuarios con calidad y disponibilidad en beneficio de los clientes y usuarios. "...Para la operación del Aeropuerto Internacional "Felipe Ángeles", se espera contar con una infraestructura de comunicación y transporte, para ofrecer un servicio de excelente calidad y que opere de forma exitosa durante el transcurso de los años..."*

7.- Estrategias prioritarias y Acciones puntuales.

Estrategia Prioritaria 1.3.- *Fomentar la participación de los usuarios de los servicios del AIFA., a través del uso de las TIC's.*

2. Artículo 74 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados Cuando el responsable pretenda poner en operación o modificar políticas públicas, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que a sus juicio y de conformidad con esta ley impliquen el tratamiento intensivo o relevante de datos personales deberá realizar una evaluación de impacto en la protección de datos personales y presentarla ante el Instituto o los organismos garantes según corresponda los cuales podrán emitir recomendaciones no vinculantes especializadas en la materia de datos personales.

3. Ley de Aviación Civil

Artículo 47 Bis 4. *Los pasajeros deberán:*

I. Brindar al permisionario o concesionario información y datos personales veraces, al momento de la compra del boleto;

II. Presentar documentos oficiales de identificación, a solicitud del permisionario o concesionario o del personal autorizado del aeropuerto;

III. Acatar las normas de seguridad y operación aeroportuarias vigentes;

IV. Ocupar el asiento asignado, a menos que la tripulación por un requerimiento justificado le solicite o le autorice ocupar uno distinto, y

V. Las demás que establezcan la Ley y demás ordenamientos.

4. Ley de Aeropuertos.

ARTICULO 46. *Corresponderá a los concesionarios o permisionarios, conforme a las disposiciones aplicables y con base en el título de concesión o permiso respectivo, asegurar que los aeródromos civiles cuenten con la infraestructura, instalaciones, equipo, señalización, módulo de primeros auxilios y emergencias médicas, servicios y sistemas de organización, adecuados y suficientes para que la operación y atención al usuario se lleve a cabo sobre bases de seguridad, eficiencia y calidad.*

ARTICULO 47. *Los concesionarios o permisionarios deberán responsabilizarse del control de los accesos y tránsito de personas, vehículos y bienes en zonas restringidas del aeródromo civil, así como de que las áreas cercanas a los equipos de ayuda a la navegación aérea instalados dentro de los mismos, se mantengan libres de obstáculos que puedan afectar su operación.*

5. Reglamento de la Ley de Aeropuertos

ARTÍCULO 152, *fracciones I, II, III y V. Tratándose de aeródromos de servicio al público, las medidas de seguridad deberán comprender lo siguiente:*

I. Los dispositivos de protección y control de accesos a las zonas restringida y estéril;

II. Las medidas de acceso y de control del movimiento de personas y vehículos en las zonas restringidas;

6. OACI

Anexo 17 *al Convenio sobre Aviación Civil Internacional, Seguridad, Protección de la aviación civil internacional contra los actos de interferencia ilícita.*

CAPÍTULO 3. ENTRADA Y SALIDA DE PERSONAS Y DE SU EQUIPAJE

C. Seguridad de los documentos de viaje.

3.7 *Los Estados contratantes actualizarán regularmente los elementos de seguridad que figuran en las nuevas versiones de sus documentos de viaje, a fin de impedir su uso indebido y facilitar la detección en los casos en que dichos documentos se hayan alterado, duplicado o emitido en forma ilegal.*

3.8 *Los Estados contratantes establecerán controles con respecto a la creación y expedición de los documentos de viaje a fin de protegerse contra el robo de sus inventarios y el apoderamiento indebido de documentos de viaje recientemente emitidos.*

3.9 Método recomendado. *Los Estados contratantes deberían incorporar datos biométricos en sus pasaportes, visados y otros documentos de viaje oficiales de lectura mecánica, utilizando una o más de las técnicas de almacenamiento de datos optativos para suplementar la zona de lectura mecánica, según se especifica en el Doc 9303, Documentos de viaje de lectura mecánica. Los datos requeridos almacenados en un microcircuito integrado son los mismos que se imprimen en la página de datos; o sea, los datos contenidos en la zona de lectura mecánica más la imagen fotográfica digitalizada. Los Estados contratantes que deseen suplementar la imagen facial con otro elemento biométrico en el pasaporte pueden utilizar imágenes de las impresiones digitales o del iris. Los Estados contratantes que incorporen datos biométricos en sus pasaportes de lectura mecánica deben almacenar los datos en un microcircuito integrado sin contacto que cumpla con la norma ISO/IEC 14443 y esté programado de conformidad con la estructura lógica de datos establecida por la OACI.*

I. Inspección de documentos de viaje

3.35.1 *Las autoridades competentes de cada Estado contratante se incautarán de los documentos de viaje fraudulentos, falsificados o imitados. Las autoridades competentes también se incautarán de los documentos de viaje de una persona que se presenta pretendiendo ser el titular legítimo del documento de viaje. Tales documentos se retirarán de la circulación inmediatamente y se devolverán a las autoridades competentes del Estado que figura como expedidor o a la misión diplomática residente de ese Estado.*

6. LEY DE CIENCIA Y TECNOLOGIA

Capítulo 1 • Articulo 1: La presente Ley es reglamentaria de la fracción V del artículo 3 de la Constitución política de los Estados Unidos Mexicanos, y tiene por objetivo: Regular los apoyos que el Gobierno Federal está obligado a otorgar para impulsar, fortalecer, desarrollar y consolidar la investigación científica, el desarrollo tecnológico y la innovación en general en el país.

Adicionalmente, el fundamento legal que sustenta la implementación del" Sistema De Procesamiento De Pasajeros", por el AIFA, es el siguiente:

Con fecha 15 de octubre del 2021 fue publicado en el Diario Oficial de la Federación el TÍTULO de Concesión que otorga la Secretaría de Comunicaciones y Transportes, a favor de la Empresa de Participación Estatal Mayoritaria Aeropuerto Internacional Felipe Ángeles, S.A. de C.V. "CONCESIÓN QUE OTORGA EL GOBIERNO FEDERAL, POR CONDUCTO DE LA SECRETARÍA DE COMUNICACIONES Y TRANSPORTES, REPRESENTADA POR SU TITULAR EL ING. JORGE ARGANIS DÍAZ LEAL, A FAVOR DE LA SOCIEDAD DENOMINADA AEROPUERTO INTERNACIONAL FELIPE ÁNGELES, S.A. DE C.V.

EMPRESA DE PARTICIPACIÓN ESTATAL MAYORITARIA DE NACIONALIDAD MEXICANA, REPRESENTADA POR SU DIRECTOR GENERAL EL GENERAL DE BRIGADA D.E.M. RENÉ TRUJILLO MIRANDA; A QUIENES EN LO SUCESIVO SE LES DENOMINARÁ LA "SECRETARÍA" Y LA "CONCESIONARIA", RESPECTIVAMENTE.

I. El Plan Nacional de Desarrollo 2019 2024, publicado en el Diario Oficial de la Federación ("DOF") el 12 de julio de 2019, establece en su Estrategia Nacional de Seguridad Pública entre otros, los siguientes objetivos: garantizar empleo, educación, salud y bienestar mediante la creación de puestos de trabajo, el cumplimiento del derecho de todos los jóvenes del país a la educación superior, la inversión en infraestructura y servicios de salud y por medio de los programas regionales, sectoriales y coyunturales de desarrollo a través del Aeropuerto "Felipe Ángeles" en Santa Lucía. En la Estrategia Política y Gobierno del Plan Nacional de Desarrollo 2019 2024, se prevé garantizar empleo, educación, salud y bienestar mediante la creación de puestos de trabajo, el cumplimiento del derecho de todos los jóvenes del país a la educación superior, la inversión en infraestructura y servicios de salud y por medio de los programas regionales, sectoriales y coyunturales de desarrollo, entre otros, el Aeropuerto "Felipe Ángeles" en Santa Lucía.

V. "LA CONCESIONARIA" es una empresa de participación estatal mayoritaria, cuya estructura accionaria está conformada con un 99% propiedad de la Secretaría de la Defensa Nacional y con un 1% propiedad del Banco Nacional del Ejército, Fuerza Aérea y Armada, S.N.C., tal y como consta en la Resolución por la que se autoriza la constitución de una Empresa de Participación Estatal Mayoritaria denominada Aeropuerto Internacional Felipe Ángeles, S.A. de C.V., misma que estará agrupada en el sector coordinado por la Secretaría de la Defensa Nacional, publicada en el Diario Oficial de la Federación el 14 de diciembre de 2020."

Siendo misión de la Subdirección de sistemas garantizar la infraestructura y los servicios de tecnologías de la información y comunicaciones al Aeropuerto Internacional Felipe Ángeles.

Y atendiendo las funciones del área como:

Supervisar que las comunicaciones, sistemas de operación aeroportuaria, administrativos, financieros y comercias, equipos de cómputo, sistemas de CCTV y control de Acceso, megafonía y Servicios de correo, internet y antivirus operan eficientemente a fin de apoyar la productividad del AIFA.

Se anexa Manual de Organización General - octubre 2021

12. […]

El principio de licitud está agotado en el punto 3 de este documento, ya que en dicho documento se encuentra toda la normatividad que rige la actividad del AIFA S.A. de C.V. para estar en posibilidades de efectuar el tratamiento de datos personales en su calidad de responsable de operación aeroportuaria

[…]"

Como se advierte, el AIFA señala que el fundamento jurídico para el Sistema de Procesamiento parte de la Constitución, específicamente en los artículos 6°, apartado A, fracción I, y 16, en la cual

se establece que la información que se refiere a la vida privada y los datos personales será protegida en los términos y con las excepciones que fijen las leyes, ya que toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley de la materia, la cual establece los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros.

Indica que también resulta aplicable el Convenio 108, así como su ratificación posterior, en el cual se advierten las reglas generales de tratamiento de datos personales, y si bien es un instrumento ratificado para efectos de su aplicación en territorio nacional, lo cierto es que el AIFA no señaló puntualmente los preceptos legales en los que descansa el recabo de datos biométricos para fines del Sistema de Procesamiento.

Igualmente, precisa que dentro del Programa Institucional del AIFA, dentro de sus objetivos 6.1, 6.3 y 7, se establece lo siguiente:

- Contribuir al desarrollo de la industria aeroportuaria del País a través de la eficiente administración de los recursos humanos, materiales, financieros y de tecnologías de la Información del Aeropuerto Internacional Felipe Ángeles, en apego a los más altos niveles de valores y normativa establecida por la Administración Pública Federal.
- Brindar servicios aeroportuarios con calidad y disponibilidad en beneficio de los clientes y usuarios, esperando contar con una infraestructura de comunicación y transporte, para ofrecer un servicio de excelente calidad y que opere de forma exitosa durante el transcurso de los años.
- Fomentar la participación de los usuarios de los servicios del AIFA., a través del uso de las TIC's.

Sobre tal punto, conforme a lo referido por el AIFA, en términos de los artículos 9, 16, fracción VI y 17, fracción II, de la Ley de Planeación[50], así como los diversos 46, 47, 48 de la Ley de Entidades Paraestatales[51] y 15 y 22 de su Reglamento[52], se establece, dentro de las disposiciones de la Ley de Planeación, que las entidades de la Administración Pública Federal, como es el caso del AIFA, deberán planear y conducir sus actividades con perspectiva intercultural, de género y con sujeción a los objetivos y prioridades de la planeación nacional de desarrollo, a fin de cumplir con la

[50] Publicada en el Diario Oficial de la Federación el 5 de enero de 1983, cuyo texto puede obtenerse del vínculo siguiente: https://www.diputados.gob.mx/LeyesBiblio/pdf/59_160218.pdf, consultado por última vez el 28/02/2023.
[51] Publicada en el Diario Oficial de la Federación el 14 de mayo de 1986, cuyo texto puede obtenerse del vínculo siguiente: https://www.diputados.gob.mx/LeyesBiblio/pdf/LFEP.pdf, consultado por última vez el 28/02/2023.
[52] Publicado en el Diario Oficial de la Federación el 26 de enero de 1990, cuyo texto puede obtenerse del vínculo siguiente: https://www.diputados.gob.mx/LeyesBiblio/regley/Reg_LFEP.pdf, consultado por última vez el 28/02/2023.

obligación del Estado de garantizar que éste sea equitativo, incluyente, integral, sustentable y sostenible, de lo cual la Secretaría de Hacienda y Crédito Público realizará la vigilancia correspondiente.

Para el caso concreto de las entidades, dicho ordenamiento puntualiza que deben elaborar sus respectivos programas institucionales atendiendo, además de las disposiciones aplicables, a las previsiones contenidas en el programa sectorial correspondiente observando en lo conducente las variables ambientales, económicas, sociales y culturales respectivas.

Aunado a lo expuesto, la Ley de Entidades Paraestatales, así como su Reglamento, especifica sobre dichas entidades:

- Sus objetivos se ajustarán a los programas sectoriales que formule la Coordinadora de Sector, y en todo caso, contemplarán: la referencia concreta a su objetivo esencial y a las actividades conexas para lograrlo; los productos que elabore o los servicios que preste y sus características sobresalientes; los efectos que causen sus actividades en el ámbito sectorial, así como el impacto regional que originen; y los rasgos más destacados de su organización para la producción o distribución de los bienes y prestación de servicios que ofrece.
- Para su desarrollo y operación, deberán sujetarse a la Ley de Planeación, al Plan Nacional de Desarrollo, a los programas sectoriales que se deriven del mismo y a las asignaciones de gasto y financiamiento autorizadas. Dentro de tales directrices las entidades formularán sus programas institucionales a corto, mediano y largo plazos.
- El Programa Institucional constituye la asunción de compromisos en términos de metas y resultados que debe alcanzar la entidad paraestatal. La programación institucional de la entidad, en consecuencia, deberá contener la fijación de objetivos y metas, los resultados económicos y financieros esperados, así como las bases para evaluar las acciones que lleve a cabo; la definición de estrategias y prioridades; la previsión y organización de recursos para alcanzarlas; la expresión de programas para la coordinación de sus tareas, así como las previsiones respecto a las posibles modificaciones a sus estructuras.
- Los titulares de las entidades paraestatales, con el objeto de garantizar que la conducción de éstas se sustente en criterios de eficiencia, eficacia y productividad, y de alcanzar las metas y objetivos de los programas institucionales respectivos, deberán instrumentar y ejecutar en sus términos los acuerdos que dicte el órgano de gobierno; cumplir con las disposiciones aplicables; establecer indicadores de gestión y sistemas adecuados de operación, registro, información, seguimiento, control y evaluación de las operaciones de la entidad; instrumentar y supervisar el cumplimiento de programas de modernización, descentralización, desconcentración, simplificación administrativa y de capacitación actualización y entrenamiento de personal, establecer, con autorización del órgano de gobierno, los sistemas de administración de personal e incentivos, así como vigilar que los distintos niveles de

servidores públicos de la entidad, desarrollen sus actividades con sujeción a lo establecido en este artículo.

- Para la ejecución de los programas las entidades elaborarán, programas anuales a partir de los cuales deberán integrarse los proyectos de presupuesto anual respectivos.
- Los órganos de gobierno emitirán los criterios y políticas de operación que las entidades deban observar, tomando en cuenta la situación financiera de las mismas y los objetivos y metas a alcanzar.
- Será obligación del presidente del órgano de gobierno, verificar que en los criterios de operación que se definan, se observe anteriormente.

Aunado a lo expuesto, el AIFA señaló que dentro de la Ley de Aviación se establecen como obligaciones de los pasajeros, las siguientes:

- Brindar al permisionario o concesionario información y datos personales veraces, al momento de la compra del boleto.
- Presentar documentos oficiales de identificación, a solicitud del permisionario o concesionario o del personal autorizado del aeropuerto.
- Acatar las normas de seguridad y operación aeroportuarias vigentes.
- Ocupar el asiento asignado, a menos que la tripulación por un requerimiento justificado le solicite o le autorice ocupar uno distinto.

Además, en la Ley de Aeropuertos y su Reglamento, se precisó que son obligaciones de los concesionarios o permisionarios:

- Asegurar que los aeródromos civiles cuenten con la infraestructura, instalaciones, equipo, señalización, módulo de primeros auxilios y emergencias médicas, servicios y sistemas de organización, adecuados y suficientes para que la operación y atención al usuario se lleve a cabo sobre bases de seguridad, eficiencia y calidad.
- Deberán responsabilizarse del control de los accesos y tránsito de personas, vehículos y bienes en zonas restringidas del aeródromo civil, así como de que las áreas cercanas a los equipos de ayuda a la navegación aérea instalados dentro de los mismos, se mantengan libres de obstáculos que puedan afectar su operación.
- Entre las medidas de seguridad que deben establecer se encuentran: los dispositivos de protección y control de accesos a las zonas restringida y estéril, así como las medidas de acceso y de control del movimiento de personas y vehículos en las zonas restringidas.

Igualmente invocó que resulta aplicable el Anexo 17 del Convenio sobre Aviación Civil Internacional, Seguridad, Protección de la aviación civil internacional contra los actos de interferencia ilícita, específicamente la recomendación "C. Seguridad de los documentos de viaje", en la que se señaló que son obligaciones de los estados contratantes:

- Actualizar regularmente los elementos de seguridad que figuran en las nuevas versiones de sus documentos de viaje, a fin de impedir su uso indebido y facilitar la detección en los casos en que dichos documentos se hayan alterado, duplicado o emitido en forma ilegal.
- Establecer los controles con respecto a la creación y expedición de los documentos de viaje a fin de protegerse contra el robo de sus inventarios y el apoderamiento indebido de documentos de viaje recientemente emitidos.

Sobre esos puntos específicos, destacó un método recomendado para tales efectos, consistente en las siguientes:

- La incorporación de los datos biométricos en sus pasaportes, visados y otros documentos de viaje oficiales de lectura mecánica, utilizando una o más de las técnicas de almacenamiento de datos optativos para suplementar la zona de lectura mecánica, según se especifica en el "Doc 9303, Documentos de viaje de lectura mecánica".
- Los datos requeridos almacenados en un microcircuito integrado son los mismos que se imprimen en la página de datos; o sea, los datos contenidos en la zona de lectura mecánica más la imagen fotográfica digitalizada.
- Los Estados contratantes que deseen suplementar la imagen facial con otro elemento biométrico en el pasaporte pueden utilizar imágenes de las impresiones digitales o del iris.
- Los Estados contratantes que incorporen datos biométricos en sus pasaportes de lectura mecánica deben almacenar los datos en un microcircuito integrado sin contacto que cumpla con la norma ISO/IEC 14443 y esté programado de conformidad con la estructura lógica de datos establecida por la OACI.
- Las autoridades competentes de cada Estado contratante se incautarán de los documentos de viaje fraudulentos, falsificados o imitados. Las autoridades competentes también se incautarán de los documentos de viaje de una persona que se presenta pretendiendo ser el titular legítimo del documento de viaje. Tales documentos se retirarán de la circulación inmediatamente y se devolverán a las autoridades competentes del Estado que figura como expedidor o a la misión diplomática residente de ese Estado.

Finalmente, el AIFA señaló que era aplicable la Ley de Ciencia y Tecnología[53], en su artículo 1, el cual establece que en dicho ordenamiento se regulan los apoyos que el Gobierno Federal está obligado a otorgar para impulsar, fortalecer, desarrollar y consolidar la investigación científica, el desarrollo tecnológico y la innovación en general en el país.

Una vez establecido lo manifestado por el AIFA; este Instituto advierte que el AIFA es un concesionario que podrá llevar a cabo todas las acciones necesarias para administrar, operar,

[53] Publicado en el Diario Oficial de la Federación el 5 de junio de 2002, cuyo texto puede obtenerse del vínculo siguiente: https://www.diputados.gob.mx/LeyesBiblio/pdf/LCT.pdf, consultado por última vez el 28/02/2023.

explotar y construir el Aeropuerto Internacional Felipe Ángeles, prestando los servicios aeroportuarios, complementarios y comerciales, por sí o por conducto de diversas figuras jurídicas de derecho público y privado; así como para obtener, bajo cualquier título, concesiones, permisos, licencias, autorizaciones y en general, ejecutar todos los actos necesarios para llevar a cabo su objeto social, de conformidad con sus Estatutos Sociales y demás disposiciones aplicables.

Bajo ese contexto, resulta importante señalar que conforme a los artículos 1, párrafo quinto, y 3, fracción XXVIII, de la Ley General, el responsable es cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos, del orden federal, estatal y municipal que deciden sobre el tratamiento de datos personales. En ese sentido, y conforme a la actualización del padrón de sujetos obligados del 11 de enero de 2023, el AIFA es reconocido como un sujeto obligado con clave 07003. Por ende, se trata de un responsable para efectos de la Ley General.

Por lo tanto, se encuentra facultado para decidir sobre el tratamiento de datos personales relacionados con las actividades que realiza el AIFA como concesionario del Aeropuerto Internacional Felipe Ángeles, como lo es la prestación por sí misma o por conducto de terceros, los servicios aeroportuarios, complementarios y comerciales de manera permanente, uniforme, regular y no discriminatoria, a todos los usuarios del aeropuerto, incluidos los concesionarios y los permisionarios del servicio de transporte aéreo regular nacional, no regular nacional, privado comercial y privado no comercial que así lo requieran.

Es oportuno considerar que conforme al artículo 48, fracciones I y II, de la Ley de Aeropuertos[54] son:

- Servicios aeroportuarios: aquellos que le corresponde prestar originariamente al concesionario o permisionario, de acuerdo con la clasificación del aeródromo civil, y que pueden proporcionarse directamente o a través de terceros que designe y contrate.
- Servicios complementarios: aquellos que pueden ser prestados por los concesionarios o permisionarios del servicio de transporte aéreo, para sí mismos o para otros usuarios, o por terceros que aquéllos designen.

Respecto de los servicios complementarios, se advierte en el artículo 56, fracción II, del Reglamento de la Ley de Aeropuertos se encuentra el tráfico, entendido como la documentación del pasajero, equipaje, carga y correo. En ese sentido, se desprende que el AIFA cuenta con atribuciones para decidir sobre el tratamiento de datos personales relacionados con dicho servicio

[54] Publicada en el Diario Oficial de la Federación el 22 de diciembre de 1995, cuyo texto puede obtenerse del vínculo siguiente: https://www.diputados.gob.mx/LeyesBiblio/pdf/15_200521.pdf, consultado por última vez el 28/02/2023.

complementario, esto considerando que dentro de la Concesión del AIFA se encuentra previsto el desempeño de esa clase de actividades.

Si bien ese servicio se encuentra previsto en una norma jurídica, ello no significa que el AIFA tenga una amplia configuración para determinar el tratamiento de los más amplios grupos o tipos de datos personales para alcanzar esos fines, pues como se abordó en su oportunidad, existen ciertos tratamientos que deben encontrarse previstos en la normatividad para que los titulares puedan comprender los alcances de este y sus límites. De ahí que para decidir sobre el tratamiento de datos personales resulte indispensable tomar en cuenta además de las funciones asignadas, los límites comprendidos en estas.

En ese sentido, este Instituto advierte que, para el tratamiento de datos biométricos relacionados con el funcionamiento del Sistema de Procesamiento, no debe atenderse únicamente al servicio complementario de tráfico y, por ello, debe contarse con un marco jurídico especifico relacionado con su tratamiento en entornos derivados de la prestación de dichos servicios.

Dentro de la normatividad invocada por el AIFA, se encuentra el Anexo 17 del Convenio sobre Aviación Civil Internacional, Seguridad, Protección de la aviación civil internacional contra los actos de interferencia ilícita, específicamente la recomendación "C. Seguridad de los documentos de viaje", específicamente en la recomendación de actualizar regularmente los elementos de seguridad que figuran en las nuevas versiones de sus documentos de viajé, a fin de impedir su uso indebido y facilitar la detección en los casos en que dichos documentos se hayan alterado, duplicado o emitido en forma ilegal.

Lo anterior, ya que esa recomendación tiene la finalidad especifica de que los estados miembros consideren mayores elementos de seguridad respecto de los documentos de viaje, como lo son los pasaportes, o la utilización de datos biométricos, **esto para evitar duplicidades o falsificaciones de tales instrumentos de identificación para viajes, no así para el aprovechamiento de datos biométricos para el tráfico de personas en los aeropuertos**.

Dentro de la actuación del marco aeronáutico, es aplicable lo previsto en el Convenio de Chicago, del cual México forma parte, y del que se desprende lo siguiente:

> *"[...]*
> *Artículo 3.- Aeronaves civiles y de Estado*
> *El presente Convenio se aplica solamente a las aeronaves civiles y no a las aeronaves de Estado.*
> *Se consideran aeronaves de Estado las utilizadas en servicios militares, de aduanas o de policía.*
> *[...]*

Artículo 90.- Adopción y enmienda de los Anexos
La adopción por el Consejo de los Anexos previstos en el párrafo /) del Artículo 54, requerirá el voto de dos tercios del Consejo en sesión convocada a ese fin; luego serán sometidos por el Consejo a cada Estado contratante.
Todo Anexo o enmienda a uno de ellos, surtirá efecto a los tres meses de ser transmitido a los Estados contratantes o a la expiración de un periodo mayor que prescriba el Consejo, a menos que en el ínterin la mayoría de los Estados contratantes registren en el Consejo su desaprobación.
[...]"

Con base en lo previsto por el Convenio de Chicago respecto a que los anexos son parte del instrumento mismo, se tiene que el Anexo 9, en su parte 1, se estableció lo siguiente:

"[...]
9.18 Método recomendado. — Los Estados contratantes que busquen establecer un sistema electrónico de viaje (ETS) deberían integrar el sistema de verificación previa al viaje en un sistema interactivo de información anticipada sobre los pasajeros.
[...]"

Asimismo, dicho ordenamiento, en el Documento 9303, en su parte 1, establece lo subsecuente:

"[...]
El Doc 9303 integra diversos documentos independientes en los cuales se agrupan especificaciones de carácter general (aplicables a todos los MRTD) así como específicas sobre el formato de esos documentos. En la sección 5.1 "Estructura del Doc 9303" figura una reseña general.
Estas especificaciones no tendrían carácter de normas para los documentos nacionales de identidad. No obstante, un Estado cuyos documentos de identidad son reconocidos por otros Estados como documentos de viaje válidos diseñará estos documentos de identidad de modo que se ajusten a las especificaciones de los Doc 9303-3, Doc 9303-4, Doc 9303-5 o Doc 9303-6.
Aunque las especificaciones que figuran en el Doc 9303-4 están concebidas para aplicarse en particular al pasaporte, dichas especificaciones se aplican igualmente a otros documentos de identidad de tamaño DV3, por ejemplo, el laissezpasser, el documento de identidad de la gente de mar y los documentos de viaje para refugiados.
[...]

5.1 Estructura del Doc 9303

El Doc 9303 consta de trece partes. Cada una de ellas describe un aspecto específico del MRTD. Las partes del Doc 9303 están integradas de tal forma que el expedidor de MRTD puede construir un conjunto completo de especificaciones pertinentes, relativas a un tipo específico de MRTD (formato). La relación entre estos formatos y las partes del Doc 9303 se describe en la Sección 5.2 de esta Parte 1.
[...]

Ciertas disposiciones de las normas internacionales, a que se hace referencia en este texto, constituyen disposiciones del Doc 9303. Cuando existan diferencias entre las especificaciones contenidas en el Doc 9303 y las normas de referencia, a efectos de hacer lugar a los requisitos de construcción específicos de los documentos de viaje de lectura mecánica, incluyendo visados de lectura mecánica, tendrán precedencia las especificaciones contenidas en este texto.
Anexo 9 Convenio sobre Aviación Civil Internacional ("Convenio de Chicago"), Anexo 9 – Facilitación.
RFC 2119 RFC 2119, S. Bradner, "Key Words for Use in RFCs to Indicate Requirement Levels", BCP 14, RFC2119, marzo de 1997."
[...]

Por su parte, el Documento 9303, en su parte 9, se señala:

"[...]

3.5 Limitaciones de las soluciones biométricas

Se reconoce que la implantación de la mayoría de las tecnologías biométricas es susceptible de desarrollo ulterior. Considerando la rapidez de los cambios tecnológicos, toda especificación (incluyendo las de este volumen) debe tener en cuenta y reconocer que habrá cambios resultantes de las mejoras tecnológicas.
La información biométrica almacenada en los documentos de viaje se ajustará a todas las leyes nacionales de protección de datos o a las leyes de confidencialidad del Estado expedidor u organización expedidora.
[...]

4.1 Característica biométrica primaria: imagen facial

Codificación de las imágenes faciales de referencia
El retrato facial impreso de un MRTD conforme a las normas de la OACI es un elemento esencial de ese documento y uno de los portadores de información más importantes, que vincula el documento a su titular. Un retrato facial normalizado de alta calidad ayuda a los organismos expedidores a controlar la identidad y a los organismos fronterizos a inspeccionar el documento de viaje manualmente o mediante un proceso automatizado. Los requisitos para captar y codificar las imágenes faciales se especifican en la norma ISO/IEC 39794-5, Anexo D.1.
[...]
Se EXIGE el uso de imágenes digitales y que éstas estén almacenadas electrónicamente en el documento de viaje.
[...]
Capacidad de almacenamiento de datos del CI sin contacto
La capacidad de almacenamiento de datos del CI queda a discreción del Estado expedidor u organización expedidora, pero SERÁ lo suficientemente grande para almacenar la imagen facial almacenada obligatoria, los datos de la ZLM duplicados y los elementos necesarios para asegurar los datos. El almacenamiento de imágenes faciales adicionales, huellas digitales o

iris, puede exigir un aumento considerable de la capacidad de almacenamiento de datos. No se especifica un valor máximo de la capacidad de datos del CI sin contacto.
[…]"

En el Anexo 17, relativo a la protección de la aviación civil internacional contra los actos de interferencia ilícita, en su parte conducente indica:

"[….]
Actos de interferencia ilícita. Actos, o tentativas, destinados a comprometer la seguridad de la aviación civil incluyendo, sin que esta lista sea exhaustiva, lo siguiente:
- *apoderamiento ilícito de aeronaves,*
- *destrucción de una aeronave en servicio,*
- *toma de rehenes a bordo de aeronaves o en los aeródromos,*
- *intrusión por la fuerza a bordo de una aeronave, en un aeropuerto o en el recinto de una instalación aeronáutica,*
- *introducción a bordo de una aeronave o en un aeropuerto de armas o de artefactos (o sustancias) peligrosos con fines criminales,*
- *uso de una aeronave en servicio con el propósito de causar la muerte, lesiones corporales graves o daños graves a los bienes o al medio ambiente,*
- *comunicación de información falsa que comprometa la seguridad de una aeronave en vuelo, o en tierra, o la seguridad de los pasajeros, tripulación, personal de tierra y público en un aeropuerto o en el recinto de una instalación de aviación civil.*

[…]
C. Seguridad de los documentos de viaje
3.7 Los Estados contratantes actualizarán regularmente los elementos de seguridad que figuran en las nuevas versiones de sus documentos de viaje, a fin de impedir su uso indebido y facilitar la detección en los casos en que dichos documentos se hayan alterado, duplicado o emitido en forma ilegal.
3.8 Los Estados contratantes establecerán controles a fin de protegerse contra el robo de sus inventarios y el apoderamiento indebido de documentos de viaje recientemente emitidos.
3.8.1 Los Estados contratantes establecerán controles apropiados para la totalidad del proceso de solicitud, otorgamiento y expedición de documentos de viaje a fin de lograr un nivel elevado de integridad y seguridad.
3.9 Método recomendado.—Los Estados contratantes deberían incorporar datos biométricos en sus pasaportes, visados y otros documentos de viaje oficiales de lectura mecánica, utilizando una o más de las técnicas de almacenamiento de datos optativos para suplementar la zona de lectura mecánica, según se especifica en el Doc 9303, Documentos de viaje de lectura mecánica. Los datos requeridos almacenados en un microcircuito integrado son los mismos que se imprimen en la página de datos; o sea, los datos contenidos en la zona de lectura mecánica más la imagen fotográfica digitalizada. Los Estados contratantes que deseen suplementar la imagen facial con otro elemento biométrico en el pasaporte pueden utilizar imágenes de las impresiones digitales o del iris. Los Estados contratantes que incorporen

datos biométricos en sus pasaportes de lectura mecánica deben almacenar los datos en un microcircuito integrado sin contacto que cumpla con la norma ISO/IEC 14443 y esté programado de conformidad con la estructura lógica de datos establecida por la OACI.
[...]"

En ese sentido, se advierte que, en el marco del derecho internacional aplicable a la aviación civil, el Convenio de Chicago, del cual México es parte, contiene diversas reglas y anexos aplicables para la uniformidad de ese servicio prestado por aeronaves civiles.

Lo anterior es importante, ya que OACI redacta y mantiene normas internacionales, como es el Anexo 9, que los Estados miembros han de poner en práctica, esto con la finalidad de crear especificaciones estándar para los documentos de viaje y los datos contenidos en ellos para establecer un grado satisfactorio de confianza en la fiabilidad de los documentos de viaje y en la eficacia de los procedimientos de inspección.

Como parte de los anexos aludidos en el artículo 90 del Convenio de Chicago, se incluyeron el Anexo 9 y el Anexo 17, el primero de los mencionados señala que los Estados contratantes que busquen establecer un sistema electrónico de viaje deberían integrar el sistema de verificación previa al viaje en un sistema interactivo de información anticipada sobre los pasajeros.

Para esos efectos, OACI emitió el Documento 9303, compuesto de trece partes en las cuales se establece las características de los documentos de viaje electrónicos, en el cual, si bien se señala que las especificaciones en ellos no tendrían carácter de normas para los documentos nacionales de identidad, lo cierto es que para el diseño de documentos de viaje válidos se realizaran conforme a los Doc 9303-3, Doc 9303-4, Doc 9303-5 o Doc 9303-6.

Como parte de los antecedentes descritos en el documento en estudio, en 2005, los 188 Estados miembros de la OACI existentes en esa fecha aprobaron la nueva norma de que todos los Estados debían comenzar a expedir pasaportes de lectura mecánica con arreglo al Doc 9303, no más allá del año 2010, de tal suerte que a más tardar para el año 2015 debieron caducar todos los documentos de viaje que no son de lectura mecánica, esto es, los pasaportes no electrónicos.

Es importante señalar que el propio Documento 9303, establece que la implantación de la mayoría de las tecnologías biométricas es susceptible de desarrollo ulterior y, considerando la rapidez de los cambios tecnológicos, toda especificación debe tener en cuenta y reconocer que habrá cambios resultantes de las mejoras tecnológicas. Sin embargo, dicho documento es puntual en establecer que la información biométrica almacenada en los documentos de viaje debe ajustarse a todas las leyes nacionales de protección de datos del Estado expedidor u organización expedidora.

En el caso mexicano, la Secretaría de Relaciones Exteriores emitió el Acuerdo del pasaporte electrónico, en el cual se señaló atendía lo previsto en el artículo 7 del Reglamento de Pasaportes y del Documento de Identidad y Viaje, así como en el anexo 9 del Convenio de Chicago, así como del Documento 9303 en su parte 9, esto con el objetivo de establecer las medidas de seguridad que sean identificadas tanto a simple vista o al tacto y mediante dispositivos ópticos o electrónicos el circuito integrado sin contacto donde se almacena la información de la página de datos, una medición biométrica del titular del pasaporte y un objeto de seguridad para proteger los datos con una tecnología criptográfica.

Incluso, sobre el reconocimiento facial, se deja en libertad a los estados contratantes la libertad de determinar la capacidad de almacenamiento de datos, pero debe ser lo suficientemente grande para almacenar la imagen facial almacenada obligatoria, los datos de la zona de lectura mecánica duplicados y los elementos necesarios para asegurar los datos. El almacenamiento de imágenes faciales adicionales, huellas digitales o iris, puede exigir un aumento considerable de la capacidad de almacenamiento de datos. No se especifica un valor máximo de la capacidad de datos del circuito integrado sin contacto existente en el documento de viaje electrónico.

En ese sentido, el retrato facial impreso en los documentos de viaje, conforme a las normas de la OACI, es un elemento esencial de ese documento y uno de los portadores de información más importantes, que vincula el documento a su titular. Un retrato facial normalizado de alta calidad ayuda a controlar la identidad y a los organismos fronterizos a inspeccionar el documento de viaje manualmente o mediante un proceso automatizado.

En ese sentido, se advierte que a nivel internacional se considera como aquellos datos biométricos para empezar con un sistema de interfuncionamiento mundial se encuentran los rasgos faciales, y solo de manera opcional el reconocimiento de huellas digitales o del iris, esto mediante imágenes de alta resolución; esto para lograr uniformidad de todos los datos obligatorios y opcionales y un ordenamiento o agrupamiento establecido de los datos que debe seguirse para lograr ese objetivo.

Por su parte, en el Anexo 17, se establece que son actos de interferencia ilícita aquellos actos, o tentativas, destinados a comprometer la seguridad de la aviación civil incluyendo, sin que esta lista sea exhaustiva, los siguientes:

- Apoderamiento ilícito de aeronaves,
- Destrucción de una aeronave en servicio,
- Toma de rehenes a bordo de aeronaves o en los aeródromos,
- Intrusión por la fuerza a bordo de una aeronave, en un aeropuerto o en el recinto de una instalación aeronáutica,

- Introducción a bordo de una aeronave o en un aeropuerto de armas o de artefactos (o sustancias) peligrosos con fines criminales,
- Uso de una aeronave en servicio con el propósito de causar la muerte, lesiones corporales graves o daños graves a los bienes o al medio ambiente, y
- Comunicación de información falsa que comprometa la seguridad de una aeronave en vuelo, o en tierra, o la seguridad de los pasajeros, tripulación, personal de tierra y público en un aeropuerto o en el recinto de una instalación de aviación civil.

Como parte de las medidas establecidas en ese anexo, se establecieron recomendaciones de seguridad de los documentos de viaje, en el que señaló que los Estados contratantes actualizarán regularmente los elementos de seguridad que figuran en las nuevas versiones de sus documentos de viaje, a fin de impedir su uso indebido y facilitar la detección en los casos en que dichos documentos se hayan alterado, duplicado o emitido en forma ilegal.

Por lo que los estados contratantes establecerán controles a fin de protegerse contra el robo de sus inventarios y el apoderamiento indebido de documentos de viaje recientemente emitidos, así como establecer controles apropiados para la totalidad del proceso de solicitud, otorgamiento y expedición de documentos de viaje a fin de lograr un nivel elevado de integridad y seguridad.

Para lograr lo anterior, se sugiere a los estados contratantes incorporar datos biométricos en sus pasaportes, visados y otros documentos de viaje oficiales de lectura mecánica, utilizando una o más de las técnicas de almacenamiento de datos optativos para suplementar la zona de lectura mecánica. Los datos requeridos almacenados en un microcircuito integrado son los mismos que se imprimen en la página de datos; o sea, los datos contenidos en la zona de lectura mecánica más la imagen fotográfica digitalizada.

Los Estados contratantes que deseen suplementar la imagen facial con otro elemento biométrico en el pasaporte pueden utilizar imágenes de las impresiones digitales o del iris.

Los Estados contratantes que incorporen datos biométricos en sus pasaportes de lectura mecánica deben almacenar los datos en un microcircuito integrado sin contacto y esté programado de conformidad con la estructura lógica de datos.

En ese sentido, este Instituto advierte que, respecto a la operación de los aeropuertos conforme al Convenio de Chicago, se desprenden dos finalidades para la utilización de documentos de viaje electrónicos, consistentes en:

- Establecer un sistema electrónico de viaje para integrar el sistema de verificación previa al viaje, en un sistema interactivo de información anticipada sobre los pasajeros.

- Verificar la seguridad de los documentos de viaje electrónicos tanto en su emisión como en la prestación de servicios aeronáuticos, además de servir para la detección, prevención, investigación o contención actos que atenten contra dicha actividad.

En virtud de lo expuesto, si bien existen disposiciones que habilitan el uso de datos biométricos, específicamente el reconocimiento facial, entre otros, lo cierto es que el fundamento de su tratamiento responde a dos finalidades diferentes entre sí, en ese sentido, se tiene que el uso de datos biométricos con base en dicha normatividad debería de atender los objetivos que el mismo regula.

En el caso de la presente evaluación, se advierte que el uso de biométricos, así como del pasaporte electrónico tienen finalidades diferentes a las contempladas en dicha normatividad, por lo que es importante señalar que el AIFA deberá considerar el tratamiento de datos personales a fin de poder justificar este, en su caso se sugiere considerar el uso de datos biométricos en función a lo regulado por OACI, así como la regulación jurídica que permite su uso, e impactarlas en el cumplimiento de los restantes principios y deberes.

Es importante, señalar que conforme a lo previsto en el Documento 9303, parte 9, la utilización del documento de viaje electrónico deberá ser apegado en todo momento a la normatividad interna del Estado contratante en materia de protección de datos personales, siendo en el caso del Estado Mexicano la Ley General y la normatividad que deriva del mismo.

En ese sentido, se considera que la normatividad citada por el AIFA sobre el tratamiento de datos personales en el Programa Institucional del AIFA tiene como objetivo atender lo previsto en la Ley de Entidades Paraestatales y su Reglamento, disposiciones que regulan el actuar administrativo del AIFA.

Igualmente, señaló la obligación de los pasajeros de brindar al permisionario o concesionario información y datos personales veraces, al momento de la compra del boleto, así como presentar documentos oficiales de identificación, a solicitud del permisionario o concesionario o del personal autorizado del aeropuerto, además de acatar las normas de seguridad y operación aeroportuarias vigentes; todas existentes en la Ley de Aviación Civil.

Al respecto, esas normas no deben interpretarse en un carácter amplio que permitan que cualquier tipo de dato personal sea tratado para que los pasajeros cumplan dichas obligaciones, esto considerando que el principio de licitud implica, dentro del tratamiento de datos personales, que los límites a tal cuestión se encuentren dentro de lo contemplado en una norma jurídica.

No pasa desapercibido que el AIFA presentó como parte del requerimiento de información adicional una Minuta Proyecto de Decreto por el que se reforma la fracción X del artículo 3 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, con número CD-LXIV-I1I-2P-287, en la que se propone la inclusión de los datos biométricos como datos personales sensibles, situación que se hace patente, pero que en el caso concreto no representa o contiene efectos jurídicos para el proceso de dictaminación.

De lo expuesto, se desprende que los datos personales deberán tratarse con apego y cumplimiento a lo dispuesto por la legislación mexicana y el derecho internacional, así como sujetarse a las facultades o atribuciones que la normativa aplicable les confiera. Por lo que en la materia específica de protección de datos biométricos, se sugiere a los responsables del sector público justifique de acuerdo con la normatividad que le es aplicable en lo específico y a la actividad concreta en la que son tratados los datos biométricos, a fin de verificar que la misma prevea el uso de este tipo de datos y en qué términos lo hace, a fin de poder llevar a cabo el tratamiento del dato lícitamente.

Sistema de Procesamiento.

Sobre este asunto en particular, y considerando la documentación que remite el AIFA, se desprende que el 23 de julio de 2021, la SEDENA celebró con las empresas Apollo Communications, S.A. de C.V., Química Apollo S.A de C.V., Vision-Box Soluções de Visão Por Computador S.A., y Amadeus IT Croup, S.A. un contrato abierto para la "Adquisición, Suministro, Instalación, Comisionamiento y Puesta en Operación de Sistemas de Seguridad de la Aviación, Operación Aeroportuaria, Procesamiento del Pasajero, Infraestructuras de Telecomunicaciones, Ciberseguridad y Soporte al Pasajero, para la Ciudad Aeroportuaria (AIFA)", identificado con el número SDN/DN8/AIFA/12916-F7/2021-ITP-043-02. De conformidad con el Anexo A denominado "Descripción Técnica" se adquirió entre otros el Sistema de Procesamiento.

Que, dentro de las cláusulas del contrato aludido, destaca la décimo octava, misma que establece textualmente, lo siguiente:

> *"[…]*
> *Décima octava. - "Cesión de derechos".*
> ***En ningún caso los derechos y obligaciones derivadas de este instrumento contractual, podrán ser cedidos en todo o en partes, en favor de otras personas físicas o morales distintas** a los que se le hubiere adjudicado el contrato, con excepción de los derechos de cobro en cuyo caso se deberá contar con la conformidad previa y por escrito de "La Dependencia".*
> *[…]"*
>
> ***[Énfasis añadido]***

Posteriormente, el 15 de diciembre de 2021, la SEDENA, el AIFA, y las empresas Apollo Communications, S.A. de C.V., Química Apollo S.A de C.V., Vision-Box Soluções de Visão Por Computador S.A., y Amadeus IT Croup, S.A., celebró un instrumento jurídico en materia de tratamiento y protección de datos personales del sistema de procesamiento de pasajeros celebrado, del cual se desprende lo siguiente:

[…]

III. Se observa que en el Contrato celebrado entre el Agto. Ings. y el Consorcio "Apollo Communications, S.A. de C.V.; Química Apollo S.A. de C.V.; Visión-Box Soluções de Visão por Computador S.A.. y Amadeus IT Croup, S.A., en la parte relativa al Sistema de Procesamiento de Pasajeros, no se establecieron cláusulas de Protección de Datos Personales en términos del Título Cuarto de la LCPDPPSO, en las cuales se señalarán las obligaciones del proveedor con respecto del tratamiento de Datos Personales Identificativos, de Origen y Biométricos y se advierte expresamente que el proveedor en su carácter de encargado no ostenta poder alguno de decisión sobre estos.

IV. Aunado a lo anterior, y derivado de que el AIFA no cuenta con figura alguna dentro del documento contractual SDN/DN8/AIFA/12916-F7/2021-ITP-043-02, el cual no contempla la legislación de Protección de Datos Personales, en atención a que no es una de las partes en la Contratación señalada con antelación, por lo que le es jurídicamente imposible pronunciarse con respecto de los instrumentos jurídicos, solicitados por el INAI, así como en la práctica otorgar instrucciones al encargado con respecto del tratamiento de datos personales.

[…]

VI. En este tenor, se requiere de una figura distinta a las de Titular, Encargado y Responsable a las que hace referencia la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, para estar en condiciones de llevar a cabo las instrucciones por parte del AIFA S.A. de C.V., al Consorcio "Apollo Communications, S.A. de C.V.; Química Apollo S.A. de C.V.; Visión-Box Soluções de Visão por Computador S.A„ y Amadeus IT Group, S.A., que tiene como encargo el tratamiento de datos personales del Sistema de Procesamiento de Pasajeros.

VII. Para resolver el problema jurídico descrito, se menciona la coexistencia de dos tipos de responsables:

a) Responsable jurídico, que recae sobre el Agto. de Ings. en su calidad de administrador del contrato, quien responde por los alcances, cláusulas y omisiones del contrato en términos de lo señalado en los puntos 1 y 2.

b) Responsable de operación aeroportuaria, que es la figura que el AIFA tendrá a partir de la firma del presente. a través del Subdirector de Sistemas, quien será el sujeto que otorgará instrucciones precisas al encargado con respecto del tratamiento de datos personales, en cumplimiento a la LGPDPPSO.

[…]

JUSTIFICACIÓN.

De conformidad a lo establecido en los artículos 58, 59, 60, 61, 62, 63 y 64 de la LGPDPPSO y 108 de los Lineamientos Generales, los cuales expresan que la relación entre el responsable y el encargado deberá estar formalizada mediante contrato o cualquier otro instrumento jurídico que le vincula con el mismo y delimita el ámbito de su actuación para la prestación de un servicio.

En este sentido, si bien el responsable de operación aeroportuaria no puede efectuar modificaciones al contrato originario, también lo es que de conformidad a lo analizado en los puntos 6, 7, 8 y 9, es viable efectuar un Instrumento Jurídico de Protección de Datos Personales (Instrumento Jurídico en materia de Tratamiento y Protección de Datos Personales entre el Responsable Jurídico, el Responsable de Operación Aeroportuaria y el encargado del Tratamiento de Datos Personales) en el que se establezcan las condiciones que regularán las instrucciones que el Responsable de Operación Aeroportuaria, otorgue al Encargado.

OBLIGACIONES.

Primera. Consistentes en las instrucciones del responsable de operación aeroportuaria para realizar el tratamiento de los datos personales.

Segunda. La abstención del encargado de tratar los datos personales para finalidades distintas a las instruidas por el responsable de operación aeroportuaria.

[...]

Cuarta. La obligación de informar al responsable de operación aeroportuaria en el caso de una vulneración de datos personales.

Quinta. El responsable de operación aeroportuaria deberá formalizar un documento con el encargado sobre el deber de confidencialidad que debe cumplir con respecto de los datos personales que se tratan.

En el caso particular del encargado, las personas morales que constituyen el mismo, deberán, en su caso, justificar las responsabilidades de cada uno de los subencargados con respecto de los datos personales que trata, estableciendo claramente el tramo de responsabilidad de cada uno, en cada transferencia, transmisión o remisión, según el caso.

Sexta. El encargado debe suprimir los datos personales objeto del tratamiento una vez cumplida la relación jurídica con el responsable de operación aeroportuaria.

Séptima. Obligación expresa del encargado de abstenerse de transferir los datos

Octava. personales que trata, salvo que el responsable de operación aeroportuaria así lo determine o, sea objeto de una subcontratación, la cual deberá estar justificada y aprobada por el responsable de operación aeroportuaria. Si el encargado subcontrata servicios de cualquier tipo que impliquen el tratamiento de datos personales del responsable de operación aeroportuaria, este último deberá autorizar el tratamiento que llevará a cabo con el subcontratado; y posterior a dicha autorización, el encargado deberá formalizar el instrumento jurídico y hacerlo del conocimiento del responsable de operación aeroportuaria.

Los contratos efectuados por el encargado deberán contar con todos los requisitos que señala la normatividad mexicana en materia de protección de datos personales.

Novena. En el caso de que los servicios del encargado estén contratados o adheridos a los servicios aplicaciones e infraestructura en el cómputo en la nube, el responsable de operación

aeroportuaria debe garantizar que, en el tratamiento de datos personales, el encargado garantice políticas de protección de datos personales en términos de la legislación mexicana. Y aunado a lo anterior el encargado deberá acreditar fehacientemente a través de documentos legales que:

a) Aplica políticas de protección de datos personales afines a los principios y deberes de la LGPDPPSO y/o la Ley Federal de Protección de Datos Personales en Posesión de Particulares;

b) Transparenta las subcontrataciones que involucren la información relativa al servicio que brinda al responsable de operación aeroportuaria;

c) Abstenerse de incluir condiciones que le autoricen la titularidad o propiedad de cualquier información de los datos personales sobre la que encuentre el servicio al subcontratado;

d) La confidencialidad que debe guardar con respecto de los datos personales sobre los que prese el servicio;

e) Dar a conocer sus políticas de privacidad;

f) Tener la posibilidad de limitar el tratamiento de los datos personales de la prestación del servicio en caso de que el responsable lo requiera;

g) Establecer las medidas de seguridad para la protección de los datos personales

h) Garantizar la supresión de los datos personales una vez que hay concluido el servicio prestado al responsable.

Décima. De ser el caso, el responsable de operación aeroportuaria debe delimitar el tratamiento de datos personales por parte de algún subencargado externo.

Décimo Primera. En el caso de que el encargado efectúe transferencias nacionales o internacionales de datos personales en algún proceso o procedimiento relacionado con el Sistema de Procesamiento de Pasajeros (v. gr. en la nube), éste debe de hacerlo saber al responsable de operación aeroportuaria, con la finalidad de que se haga del conocimiento del Titular a través del Aviso de privacidad y se cuente con consentimiento de este.

Asimismo, deberá señalar el alcance del tratamiento de los datos y obligaciones y responsabilidades asumidas por las partes.

Décimo Segunda. El o los encargados se obligan a tomar capacitación en materia de Protección de Datos Personales, a través del Programa de Capacitación impulsado por el Comité de Transparencia.

Décimo Tercera. Para tal efecto deberá acreditar ante el responsable de operación aeroportuaria, que las personas que se dedican al tratamiento de datos personales a cuenta del encargado están en capacitación constante en esta materia.

El encargado se compromete ante el responsable de Operación Aeroportuaria y el Responsable Jurídico a:

a) Permitir que Instituto y/ o el responsable de operación aeroportuaria, realicen verificaciones en el lugar o establecimiento donde lleva a cabo el tratamiento de datos personales;

b) Colaborar con el INAI en las investigaciones previas y en las verificaciones, proporcionando la información necesaria.

c) Generar, actualizar y conservar la documentación que permita acreditar el cumplimiento de sus obligaciones.

d) d) El encargado tomar las medidas necesarias, a fin de garantizar el estricto cumplimiento a la protección de lo datos personales, materia del presente Instrumento.
Décimo Cuarta. De existir transferencia de datos personales fuera del territorio nacional por parte de los servicios otorgados por el encargado, éste se obliga a que el receptor o destinatario proteja los datos personales conforme a los principios, deberes y demás obligaciones similares o equiparables a las previstas en la Ley General y demás normatividad mexicana en la materia, así como a los términos previstos en el aviso de privacidad que le será comunicado por el responsable de operación aeroportuaria.
Décimo Quinta. De incumplir el encargado con cualesquiera de las condiciones efectuadas en el presente Instrumento Jurídico para el tratamiento y protección de datos personales, el responsable de operación aeroportuaria hará del conocimiento del responsable jurídico esa situación, a fin de solicitar la rescisión del Contrato originario o modificatorio entre este y el encargado o subencargados.
Décimo Sexta. Si el encargado incumple con las instrucciones del responsable de operación aeroportuaria, y decide por sí mismo sobre el tratamiento de datos personales, asumirá el carácter de responsable de conformidad con la normatividad en la materia.
Décimo Séptima. El presente instrumento jurídico de ninguna manera cede los derechos y obligaciones derivados del instrumento contractual originario entre el Responsable jurídico, y el Encargado en términos de la Cláusula Décimo Octava del Contrato abierto para la "Adquisición, Suministro, Instalación, Comisionamiento y Puesta en Operación de Sistemas de Seguridad de la Aviación, Operación Aeroportuaria, Procesamiento del Pasajero, Infraestructuras de Telecomunicaciones, Ciberseguridad y Soporte al Pasajero para la Ciudad Aeroportuaria (AIFA). y su interpretación solo es aplicable para el tratamiento de los datos personales del Sistema de Procesamiento de Pasajeros.
Décimo Octava. El presente instrumento jurídico, puede tener modificaciones a solicitud de cualquiera de las partes, previo análisis y aprobación conjunta de las mismas, debiendo quedar dicha modificación por escrito.
Décimo Novena Alcance. El presente acuerdo tiene como finalidad que las partes en su tramo de control llevan a cabo las acciones, actividades, funciones o tareas que les corresponda en términos de las responsabilidades relacionadas con el tratamiento de datos personales con base en la legislación en materia de protección de datos personales, aplicable.
Vigésima. Las presentes obligaciones son de carácter enunciativo y no de carácter limitativo en el marco del cumplimiento a la LGPDPPSO y demás normatividad aplicable.
[...]

De los anteriores antecedentes, se desprende lo siguiente:

- Que la SEDENA celebró con las empresas Apollo Communications, S.A. de C.V., Química Apollo S.A de C.V., Vision-Box Soluções de Visão Por Computador S.A., y Amadeus IT Croup, S.A. un contrato abierto para la "Adquisición, Suministro, Instalación, Comisionamiento y Puesta en Operación de Sistemas de Seguridad de la Aviación, Operación Aeroportuaria, Procesamiento del Pasajero, Infraestructuras de Telecomunicaciones, Ciberseguridad y

Soporte al Pasajero, para la Ciudad Aeroportuaria (AIFA)", identificado con el numero SDN/DN8/AIFA/12916-F7/2021-ITP-043-02; que incluyó, de conformidad con el Anexo A denominado "Descripción Técnica" se adquirió entre otros el Sistema de Procesamiento

- Que dentro en la cláusula décimo-octava del referido contrato se estableció que en ningún caso los derechos y obligaciones derivadas de este instrumento contractual, podrán ser cedidos en todo o en partes, en favor de otras personas físicas o morales distintas a los que se le hubiere adjudicado el contrato, con excepción de los derechos de cobro en cuyo caso se deberá contar con la conformidad previa y por escrito de "la SEDENA.
- Que posterior a ello, el 15 de diciembre de 2021, la SEDENA, el AIFA, y las empresas Apollo Communications, S.A. de C.V., Química Apollo S.A de C.V., Vision-Box Soluções de Visão Por Computador S.A., y Amadeus IT Croup, S.A., celebró un instrumento jurídico en materia de tratamiento y protección de datos personales del sistema de procesamiento de pasajeros celebrado.
- Que en dicho instrumento jurídico se señaló que en el contrato SDN/DN8/AIFA/12916-F7/2021-ITP-043-02, específicamente en la parte relativa al Sistema de Procesamiento de Pasajeros, no se advierten cláusulas en materia de protección de datos personales en términos del Título Cuarto de la Ley General.
- También se estableció que el AIFA no cuenta con figura alguna dentro del documento contractual SDN/DN8/AIFA/12916-F7/2021-ITP-043-02, el cual no contempla la legislación de Protección de Datos Personales, en atención a que no es una de las partes en la Contratación señalada con antelación, por lo que le estimó que era jurídicamente imposible pronunciarse con respecto de los instrumentos jurídicos, solicitados por el INAI, así como en la práctica otorgar instrucciones al encargado con respecto del tratamiento de datos personales.
- Que para resolver el problema jurídico descrito, las partes señalaron la coexistencia de dos tipos de responsables.
- Inicialmente, se consideró al responsable jurídico, que recae sobre el Agrupamiento de Ingenieros "Felipe Ángeles", adscrito a la SEDENA, en su calidad de administrador del contrato, quien responde por los alcances, cláusulas y omisiones del contrato en términos de lo señalado en los puntos 1 y 2.
- Por otra parte, se designó al responsable de operación aeroportuaria, que es la figura que el AIFA tendrá a partir de la firma del presente. a través del Subdirector de Sistemas, quien será el sujeto que otorgará instrucciones precisas al encargado con respecto del tratamiento de datos personales, en cumplimiento a la Ley General, y
- Que dicho instrumento se justificaba en los artículos 58, 59, 60, 61, 62, 63 y 64 de la Ley General y 108 de los Lineamientos Generales, los cuales expresan que la relación entre el responsable y el encargado deberá estar formalizada mediante contrato o cualquier otro instrumento jurídico que le vincula con el mismo y delimita el ámbito de su actuación para la prestación de un servicio, pues el responsable de operación aeroportuaria no puede efectuar

modificaciones al contrato originario, por lo que era necesario se establecieran las condiciones que regularán las instrucciones que el Responsable de Operación Aeroportuaria, otorgue al Encargado.

En ese sentido, en el instrumento jurídico de mérito se establecieron las siguientes obligaciones:

- Que el encargado deberá seguir las instrucciones del responsable de operación aeroportuaria para realizar el tratamiento de los datos personales.
- Que el encargado debe abstenerse de tratar los datos personales para finalidades distintas a las instruidas por el responsable de operación aeroportuaria.
- Que los encargados tienen la obligación de informar al responsable de operación aeroportuaria en el caso de una vulneración de datos personales.
- Que el responsable de operación aeroportuaria deberá formalizar un documento con el encargado sobre el deber de confidencialidad que debe cumplir con respecto de los datos personales que se tratan.
- Que, en el caso particular del encargado, las personas morales que constituyen el mismo, deberán, en su caso, justificar las responsabilidades de cada uno de los subencargados con respecto de los datos personales que trata, estableciendo claramente el tramo de responsabilidad de cada uno, en cada transferencia, transmisión o remisión, según el caso.
- Que el encargado debe suprimir los datos personales objeto del tratamiento una vez cumplida la relación jurídica con el responsable de operación aeroportuaria.
- Que el encargado tiene la obligación expresa de abstenerse de transferir los datos personales que trata, salvo que el responsable de operación aeroportuaria así lo determine o, sea objeto de una subcontratación, la cual deberá estar justificada y aprobada por el responsable de operación aeroportuaria.
- Que si el encargado subcontrata servicios de cualquier tipo que impliquen el tratamiento de datos personales del responsable de operación aeroportuaria, este último deberá autorizar el tratamiento que llevará a cabo con el subcontratado; y posterior a dicha autorización, el encargado deberá formalizar el instrumento jurídico y hacerlo del conocimiento del responsable de operación aeroportuaria.
- Que los contratos efectuados por el encargado deberán contar con todos los requisitos que señala la normatividad mexicana en materia de protección de datos personales.
- Que en el caso de que los servicios del encargado estén contratados o adheridos a los servicios aplicaciones e infraestructura en el cómputo en la nube, el responsable de operación aeroportuaria debe garantizar que, en el tratamiento de datos personales, el encargado garantice políticas de protección de datos personales en términos de la legislación mexicana.
- Que aunado a lo anterior el encargado deberá acreditar fehacientemente a través de documentos legales que aplica políticas de protección de datos personales afines a los principios y deberes de la Ley General y/o la Ley Federal de Protección de Datos Personales

en Posesión de Particulares; transparenta las subcontrataciones que involucren la información relativa al servicio que brinda al responsable de operación aeroportuaria; abstenerse de incluir condiciones que le autoricen la titularidad o propiedad de cualquier información de los datos personales sobre la que encuentre el servicio al subcontratado; la confidencialidad que debe guardar con respecto de los datos personales sobre los que prese el servicio; dar a conocer sus políticas de privacidad; tener la posibilidad de limitar el tratamiento de los datos personales de la prestación del servicio en caso de que el responsable lo requiera; establecer las medidas de seguridad para la protección de los datos personales y garantizar la supresión de los datos personales una vez que hay concluido el servicio prestado al responsable.

- Que, en el caso, el responsable de operación aeroportuaria debe delimitar el tratamiento de datos personales por parte de algún subencargado externo.
- Que en el caso de que el encargado efectúe transferencias nacionales o internacionales de datos personales en algún proceso o procedimiento relacionado con el Sistema de Procesamiento de Pasajeros, como en el computo en la nube, éste debe de hacerlo saber al responsable de operación aeroportuaria, con la finalidad de que se haga del conocimiento del Titular a través del Aviso de privacidad y se cuente con consentimiento de este, además de señalar el alcance del tratamiento de los datos y obligaciones y responsabilidades asumidas por las partes.
- Que el o los encargados se obligan a tomar capacitación en materia de Protección de Datos Personales, a través del Programa de Capacitación impulsado por el Comité de Transparencia.
- Que para el efecto deberá acreditar ante el responsable de operación aeroportuaria, que las personas que se dedican al tratamiento de datos personales a cuenta del encargado están en capacitación constante en esta materia, el encargado se compromete ante el responsable de Operación Aeroportuaria y el Responsable Jurídico a permitir que Instituto y/ o el responsable de operación aeroportuaria, realicen verificaciones en el lugar o establecimiento donde lleva a cabo el tratamiento de datos personales; colaborar con el INAI en las investigaciones previas y en las verificaciones, proporcionando la información necesaria; generar, actualizar y conservar la documentación que permita acreditar el cumplimiento de sus obligaciones y tomar las medidas necesarias, a fin de garantizar el estricto cumplimiento a la protección de los datos personales, materia del presente Instrumento.
- Que en el caso de existir transferencia de datos personales fuera del territorio nacional por parte de los servicios otorgados por el encargado, éste se obliga a que el receptor o destinatario proteja los datos personales conforme a los principios, deberes y demás obligaciones similares o equiparables a las previstas en la Ley General y demás normatividad mexicana en la materia, así como a los términos previstos en el aviso de privacidad que le será comunicado por el responsable de operación aeroportuaria.

- Que, de incumplir el encargado con cualesquiera de las condiciones efectuadas en el presente Instrumento Jurídico para el tratamiento y protección de datos personales, el responsable de operación aeroportuaria hará del conocimiento del responsable jurídico esa situación, a fin de solicitar la rescisión del Contrato originario o modificatorio entre este y el encargado o subencargados.
- Que, si el encargado incumple con las instrucciones del responsable de operación aeroportuaria, y decide por sí mismo sobre el tratamiento de datos personales, asumirá el carácter de responsable de conformidad con la normatividad en la materia.
- Que lo anterior no implica la cesión de derechos y obligaciones derivados del instrumento contractual originario entre el responsable jurídico, y el encargado. y su interpretación solo es aplicable para el tratamiento de los datos personales del Sistema de Procesamiento de Pasajeros.
- Que puede tener modificaciones a solicitud de cualquiera de las partes, previo análisis y aprobación conjunta de las mismas, debiendo quedar dicha modificación por escrito.
- Que dicho acuerdo tiene como finalidad que las partes en su tramo de control llevan a cabo las acciones, actividades, funciones o tareas que les corresponda en términos de las responsabilidades relacionadas con el tratamiento de datos personales con base en la legislación en materia de protección de datos personales, aplicable.

Sobre el punto en particular que nos ocupa, es oportuno recordar que el AIFA es un concesionario que podrá llevar a cabo todas las acciones necesarias para administrar, operar, explotar y construir el Aeropuerto Internacional Felipe Ángeles, prestando los servicios aeroportuarios, complementarios y comerciales, por sí o por conducto de diversas figuras jurídicas de derecho público y privado; así como para obtener, bajo cualquier título, concesiones, permisos, licencias, autorizaciones y en general, ejecutar todos los actos necesarios para llevar a cabo su objeto social, de conformidad con sus Estatutos Sociales y demás disposiciones aplicables.

Cabe recordar que la intervención de la SEDENA dentro de creación del AIFA es, conforme a la Resolución AIFA, de accionista mayoritario, sin embargo, ello implica que son dos entes diferentes, pues si bien el primero de los mencionados es accionista del segundo, lo cierto es que ello no los equipara como responsables en términos de la Ley General.

Esto, ya que conforme a los artículos 1, párrafo quinto, y 3, fracción XXVIII, de la Ley General, el **responsable es** cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos, del orden federal, estatal y municipal **que deciden sobre el tratamiento de datos personales**.

En tanto, no debe perderse de vista que quien ostenta la concesión respecto al Aeropuerto Internacional Felipe Ángeles es el AIFA y no así la SEDENA, de acuerdo con la Concesión AIFA. Sin embargo, este Instituto observa que el Sistema de Procesamiento fue adquirido por la SEDENA, el cual es materia de análisis en el presente dictamen.

Por lo tanto, es importante considerar que en los artículos 3, fracción XV, 58, y 59 de la Ley General así como 109 de los Lineamientos Generales establecen lo siguiente:

- Que el encargado deberá realizar las actividades de tratamiento de los datos personales sin ostentar poder alguno de decisión sobre el alcance y contenido de este, así como limitar sus actuaciones a los términos fijados por el responsable.
- Que la relación entre el responsable y el encargado deberá estar formalizada mediante contrato o cualquier otro instrumento jurídico que decida el responsable, de conformidad con la normativa que le resulte aplicable, y que permita acreditar su existencia, alcance y contenido.
- Que dicho instrumento jurídico debe contener al menos respecto de los servicios que preste el encargado: Realizar el tratamiento de los datos personales conforme a las instrucciones del responsable; abstenerse de tratar los datos personales para finalidades distintas a las instruidas por el responsable; implementar las medidas de seguridad conforme a los instrumentos jurídicos aplicables; informar al responsable cuando ocurra una vulneración a los datos personales que trata por sus instrucciones; guardar confidencialidad respecto de los datos personales tratados; suprimir o devolver los datos personales objeto de tratamiento una vez cumplida la relación jurídica con el responsable, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales, y abstenerse de transferir los datos personales salvo en el caso de que el responsable así lo determine, o la comunicación derive de una subcontratación, o por mandato expreso de la autoridad competente.
- Que igualmente debe establecerse dentro de las cláusulas permitir al Instituto o al responsable realizar verificaciones en el lugar o establecimiento donde lleva a cabo el tratamiento de los datos personales; así como la obligación de colaborar con el Instituto en las investigaciones previas y verificaciones que lleve a cabo en términos de lo dispuesto en la Ley General y los presentes Lineamientos generales, proporcionando la información y documentación que se estime necesaria para tal efecto, y generar, actualizar y conservar la documentación necesaria que le permita acreditar el cumplimiento de sus obligaciones.

En ese sentido, este Instituto advierte que, en el instrumento jurídico celebrado entre la SEDENA, el AIFA, y las empresas Apollo Communications, S.A. de C.V., Química Apollo S.A de C.V., Vision-Box Soluções de Visão Por Computador S.A., y Amadeus IT Croup, S.A., estableció las figuras del responsable de jurídico y de responsable de administración aeroportuaria, así como del encargado.

Sin embargo, y considerando las características del responsable en términos de la Ley General, se desprende una disparidad entre esa definición con las que se denominó "responsable jurídico" y "responsable de administración aeroportuaria", dado que solamente el AIFA es quien puede ostentar el carácter de responsable para efectos de la normatividad en materia de protección de datos personales en posesión de sujetos obligados.

Este Instituto advierte que si bien fue la SEDENA quien celebró el contrato que incluyó, entre otros sistemas, el Sistema de Procesamiento, esto de forma previa a la emisión y publicación de la Concesión AIFA, lo cierto es que dicha solución debió ser celebrada considerando al AIFA, en tanto que como se ha insistido a lo largo del presente dictamen, es quien ostenta el carácter de responsable para efectos del tratamiento de datos personales, ya que es quien se encuentra facultado para prestar el servicio complementario de tráfico de pasajeros en dicho aeropuerto.

Finalmente, para aquellos enrolamientos en mostrador mediante V bMostrador convencional CUPPS-VDesk, este Instituto no advierte instrumento jurídico o relación con las empresas que realicen la venta de boletos de avión, aun cuando de la evaluación de impacto se desprende que dicho personal podría realizarlo, cuando ello es una función que el AIFA manifestó sería parte del tratamiento dentro del Sistema de Procesamiento.

Temas específicos de licitud relacionados con el enrolamiento en el Sistema de Procesamiento

Como se describió en el apartado denominado "IV. Descripción del Sistema de Procesamiento de Pasajeros del AIFA, contexto y justificación de la evaluación de impacto", existen tres medios a través de los cuales los titulares pueden capturar sus datos biométricos, así como de los datos insertos en el pasaporte electrónico, que son: V bMostrador convencional CUPPS-VDesk, Aplicación móvil y Quiosco de autoservicio - CUSS. En todos se desprende un proceso de enrolamiento, con el propósito de facilitar el tránsito de personas y pasajeros para abordar alguno de los vuelos con terminal de origen en el Aeropuerto Internacional Felipe Ángeles.

El enrolamiento debe distinguirse de la verificación biométrica, pues el primero implica la captación de datos biométricos para realizar la identificación de las personas para efectos de establecer su identidad, mientras que el segundo implica únicamente su contraste con un registro previamente tomado para corroborar que la persona que se ostenta como tal lo sea para dichos efectos.

En este punto es oportuno destacar que la importancia del principio de licitud dentro del tratamiento de datos biométricos radica en las garantías de que el tratamiento estará sujeto a controles incluso

desde la construcción de la norma habilitante, pues su aprovechamiento resulta muy intrusivo para los derechos y libertades fundamentales de las personas físicas, esto ya que se tiene plena constancia de la identidad de la persona de la que se obtuvieron, esto mediante el enrolamiento.

Lo anterior debe ser sumado a los restantes datos personales que serán recabados con dicha biometría, pues debe considerarse que su tratamiento debe obedecer a los principios y deberes previstos en la Ley General.

Ahora bien, es preciso tener en cuenta que, conforme a la descripción del Sistema de Procesamiento, este Instituto advierte que los procesos efectuados mediante la aplicación móvil y Quiosco de autoservicio – CUSS se puede utilizar únicamente el pasaporte electrónico; mientras que para el caso de V bMostrador convencional CUPPS-VDeskm, se puede utilizar ese documento, el pasaporte físico y la credencial para votar.

Sin embargo, en el "Anexo 4. MANUALES DE OPERACIÓN" en el documento denominado "Especificación del sistema – Registro asistido" se señala de forma textual:

> *4.1.1.8 Documentos elegibles*
> *La siguiente lista indica los documentos respaldados para la inscripción de pasajeros:*
> *- Pasaporte electrónico*
> *- Pasaporte*
> *- Tarjeta de identificación mexicana*
> ***- Licencia de conducir mexicana***
>
> ***[Énfasis añadido]***

Como se advierte, adicionalmente a lo mencionado en la evaluación de impacto y en el requerimiento de información adicional, se considera a la licencia como documento viable para la inscripción de los usuarios.

Sobre el uso específico del pasaporte electrónico, es oportuno considerar el Acuerdo del pasaporte electrónico, se establece que los pasaportes ordinario, oficial y diplomático serán de lectura mecánica con un circuito integrado sin contacto donde se almacena la información de la página de datos, una medición biométrica del titular del pasaporte y un objeto de seguridad para proteger los datos con una tecnología criptográfica, conocido como pasaporte electrónico, esto conforme al Documento 9303 emitido por la OACI.

En ese sentido, dentro de ese documento se estableció que los documentos de viaje de lectura mecánica desempeñan un papel cardinal en todo sistema moderno dedicado a ese fin, relacionado con las resultantes mejoras en materia de seguridad, rapidez de despacho y confianza en la

exactitud de la verificación que tales sistemas proporcionan y estima que su uso en los sistemas de despacho automatizados puede permitir a los estados prescindir de documentos en papel tales como los manifiestos de pasajeros y las tarjetas de embarque/desembarque, eliminando así los costos administrativos relacionados con los procedimientos manuales conexos.

Por lo expuesto, se desprende que la finalidad del pasaporte electrónico es permitir la mejora en materia de seguridad, rapidez de despacho y confianza en la exactitud de la verificación en los sistemas de despacho automatizados que puede permitir a los estados prescindir de documentos en papel tales como los manifiestos de pasajeros y las tarjetas de embarque/desembarque, así como en las cuestiones de seguridad inherentes a los servicios aeroportuarios.

Por lo tanto, si bien en principio se advierte que, si bien la finalidad de la expedición del pasaporte electrónico es agilizar los procesos mediante los cuales se realiza la documentación de pasajeros, esto establecido tanto en el Acuerdo del pasaporte electrónico como en el Documento 9303, sin embargo, ello debe ir acompañado de criterios mínimos para ese aprovechamiento.

Cabe puntualizar en este punto que el proceso en V bMostrador convencional CUPPS-VDeskm, se advierte la descripción de un proceso de verificación visual de la identidad para los casos en que se presente un pasaporte emitido antes del Acuerdo del pasaporte electrónico o la credencial para votar expedida por el INE, aunque en el documento denominado "Propuesta técnica Experiencia sin contacto en aeropuertos con tecnología biométrica", este Instituto advierte que dentro del apartado "Registro asistido en mostradores de documentación (OPCIONAL)" además del proceso relacionado con el pasaporte electrónico, también se contempla lo siguiente:

> *"[...]*
> *Tarjeta INE mexicana – Captura de rostro y huellas dactilares; escaneo del documento y verificación con el sistema del INE.*
> *[...]"*

En ese sentido, este Instituto no tiene certeza de que procesos serán aplicados para validar los casos del pasaporte emitido antes del Acuerdo del pasaporte electrónico y la credencial para votar, aunado a lo establecido en el documento aludido, genera incertidumbre en esos casos.

En el caso del INE, en atención a la exhaustividad que debe regir en la emisión de dictámenes, es oportuno considerar que el Servicio de Verificación proporcionado por el INE en los acuerdos CG92 como en el CG91, de los cuales se desprende que aquellos datos personales de los electores que serán motivo de verificación por parte del INE para aquellas instituciones públicas y privadas que así lo soliciten son el nombre, apellido paterno, apellido materno y la Clave de Elector del ciudadano, así como, de ser necesario, las huellas dactilares del dedo índice de ambas manos y los rasgos faciales siempre que se cubran los costos respectivos por parte de quien lo utilice, así

como en todos los casos debe recabarse el consentimiento expreso, pues ello puede ser materia de requerimiento por parte del INE.

Establecido lo previo, es oportuno señalar que el AIFA no acreditó la celebración de convenios con el INE para efectos del servicio de verificación, y aun en el supuesto de que los remitiera, ello no serviría para realizar el enrolamiento para aquellas personas que presenten su pasaporte emitido antes de la vigencia del Acuerdo del pasaporte electrónico.

Tampoco se desprende que el AIFA remitiera las reglas aplicables para aquellos enrolamientos de personas extranjeras que utilicen el Aeropuerto Internacional Felipe Ángeles para abordar algún vuelo.

Finalmente, es oportuno precisar al AIFA que este Instituto no tiene atribuciones para determinar por sí mismo las medidas que deben cumplirse en materia de protección de datos, pues su deber de vigilancia y atribuciones de coadyuvancia y apoyo devienen de la Ley General y sus Lineamientos, por lo que, en principio, la actuación de este Instituto se encuentra sustentada en dichos ordenamientos.

En términos de lo señalado previamente, se advierte que los supuestos de tratamiento de datos personales que se describen en Sistema de Procesamiento y, que, en el marco de su implementación, podrían tener incidencia en la **licitud** del tratamiento de datos personales, dan lugar a las recomendaciones siguientes:

Recomendaciones en torno al principio de licitud

Clave	Recomendación
AIFA_LI_001	Se recomienda realizar una verificación de forma constante las reformas al marco normativo aplicable, tanto nacional como internacional, relacionadas con el tratamiento de datos biométricos para el tráfico de personas dentro de las instalaciones del Aeropuerto Internacional Felipe Ángeles, esto como servicio complementario en términos de la Ley de Aeropuertos y su Reglamento. De manera particular, el responsable deberá corroborar que el tratamiento de datos personales biométrico sea congruente y coherente con los estándares aplicables, como en el caso de los previstos por la OACI.
AIFA_LI_002	Se recomienda realizar un análisis sobre el tratamiento de datos personales en consideración con la normatividad que le aplica al sujeto obligado y se relacionada con el servicio complementario de tráfico de pasajeros y que apliquen a México a fin de considerar los alcances y finalidades de esto.

AIFA_LI_003	Se recomienda, realizar el tratamiento de datos personales en sistemas o plataformas informáticas en las que tenga poder de decisión sobre estos.
AIFA_LI_004	Se sugiere considerar lo manifestado en el principio de licitud con la finalidad de poder incluir lo respectivo en el instrumento jurídico celebrado para que la SEDENA a fin de que las figuras jurídicas sean apegadas la normatividad en materia de datos personales.
AIFA_LI_005	Se sugiere considerar lo manifestado en el principio de licitud y demás principios, a fin de poder plasmar lo referente en el instrumento jurídico celebrado para establecer SEDENA y las empresas Apollo Communications, S.A. de C.V., Química Apollo S.A de C.V., Visión Box Soluções de Visão Por Computador S.A., y Amadeus IT Group, S.A. a fin de que puedan atende lo previsto en la normatividad de protección de datos personales y se considere con precisión los deberes en el marco del Sistema de Procesamiento.
AIFA_LI_006	Se recomienda considerar que la implantación de la mayoría de las tecnologías biométricas es susceptible de desarrollo ulterior ante la rapidez de los cambios tecnológicos; por lo que toda especificación debe tener en cuenta y reconocer que existirán cambios resultantes de las mejoras tecnológicas; siempre ajustado a los principios y deberes establecidos en la Ley General.
AIFA_LI_007	Se sugiere ceñirse a las figuras de responsable y encargado previstas en la Ley General y el apartado relativo para la celebración de la reestructuración del instrumento jurídico celebrado.
AIFA_LI_008	Se sugiere considerar lo manifestado en el presente principio en los instrumentos jurídicos celebrados con motivo del Sistema de Procesamiento y en el que se consideren los deberes del responsable y encargado previstas en la Ley General y en los Lineamientos en relación al cómputo en la nube.
AIFA_LI_009	Se sugiere que el AIFA en su carácter de responsable y en atención al Sistema de Procesamiento, se pueda considerar la emisión de instrumentos jurídicos necesarios para que las aerolíneas realicen el enrolamiento en mostrador, conforme lo previsto en el artículo 59 de la Ley General.
AIFA_LI_010	Se recomienda que el AIFA emita los instrumentos jurídicos necesarios para que las aerolíneas realicen el enrolamiento en mostrador, conforme lo previsto en el artículo 59 de la Ley General.
AIFA_LI_011	Respecto del enrolamiento de personas extranjeras en el Sistema de Procesamiento, se recomienda identificar la normatividad que permite

	efectuarlo, considerando en su caso los documentos emitidos por la OACI y la Ley General, los Lineamentos y demás legislación en la materia.
AIFA_LI_012	Se sugiere realizar un análisis sobre los documentos de identidad que se pretenden aceptar en el marco del Sistema de Procesamiento a fin de homologar los procedimientos de recabo descritos, asimismo, en caso de considerar viables la incorporación de otros documentos, se sugiere contemplar la normatividad aplicable, así como los principios y deberes establecidos en la Ley General, para poder llevar a cabo la correcta implementación del aludido sistema.

1.2. Principio de finalidad

El artículo 18 de la Ley General establece lo siguiente:

*"**Artículo 18.** Todo tratamiento de datos personales que efectúe el responsable deberá estar justificado por finalidades concretas, lícitas, explícitas y legítimas, relacionadas con las atribuciones que la normatividad aplicable les confiera.*

El responsable podrá tratar datos personales para finalidades distintas a aquéllas establecidas en el aviso de privacidad, siempre y cuando cuente con atribuciones conferidas en la ley y medie el consentimiento del titular, salvo que sea una persona reportada como desaparecida, en los términos previstos en la presente Ley y demás disposiciones que resulten aplicables en la materia."

Por su parte, los artículos 9 y 10 de los Lineamientos generales indican:

*"**Principio de finalidad***

***Artículo 9.** Para efectos de lo previsto en el artículo 18, primer párrafo de la Ley General y los presentes Lineamientos generales se entenderá que las finalidades son:*

- ***I.** Concretas: cuando el tratamiento de los datos personales atiende a la consecución de fines específicos o determinados, sin que se admitan errores, distintas interpretaciones o provoquen incertidumbre, dudas o confusión en el titular.*
- ***II.** Explícitas: cuando las finalidades se expresan y dan a conocer de manera clara en el aviso de privacidad;*
- ***III.** 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, y*
- ***IV.** 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.*

Tratamiento para finalidades distintas

> ***Artículo 10.*** *En el tratamiento de datos personales para finalidades distintas a aquellas que motivaron su tratamiento original a que se refiere el artículo 18, segundo párrafo de la Ley General, el responsable deberá considerar:*
>
> *I. La expectativa razonable de privacidad de la titular basada en la relación que tiene con éste;*
> *II. La naturaleza de los datos personales;*
> *III. Las consecuencias del tratamiento posterior de los datos personales para el titular, y*
> *IV. Las medidas adoptadas para que el tratamiento posterior de los datos personales cumpla con las disposiciones previstas en la Ley General y los presentes Lineamientos generales."*

De lo anterior, se desprende que el responsable tiene la obligación de definir las finalidades concretas, lícitas, explícitas y legítimas a que serán sometidos los datos personales para cumplir con los objetivos que persigue, los cuales, en todo momento, deberán ser acordes con las atribuciones que la normatividad aplicable le confiera a éste.

Se entenderá que las finalidades son:

- **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:** 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, en su caso, 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.

En caso de que el responsable pretendiera tratar los datos personales para finalidades distintas a las originalmente previstas, podrá hacerlo siempre y cuando cuente con atribuciones conferidas en la ley y solicite el consentimiento del titular.

Sobre el particular, en la Evaluación de impacto, el AIFA manifestó lo siguiente:

> ***"III. Objetivos generales y específicos.***
> ***Objetivo Generales:***
> *Optimizar el procesamiento de pasajeros, agilizando los procesos de pre-seguridad y abordaje, mediante la implementación de sistemas biométricos y sin contacto, para optimizar el uso de infraestructura del aeropuerto, generar eficiencias operativas para el aeropuerto, las aerolíneas y los operadores aeroportuarios, creando una mejor experiencia para el pasajero.*

Objetivos Específicos:

Beneficios para el pasajero:

• Experiencia sin contacto.

• Minimiza el uso papel.

• Auto-servicio.

• Reduce el tiempo de procesamiento para pasar a los filtros de pre-seguridad y realizar el embarque a la aeronave de manera rápida y segura.

Beneficios para la aerolínea:

• Optimiza el uso de recursos humanos.

• Reduce el tiempo de documentación y abordaje, acelerando el flujo de salida de pasajeros.

• Permite la validación automatizada de la identidad del pasajero.

• Disminuir reclamo de pasajeros por atraso a sus vuelos.

Beneficios para el aeropuerto:

• Posiciona al AIFA como un aeropuerto de clase mundial y vanguardista.

• Acelera los tiempos de procesamiento de pasajeros y reduce el congestionamiento de las áreas críticas (Pre-seguridad y abordaje).

• Fortalece el proceso de seguridad mediante la identificación de pasajeros que ingresan a la zona de Pre-seguridad y confirmando la validez del pase de abordar con las aerolíneas.

• Permite contar con información estadística del número de pasajeros que ingresan a los filtros de seguridad y realizan el abordaje mediante el uso de los e-gates (esta información no incluye datos personales).

• Permite desahogar áreas que son críticas: Pre-seguridad y abordaje, en consecuencia, permite a los pasajeros estar en mejor disposición y disponer de más tiempo para consumir alimentos, bienes y servicios en el área comercial del aeropuerto."

...]

VII. Finalidades del tratamiento intensivo o relevante de datos personales.

La finalidad del tratamiento de datos personales dentro de la solución de procesamiento de pasajeros consiste en:

Finalidades Concretas

Finalidad CUPPS: Realizar el registro biométrico, en sitio y asistido por un agente, en los mostradores convencionales de documentación (Check-in), con la finalidad de permitir el proceso de flujo ininterrumpido para el acceso de los pasajeros a salas de última espera. Realizando la validación de existencia y coincidencia entre los registros biométricos.

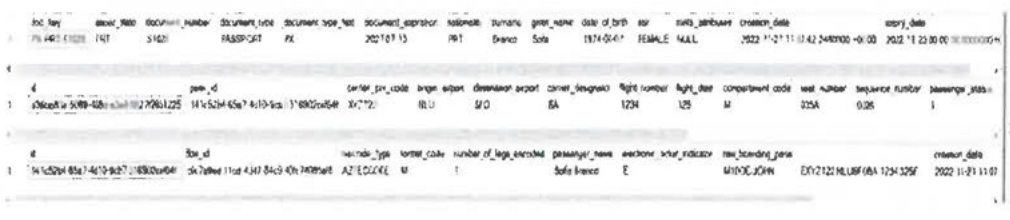
Finalidad APP: Esta empresa realiza la validación del pasajero, permitiendo identificar al pasajero por los puntos de validación desde el ingreso a salas de última espera, hasta el abordaje a la aeronave.

Finalidad quiosco de autoservicio: Ofrecer al pasajero la posibilidad de realizar el registro biométrico, en sitio, de manera autónoma, a través de los quioscos de autoservicio de documentación/checkin. Permite realizar la validación del pasajero, su identificación por los puntos de validación desde el ingreso a salas de última espera, hasta el abordaje.

Finalidades Explicitas *Estas se mencionan en los avisos de privacidad dentro del apartado de "finalidad".*

Finalidades Legitimas

1. Anexo 17 al Convenio sobre Aviación Civil Internacional, Capitulo 3 "Entrada y salida de personas y de su equipaje"
2. Items. 3.7, 3.8 y 3.9, del Inciso "C". Seguridad de los documentos de viaje.
3. Items. 3.35.1, del Inciso "I" Inspección de documentos de viaje.
4. Artículo 47 Bis 4. de la Ley de Aviación Civil y Articulo 46 y 47 de la Ley de Aeropuertos, Artículo 152, fracciones I, II, III y V. del Reglamento de la Ley de Aeropuertos.
5. 6.1, párrafo 7 y 8, Relevancia del objetivo prioritario 1; 6.3, párrafo 4; Relevancia del objetivo Prioritario 3, del ítem 6; Estrategias prioritarias 1.3 del ítem 7, del Programa Institucional 2021-2024 de la Empresa de Participación Estatal Mayoritaria Aeropuerto Internacional Felipe Ángeles.
6. Manual de Organización General del AIFA, Numeral 3.2.4 Subdirección de Sistemas. Función: Evaluar y dirigir las actividades de planeación, desarrollo y soporte de los recursos tecnológicos, informático de redes y comunicaciones de voz, datos y video del AIFA. Para lograr esta finalidad existen dos opciones: Proceso No biométrico y Biométrico.
***Proceso no biométrico:** Se crean canales de comunicación entre los sistemas del aeropuerto y las aerolíneas, que permitan identificar la validez del pase de abordar.*
La información del pase de abordar no es almacenada en el AIFA.
***Proceso biométrico:** Se crea una identificación digital, PDE (Personal Data Envelope por sus siglas en inglés) que permitirá identificar y determinar la elegibilidad del pasajero para ingresar al área estéril del AIFA y realizar el embarque.*
Después de creado el PDE se almacena en la base de datos del AIFA, diariamente el sistema crea Galerías de Pre-Seguridad y Abordaje, las cuales son extractos de la base de datos de los PDEs de los vuelos de cada día, con el objetivo de optimizar la velocidad de búsqueda, coincidencia e identificación de pasajeros.
Los datos serán cancelados, conforme a lo descrito en el punto VI, Cancelación o Supresión de Datos Personales, del ítem 3, Representación del ciclo de vida de los datos Personales a tratar.
La plataforma vb orchestra™ gestiona todo el ciclo de vida de todos los PDE (creación, lectura, actualización y eliminación en los momentos adecuados). También garantiza que todas las interacciones y el progreso de los pasajeros se mantengan actualizados en los PDE correspondientes, manteniendo todas las relaciones entre los diferentes PDEs. El PDE se utiliza como una identificación digital por una sola vez. Esto quiere decir que se utiliza un PDE por pasajero por viaje de salida. Cada vez que el pasajero realice un viaje por el AIFA y desee vivir la experiencia biométrica deberá registrarse/enrolarse. Todos los datos personales almacenados y transmitidos o transferidos están encriptados de forma segura, siendo solo accesible a los usuarios acreditados con los privilegios apropiados. Los PDEs tienen un tamaño máximo 1.3MB, según el método de registro o enrolamiento. Los datos están almacenados en locaciones lógicas diferentes de manera encriptada (AES 256) dentro de la base de datos.



Ejemplo de los campos que son empleados para la construcción de un PDE.
Un ejemplo de casos de uso de registro biométrico se encuentra en el documento Experiencia sin contacto con tecnología biométrica, Gestión de Datos Personales, Solución Biométrica, 2 Descripción de la Solución, Diagrama "Descripción de la solución de biometría como componente de la solución de procesamiento de pasajeros".

Por otro parte, en el desahogo al requerimiento de información adicional, respecto al principio en cuestión

***5.** [...]*
***La finalidad general:** se consideran elementos de automatización para el procesamiento de pasajeros y sus bienes, privilegiando la infraestructura de uso común, así como las funcionalidades para crear condiciones "touchless", "paperless", "contactless", en un entorno post Covid, así como, la creación de un entorno de procesamiento automatizado desde el check-in hasta el abordaje mediante el apoyo con tecnologías biométricas en balance con las tradicionales, el Proveedor implementara de la Plataforma Orchestra y los puntos de contacto de identificación biométrica "en movimiento" (onte move) o "pausa y marcha" (Stop and go) de Vision-Box, como el componente principal de Gestión biométrica para el procesamiento de pasajeros dentro del AIFA, integrada al sistema de uso común de Amadeus.*
La plataforma Orchestra de Vision-Box, junto con los puntos de contacto de identificación biométrica "en movimiento" (on the move) o "pausa y marcha" (Stop and go), serán los responsables por la gestión de la identidad digital del pasajero, a través de un token digital llamado PDE (Passenger Data Envelope), desde su creación, al momento del enrolamiento o registro, durante su evolución, a medida que circula por cada punto de control y hasta su eliminación, luego del abordaje en la aeronave. Permitiéndole al pasajero emplear su rostro como su identificación durante todo el proceso. Además de la integración con el sistema de uso común propuesto.
***Las finalidades específicas** que se encuentran en los avisos de privacidad son consideradas dentro de cada punto de registro y validación siendo las siguientes:*
• Vdesk: realizar el registro biométrico, en sitio y asistido por un agente, en los mostradores convencionales de documentación (Check-in).
• Quiosco: ofrecer al pasajero la posibilidad de realizar el registro biométrico, en sitio, de manera autónoma, a través de los quioscos de auto-servicio de documentación-check in.

• App: ofrece al pasajero la posibilidad de realizar un registro o enrolamiento biométrico en cualquier lugar y en cualquier momento, a través de la aplicación móvil del AIFA.
• Pre-seguridad: llevar a cabo la validación de existencia de un registro biométrico en la base de datos (galería de pre-seguridad) o en su defecto verificar la elegibilidad de acceso de un pasajero mediante el pase de abordar, para permitir el acceso al área de filtros de seguridad.
• Abordaje: llevar a cabo la validación de existencia de un registro biométrico en la base de datos (galería de abordaje) o en su defecto verificar la elegibilidad de acceso de un pasajero mediante el pase de abordar, para permitir el acceso a la aeronave, enviando un mensaje de confirmación de abordaje al sistema de control de salidas de la aerolínea.
***Las finalidades primarias** por las cuales se recaban datos personales no conllevan algún tipo de finalidades secundarias, esta es una de las razones por las que se considera que el PDE solo debe conservarse por un periodo de 24 hs.*
***Las finalidades licitas** están expresadas en el punto 3 del presente documento.*

Por lo que hace a los avisos de privacidad integrales remitidos en la evaluación de impacto, se señalan:

Aviso de privacidad integral del registro biométrico asistido mostrador convencional (vdesk)

Finalidad	¿Requieren consentimiento del titular?	
	NO	SI
Realizar el registro biométrico, en sitio y asistido por un agente, en los mostradores convencionales de documentación (Check-in), con la finalidad de permitir el proceso de flujo ininterrumpido para el acceso de los pasajeros a salas de última espera. Realizando la validación de existencia y coincidencia entre los registros biométricos.		X

Aviso de privacidad integral de la app

Finalidad	¿Requieren consentimiento del titular?	
	NO	SI
• Esta empresa realiza la validación del pasajero, permitiendo identificar al pasajero por los puntos de validación desde el ingreso a salas de última espera, hasta el abordaje a la aeronave.		X

Aviso de privacidad integral del sistema registro biométrico quiosco de autoservicio

Finalidad	¿Requieren consentimiento del titular?	
	NO	SI
Ofrecer al pasajero la posibilidad de realizar el registro biométrico, en sitio, de manera autónoma, a través de los quioscos de auto-servicio de documentación/checkin. Permite realizar la validación del pasajero, su identificación por los puntos de validación desde el ingreso a salas de ultima espera, hasta el abordaje.		X

Conforme a lo anterior, si bien existen múltiples fuentes de obtención de datos personales, es importante señalar que los mismo integran al Sistema de Procesamiento de Pasajeros del AIFA, asimismo, tienen el mismo objetivo, pero las vías son diferentes, en ese sentido se tiene que las finalidades del sistema en General son las siguientes:

- Crear y realizar el registro biométrico (enrolamiento biométrico) del pasajero mediante un token digital denominado PDE.
- Almacenar los datos personales del pasajero dentro de la plataforma vb orchestra.
- Identificar y validar biométricamente a los pasajeros en los puntos de validación desde el ingreso a salas de última espera, hasta el abordaje a la aeronave.
- Validar la existencia de registros biométricos para pasar a los filtros de pre-seguridad y realizar el abordaje.
- Permitir el flujo ininterrumpido para el acceso de los pasajeros para pasar a los filtros de pre-seguridad y realizar el embarque a la aeronave de manera rápida y segura.
- Transferir datos a las aerolíneas para avisar que el pasajero ha abordado la aeronave.
- Permitir el paso de los pasajeros que no realizaron su registro biométrico.
- Fortalecer el proceso de seguridad mediante la identificación de pasajeros que ingresan a la zona de pre-seguridad y confirmar la validez del pase de abordar con las aerolíneas.
- Contar con información estadística del número de pasajeros que ingresan a los filtros de seguridad y realizan el abordaje mediante el uso de los E-gates (esta información no incluye datos personales).
- Validar que no exista un enrolamiento/registro previo del pasajero

Es importante señalar que en la evaluación e impacto en el apartado denominado "VI. Cancelación o supresión de datos personales." se señala lo siguiente:

> *"[...]*
> *Después de 24 horas posteriores a la fecha de la salida del vuelo, se ejecuta una acción de borrado, de manera automática, de todos los PDE almacenados en las Galerías de la solución*

biométrica. Esto se realiza con el objetivo de asegurar el borrado de los datos de los pasajeros, debido a que podrían presentarse los siguientes casos:
Que el pasajero no ingrese al área estéril del aeropuerto o no realice el abordaje.
Que el pasajero use el procedimiento de pre-seguridad de manera tradicional, con la asistencia de un agente, presentando el pase de abordar de forma física.
Que el pasajero use el procedimiento de abordaje tradicional, presentando el pase de abordar de forma física.
Que el vuelo sea suspendido.
Que exista requerimiento de las autoridades (transporte de drogas ilegales, casos de ebriedad o bajo el influjo de estupefacientes, psicotrópicos o enervantes, otros)
[...]"

[Énfasis añadido]

Conforme a lo antés expuesto, se observa que el mismo responsable advierte la posibilidad de un requerimiento por parte de las autoridades ante situaciones de transporte de drogas ilegales, casos de ebriedad o bajo el influjo de estupefacientes, psicotrópicos o enervantes, otros, no obstante, no se proporcionó mayor información sobre este supuesto.

Lo anterior es de gran relevancia ya que deja abierta la posibilidad de supuestos en los que existan requerimientos por parte de las autoridades lo cual pudiera implicar una finalidad adicional a las manifestadas por el AIFA relativas a temas de seguridad, inclusive de seguridad nacional.

Por lo anterior, es de suma importancia que el responsable identifique si el tratamiento que se pretende llevar a cabo mediante el Sistema de Procesamiento y los datos personales que serán utilizados, tenga el alcance de que pueda ser, eventualmente, usado para finalidades adicionales como puede ser la atención al requerimiento de autoridades por causas de seguridad, inclusive de seguridad nacional.

Lo anterior, en razón de que, en caso de que esto sea así, tener en consideración que implica una finalidad distinta a aquéllas que motivaron su tratamiento original y sus implicaciones en el cumplimiento de los principios, deberes y obligaciones cambiaría a lo que se está considerando en el presente dictamen, por lo que, el AIFA, tendría que considerar: la expectativa razonable de privacidad del titular basada en la relación que tiene con éste; la naturaleza de los datos personales; las consecuencias del tratamiento posterior de los datos personales para el titular, y las medidas adoptadas para que el tratamiento posterior de los datos personales cumpla con las disposiciones previstas en la Ley General y sus Lineamientos generales, y en su caso, valorar la presentación de una nueva evaluación de impacto en virtud de que se estaría ante una modificación sustancial del funcionamiento del Sistema de Procesamiento.

Respecto a la cualidad de que las finalidades deben ser concretas, es posible advertir que existen finalidades que no son concretas pues las mismas no se materializan en fines específicos o claros relacionados con los procesos que se pretenden realizar, como son las finalidades para realizar con las aerolíneas, asimismo, no se encuentran contempladas todas las finalidades como podrían ser las consideradas con motivo del borrado de los datos.

Referente a la cualidad de ser explícitas, se advierte, existen múltiples finalidades que se pretenden llevar a cabo del tratamiento de datos personales, es importante señalar que se observa diferentes finalidades a las contempladas en los avisos de privacidad.

Por lo que hace a la cualidad de licitud, se deberá de considerar lo manifestado en el apartado de "1.1. Principio de licitud" del presente documento, pues es importante que las mismas sean acordes con las atribuciones o facultades del responsable.

Finalmente, por lo que hace a la legitimación es importante considerar lo previsto en el apartado "1.4 Principio de consentimiento" a fin de que el consentimiento del titular se encuentre habilitada por el consentimiento respectivo.

En ese sentido, se realizan las recomendaciones siguientes:

Recomendaciones en torno al principio de finalidad

Clave	Recomendación
AIFA_FI_001	Se recomienda considerar la totalidad de las finalidades que se pretenden realizar tanto en el aviso de privacidad integral como simplificado, de conformidad con los elementos para el cumplimiento del principio de información.
AIFA_FI_002	Se recomienda revisar a efecto de identificar claramente la totalidad de las finalidades que se pretendan realizar con motivo del tratamiento de datos, tomando en cuenta las consideraciones vertidas por este Instituto en el apartado de finalidad.
AIFA_FI_003	Se sugiere considerar lo manifestado en el principio de licitud a fin de poder identificar claramente la totalidad de las finalidades que se pretenden realizar con motivo del tratamiento de datos y verificar que éstas se encuentren de acuerdo a las atribuciones que facultan al AIFA.
AIFA_FI_004	Con relación a la posible finalidad de utilizar los datos personales recabados en el marco del Sistema de Procesamiento en materia de

	seguridad, se recomienda tomar en consideración lo respectivo, vertido en el principio de licitud.
AIFA_FI_005	Con base en la totalidad de las finalidades que se adviertan, se recomienda identificar todas aquellas en las que se requiere el consentimiento y aquellas que no lo requieren.
AIFA_FI_006	Se recomienda revisar e identificar si el tratamiento que se pretende llevar a cabo mediante el Sistema de Procesamiento tiene el alcance de que, eventualmente, atienda la finalidad de dar atención al requerimiento de autoridades competentes por causas de seguridad inclusive de seguridad nacional. En caso de que así sea, se recomienda considerar: la expectativa razonable de privacidad del titular basada en la relación que tiene con éste; la naturaleza de los datos personales; las consecuencias del tratamiento posterior de los datos personales para el titular, y las medidas adoptadas para que el tratamiento posterior de los datos personales cumpla con las disposiciones previstas en la Ley General y sus Lineamientos generales.
AIFA_FI_007	Se identifica que conforme los estándares aplicables para el uso de datos biométricos en el ámbito aeroportuario, eventualmente podrían agregarse finalidades o las finalidades existentes podrían ser modificadas, por lo cual, el responsable deberá identificar los cambios aplicables requeridos de conformidad con la normatividad de protección de datos personales y, en su caso, verificar la procedencia de presentación de una nueva evaluación de impacto en la protección de datos personales; razón por la cual, deberán identificarse dichas finalidades potenciales en el marco de la normatividad y estándares aplicables, e identificar dentro del documento de seguridad, si forman parte del alcance del tratamiento, si se encuentran excluidas, o, en su caso, si podrán ser susceptibles de consideración de manera posterior, para lo cual, deberá señalarse en el plan de trabajo respectivo o, en su caso, en el programa de protección de datos institucional.

1.3. Principio de lealtad

El artículo 19 de la Ley General establece lo siguiente:

> *"**Artículo 19.** El responsable no deberá obtener y tratar datos personales, a través de medios engañosos o fraudulentos, privilegiando la protección de los intereses del titular y la expectativa razonable de privacidad."*

Por su parte, el artículo 11 de los Lineamientos generales señala lo siguiente:

> *"**Principio de lealtad***
>
> ***Artículo 11.** En términos de lo dispuesto en el artículo 19 de la Ley General y los presentes Lineamientos generales, se entenderá:*
>
> ***I.** Por medios engañosos o fraudulentos aquellos que el responsable utilice para tratar los datos personales con dolo, mala fe o negligencia;*
>
> ***II.** Que el responsable privilegia los intereses del titular cuando el tratamiento de datos personales que efectúa no da lugar a una discriminación o trato injusto o arbitrario contra éste, y*
>
> ***III.** Por expectativa razonable de privacidad, la confianza que el titular ha depositado en el responsable respecto a que sus datos personales serán tratados conforme a lo señalado en el aviso de privacidad y en cumplimiento a las disposiciones previstas en la Ley General y los presentes Lineamientos generales."*

De lo anterior, este Instituto observa que el responsable no debe actuar de manera engañosa o fraudulenta respecto al tratamiento de los datos personales que lleve a cabo, para lo cual se entiende:

- Por medios engañosos o fraudulentos: aquéllos que el responsable utilice para tratar los datos personales con dolo, mala fe o negligencia.
- Que el responsable privilegia los intereses del titular: cuando el tratamiento de datos personales que efectúa no da lugar a una discriminación o trato injusto o arbitrario contra éste.
- Por expectativa razonable de privacidad: la confianza que el titular ha depositado en el responsable respecto a que sus datos personales serán tratados conforme a lo señalado en el aviso de privacidad y en cumplimiento a las disposiciones previstas en la Ley General y los Lineamientos generales.

Al respecto, en la Evaluación de impacto presentada por el AIFA, se mencionó lo siguiente en relación con el cumplimiento de este principio:

> ***IX. Forma en que se recabarán los datos.***
>
> *Forma en que se recabarán los datos personales o, en su caso, las fuentes de las cuales provienen;*
>
> *Para el **proceso biométrico**, los datos se recaban de la siguiente manera:*
>
> *a) Proceso de registro en la aplicación móvil del AIFA.*
>
> *1. El pasajero realiza una reservación con la aerolínea.*
>
> *2. El pasajero cuenta con su pase de abordar.*
>
> *3. El pasajero entra en la aplicación del AIFA.*
>
> *4. El pasajero acepta los términos del aviso de privacidad.*
>
> *5. El pasajero deberá escanear el pase de abordar.*

6. El pasajero deberá escanear el documento de identidad (pasaporte electrónico) con su teléfono móvil (MRZ y chip).
7. El SDK realiza la verificación del documento de identidad.
8. El SDK realiza la prueba de vida del pasajero.
9. El SDK realiza el match 1:1 entre el pasajero versus su documento.
10. El SDK envía los datos a la plataforma vb orchestra™
11. La plataforma vb orchestra™ crea el PDE.
*b) Proceso de registro en el **quiosco de autoservicio** (CUSS) del AIFA.*
1. El pasajero realiza una reservación con la aerolínea.
2. El pasajero ingresa a la aplicación de la aerolínea (DCS) en el quiosco de autoservicio. 3. La aerolínea genera el pase de abordar.
4. El pasajero imprime el pase de abordar en el Quiosco de autoservicio del AIFA.
5. En pantalla se muestra la solicitud de consentimiento de enrolamiento biométrico.
6. El usuario acepta los términos del aviso de privacidad.
7. El usuario deberá escanear el pase de abordar.
8. ACUS envía los datos del pase de abordar a la plataforma Vision Box vb orchestra.
9. El Quiosco envía la confirmación de lectura del pase de abordar.
10. El usuario escanea el pasaporte electrónico.
11. ACUS envía los datos del pasaporte a la plataforma Vision Box vb orchestra™.
12. La plataforma Vision Box vb orchestra™ valida que los datos sean iguales a los recabados en el pase de abordar.
13. Se envía mensaje de confirmación.
14. El quiosco toma una fotografía del pasajero y realiza la validación de la calidad de la misma (según las normas ISO19794-5).
15. Vb orchestra™ valida si ya existe un PDE asociado a este pasajero.
16. Vb orchestra™ verifica la identidad del pasajero.
17. Vb orchestra™ genera el PDE

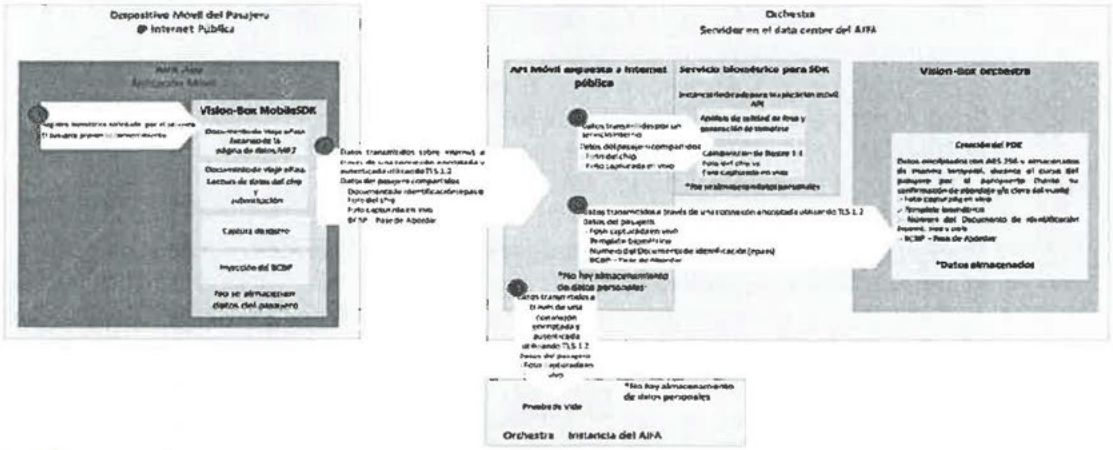
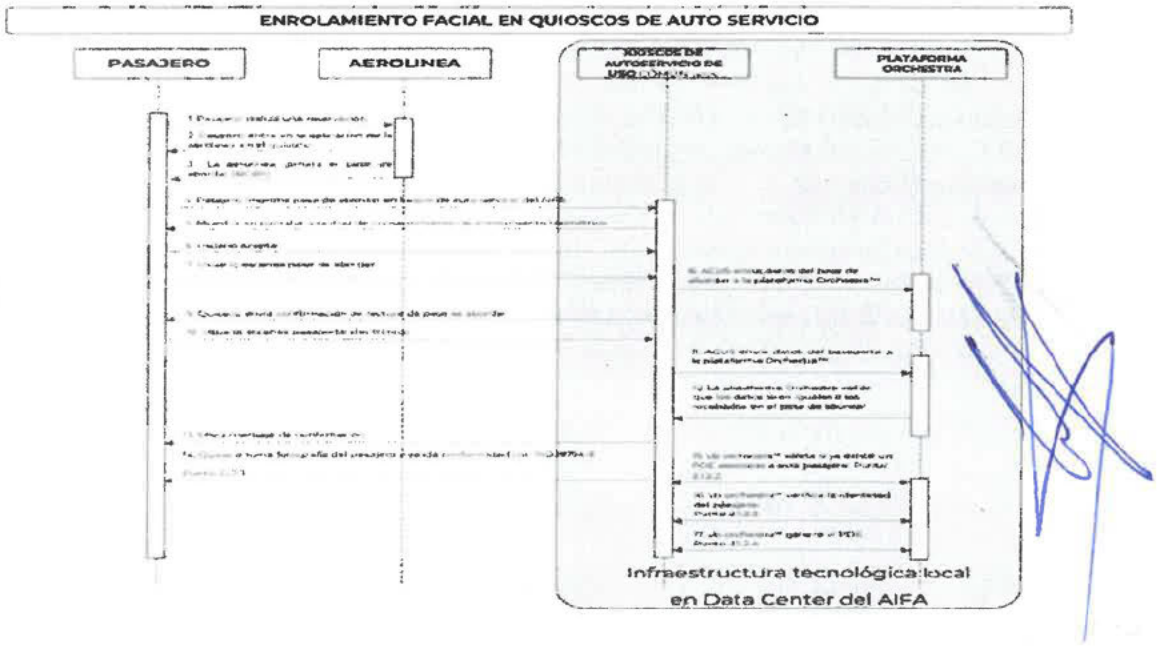


Diagrama del proceso de registro biométrico en APP.

*b) Proceso de registro en el **quiosco de autoservicio** (CUSS) del AIFA.*
1. El pasajero realiza una reservación con la aerolínea.
2. El pasajero ingresa a la aplicación de la aerolínea (DCS) en el quiosco de autoservicio. 3. La aerolínea genera el pase de abordar.
4. El pasajero imprime el pase de abordar en el Quiosco de autoservicio del AIFA.
5. En pantalla se muestra la solicitud de consentimiento de enrolamiento biométrico.
6. El usuario acepta los términos del aviso de privacidad.
7. El usuario deberá escanear el pase de abordar.
8. ACUS envía los datos del pase de abordar a la plataforma Vision Box vb orchestra.
9. El Quiosco envía la confirmación de lectura del pase de abordar.
10. El usuario escanea el pasaporte electrónico.
11. ACUS envía los datos del pasaporte a la plataforma Vision Box vb orchestra™.
12. La plataforma Vision Box vb orchestra™ valida que los datos sean iguales a los recabados en el pase de abordar.
13. Se envía mensaje de confirmación.
14. El quiosco toma una fotografía del pasajero y realiza la validación de la calidad de la misma (según las normas ISO19794-5).
15. Vb orchestra™ valida si ya existe un PDE asociado a este pasajero.
16. Vb orchestra™ verifica la identidad del pasajero.
17. Vb orchestra™ genera el PDE



c) Proceso de registro en el mostrador de documentación (CUPPS) y luego realiza registro biometrico en el vDesk del AIFA.

1. El pasajero reserva un vuelo con la aerolínea.
2. El usuario se presenta en el mostrador con una identificación oficial.
3. El agente de la aerolínea valida la coincidencia de la foto en el documento de identificación con el pasajero, de manera visual.
4. La aerolínea registra al pasajero e imprime el pase de abordar.
5. El personal de la aerolínea invita al pasajero a enrolarse en el sistema de procesamiento biométrico.
6. El pasajero acepta participar en el enrolamiento facial.
7. El agente de la aerolínea inicia proceso.
8. El pasajero deberá escoger el idioma de su preferencia (inglés o español).
9. Se muestra en pantalla el aviso de privacidad relativo al procesamiento de datos.
10. El pasajero otorga su consentimiento para el procesamiento de sus datos.
11. El agente de la aerolínea escanea el pase de abordar.
12. Se envían los datos por protocolo AIDX a través de la red local del AIFA.
13. Se almacena los datos en el Data Center del AIFA.
14. Se envía un mensaje de solicitud de escaneo de documento.
15. El agente valida visualmente que la identificación proporcionada corresponda al pasajero y procede con el escaneo del documento.
16. Se envían los datos correspondientes tomados del pase de abordar y de la identificación del pasajero a la plataforma de vb orchestra™.

17. Se realiza la validación de coincidencia del pase de abordar con la Identificación y se almacenan los datos en plataforma vb orchestra™ (Data Center AIFA) para su procesamiento.
18. Se activa el dispositivo Vdesk para la captura de imagen facial, colocando automáticamente la cámara a la altura de los ojos para una mejor calidad.
19. El dispositivo vDesk realiza una prueba de vida, para asegurar que quien realiza el proceso sea una persona viva.
20. Se toma la fotografía.
21. Se almacenan datos biométricos en el Data Center del AIFA y se genera el PDE.
22. Se envía mensaje de registro exitoso.
23. El agente finaliza el enrolamiento y entrega los documentos al pasajero.

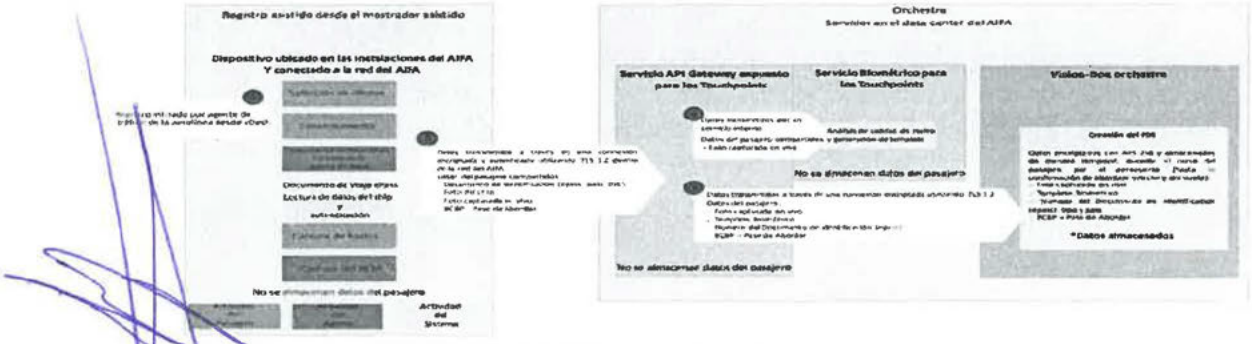


Diagrama ilustrativo del registro biométrico vía el vDesk en el mostrador de documentación del AIFA

Nota: En caso de que el pasajero no de su consentimiento para realizar el enrolamiento biométrico podrá realizar su procesamiento e identificación (en el área de pre-seguridad y abordaje) de la forma tradicional, presentando su pase de abordar.

[...]

4. Representación del ciclo de vida de los datos personales a tratar.

I. Fuentes.

Fuentes, así como los medios y procedimientos a través de los cuales se recabarán los datos personales.

I. Obtención de los datos personales (Registro) *En el sistema tenemos diferentes formas de registro de datos personales de los pasajeros:*

a) Documentación/Check-in, en modo no biométrico. Que corresponde a la documentación tradicional del pasajero, donde se le entrega su pase de abordar (BCBP). b) Documentación/Check-in, con modo biométrico. Donde adicional al BCBP, se realiza el enrolamiento o registro biométrico.

o Quioscos de documentación.
o Mostradores de documentación (VDESK).
o Aplicación Móvil AIFA.

Los datos personales obtenidos para el procesamiento de pasajeros en modo biométrico son los siguientes:

a) Quioscos de autoservicio (CUSS) Los datos que se reciben del quiosco son los siguientes:

• Datos del dispositivo (quiosco)

1. Nombre del dispositivo
2. Tipo de Dispositivo
3. Nombre del aeropuerto
4. Número de Terminal
5. Código de Aerolínea
6. Vendedor
7. Horario

• Datos del documento del pasajero (Pasaporte electrónico)

1. Nombre completo
2. Fecha de nacimiento
3. País de Nacionalidad
4. Género
5. Tipo de documento
6. Número de documento
7. País de emisión de documento
8. Fecha de expiración del documento

• Datos del Pase de Abordar

1. Tipo de Código de Barra
2. Formato de Código
3. Indicador de Ticket Electrónico
4. RAW
5. Nombre del Pasajero
6. Código PNR
7. Aeropuerto de Origen
8. Aeropuerto de Destino
9. Código del Carrier
10. Número de Vuelo
11. Fecha del Vuelo
12. Código de Compartimiento
13. Número de Asiento
14. Número de Secuencia
15. Estatus del Pasajero
16. Número Serial del Documento
17. Leg Order

• Datos de la fotografía

1. Foto (vector)
2. Id de la cámara

b) Mostradores de documentación CUPPS-Vdesk.

Los datos que se reciben del Mostrador de documentación (CUPPS) a través del VDESK son los siguientes:

• Datos del dispositivo
1. Nombre del dispositivo (VDESK)
2. Tipo de Dispositivo
3. Nombre del aeropuerto
4. Número de Terminal
5. Código de Aerolínea
6. Vendedor
7. Horario

• Datos del documento del pasajero (INE)
1. Nombre completo
2. Número de documento
3. País de Nacionalidad
4. Fecha de Validez del documento
5. Género

• Datos del documento del pasajero (Pasaporte no electrónico)
1. Nombre completo
2. Número de pasaporte
3. País de Emisión
4. País de Nacionalidad
5. Fecha de validez del documento
6. Fecha de Nacimiento
7. Género

• Datos del documento del pasajero (Pasaporte electrónico)
1. Fecha de Nacimiento
2. Número de documento
3. Nombre completo
4. País de Nacionalidad
5. País de Emisión
6. Fecha de Validez del documento
7. Género

• Datos del Pase de Abordar
1. Tipo de Código de Barra
2. Formato de Código
3. Indicador de Ticket Electrónico
4. RAW
5. Nombre del Pasajero
6. Código PNR
7. Aeropuerto de Origen
8. Aeropuerto de Destino
9. Código del Carrier

10. Número de Vuelo
11. Fecha del Vuelo
12. Código de Compartimiento
13. Número de Asiento
14. Número de Secuencia
15. Estatus del Pasajero
16. Número Serial del Documento
17. Leg Order
• Datos de la fotografía
1. Foto (vector)
2. Id de la cámara
c) Aplicación móvil AIFA.
• Los datos leídos del pasaporte electrónico para el procesamiento del pasajero son los siguientes:
1. Nombre completo
2. Fecha de nacimiento
3. País de Nacionalidad
4. Género
5. Tipo de Documento
6. Número de documento
7. País de emisión de documento
8. Fecha de expiración del documento
9. Foto del chip del pasaporte
10. Foto capturada por el dispositivo móvil (vector)
• Datos del Pase de Abordar
1. Tipo de Código de Barra
2. Formato de Código
3. Indicador de Ticket Electrónico
4. RAW
5. Nombre del Pasajero
6. Código PNR
7. Aeropuerto de Origen
8. Aeropuerto de Destino
9. Código del Carrier
10. Número de Vuelo
11. Fecha del Vuelo
12. Código de Compartimiento
13. Número de Asiento
14. Número de Secuencia
15. Estatus del Pasajero
16. Número Serial del Documento
17. Leg Order d

) Modo no biométrico. Los datos que se obtienen del pase de abordar son los siguientes: 1. Tipo de Código de Barra
2. Formato de Código
3. Indicador de Ticket Electrónico
4. RAW
5. Nombre del Pasajero
6. Código PNR
7. Aeropuerto de Origen
8. Aeropuerto de Destino
9. Código del Carrier
10. Número de Vuelo
11. Fecha del Vuelo
12. Código de Compartimiento
13. Número de Asiento
14. Número de Secuencia
15. Estatus del Pasajero
16. Número Serial del Documento
17. Leg Order
[…]"

Por su parte, en el desahogo de requerimiento de información adicional, el AIFA señaló lo siguiente con relación al cumplimiento de este principio:

"En cuanto al principio de lealtad, en el artículo 19 de la ley general de datos, contempla el deber del responsable de demostrar el tratamiento apegado a la normatividad y que la obtención del titular no se realizó a través de medios engañosos o fraudulentos, así mismo que se privilegie la protección de los intereses del titular y la expectativa razonable de privacidad; en el que se confirme que el tratamiento no da lugar a discriminación o trato injusto orbitario en contra del titular, por lo cual, deberá señalar las razones que se consideren sustenta en el cumplimiento de este principio por parte del responsable.
Además de lo ya mencionado, en los avisos de privacidad (simple e integral) se ve reflejada la obtención del consentimiento expreso del particular, así como las finalidades por las cuales se recaban los datos, así como las transferencias que para el procesamiento de pasajeros se requieran, lo anterior en cumplimiento a lo que dispone el último párrafo del artículo 21 de la LGTAIP, que expresa que tratándose de datos personales sensibles el responsable deberá obtener el consentimiento expreso y por escrito del titular para su tratamiento, a través de mecanismos como el de autenticación que se establezca.
A mayor abundamiento, el proceso de validación de identidad se realiza de la siguiente manera: Paso Uno: será mostrado el aviso de privacidad simplificado en el que también se da a conocer en donde se puede consultar el aviso de privacidad integral, si este aviso no es aceptado por el titular, se finaliza el proceso de enrolamiento.
Paso Dos: Una vez aceptado el dicho aviso se procede a realizar la validación de identidad 1:1 cruzando los valores de los vectores obtenidos de la imagen del documento de identidad

con los vectores de la imagen capturada en tiempo real, la cual permite identificar que efectivamente sea el titular quien está dando la aceptación del aviso de privacidad
En caso de no encontrar coincidencias, es finalizado el proceso de enrolamiento y no es almacenado ninguno de los datos leídos. En la página web será publicado el procedimiento de enrolamiento para conocimiento de los particulares, como un ejercicio del principio de información.
De conformidad con el artículo 25 de la ley general de datos, referente al principio de proporcionalidad, si bien, se identifican los datos personales requeridos para cada finalidad, hoy se solicita indicar los esfuerzos razonables y que se han realizado para limitar los datos personales tratados al mínimo necesario, con relación a la finalidad que motiva su tratamiento. así mismo, indicar las razones y justificaciones por las cuales se determina que los datos personales tratados son adecuados, relevantes y estrictamente necesarios, de conformidad con el artículo 24 de los lineamientos generales.
En relación con la finalidad definida del tratamiento de los datos guarda relación únicamente con el procesamiento y abordaje de los usuarios, el hecho de guardarlos por un tiempo mayor, incluso, podría considerarse como un incumplimiento al criterio de minimización señalado en el articulo 25 de los lineamientos.
Cabe mencionar que La solución de gestión de identidades Vision-Box, vb orchestra™, cuenta con la certificación "Privacy by Design (PbD)". Esto significa que los datos personales de los pasajeros (biográficos y biométricos) serán gestionados por una plataforma de software que fue diseñada con la máxima protección y privacidad y con un riesgo minimizado de fuga.
El PbD se encuentra apegado a las regulaciones de gestión de datos personales, incluidas las regulaciones GDPR (General Data Protection Regulation) de la Unión Europea, también se tienen en cuenta al diseñar la plataforma Orchestra.
General Data Protection Regulation o, en español, Reglamento General de Protección de Datos teniendo como principio de implementación la Minimización de datos, así como en el propósito delimitado de recolectar datos personales adecuados y relevantes para la finalidad.
Con relación a la "expectativa razonable de privacidad; en el que se confirme que el tratamiento no da lugar a discriminación o trato injusto orbitario en contra del titular, por lo cual, deberá señalar las razones que se consideren sustenta en el cumplimiento de este principio por parte del responsable."
Se encuentra agotado en el punto inmediato anterior, este incluye el curso "Tronco común", en el que se contempla la información correspondiente a Derechos Humanos, para prevenir la discriminación de los usuarios del AIFA.
En el documento Experiencia sin contacto con tecnología biométrica. Gestión de Datos Personales, Solución Biométrica, 2.1 Puntos de Registro o Enrolamiento Biométrico, se puede apreciar el detalle de estos procesos en los Diagramas de flujo ilustrativos del registro biométrico a través de la Aplicación móvil del AIFA, del quiosco de autoservicio (CUSS) y del mostrador de documentación (CUPPS/Vdesk).
[…]"

En primer término, de conformidad con lo señalado previamente en cuanto a este principio, se identifica que, por lo que hace a los medios de obtención de los datos personales, este Instituto

advierte que existen múltiples avisos de privacidad, relacionados con los medios con los que se realiza el enrolamiento de las personas que utilizaran el Sistema de Procesamiento.

Si bien existen consideraciones específicas que este Instituto realizara en el apartado relacionado con el principio de información, es oportuno señalar que es recomendable que siempre las circunstancias lo permitan, evitar expedir múltiples avisos de privacidad, pues ello puede llevar a la confusión a los particulares respecto del tratamiento de sus datos personales.

Igualmente es oportuno considerar que en los avisos de privacidad exhibidos no cuentan con un apartado relacionado con los derechos ARCO, que, si bien cuenta con una sección específica dentro del dictamen que se emite, para efectos del principio en estudio es importante señalar que para generar en los titulares una expectativa razonable de privacidad, es importante que dichos apartados se encuentren presentes en los avisos de privacidad.

Igualmente, los particulares deben contar con los elementos suficientes para conocer los datos que serán objeto de tratamiento de datos personales, los periodos de conservación y la destrucción después de que culminen los periodos de conservación respectivos.

No pasa desapercibido a este Instituto que el AIFA señaló que 24 horas después de la salida del vuelo de dicho aeropuerto la información recabada sería destruida, esto ya que, si bien dentro del principio de calidad se realizarán las precisiones correspondientes, es importante que el AIFA establezca puntualmente las razones por las que ese plazo fue elegido, esto considerando que dicha información podría serle útil al titular con posterioridad a su utilización en el Sistema de Procesamiento.

Aunado a lo anterior, es importante señalar que el PDE podría tratarse de información relacionada con documentos de archivo en términos del artículo 4, fracción XXIV, cuya destrucción constituye una infracción en términos del artículo 116, fracción VI, de la LGA. Igualmente, el sujeto obligado fue omiso en exhibir ante este Instituto su Catálogo de Disposición Documental, relacionado con los periodos de conservación de la información.

También se advierte que el AIFA no consideró los perfiles que en su caso pudieran presentarse respecto de los titulares de datos personales que puedan, en su caso, ser enrolados en el Sistema de Procesamiento, esto considerando que el perfil elegido para utilizar dicho sistema puede incluir a personas con diferentes grados de instrucción o de salud; ya que respecto al punto en estudio, sin que se logre verificar con precisión las consideraciones en torno al tipo de usuarios y el impacto que tiene el sistema en estudio.

Cuando se solicitó al AIFA justificar la aplicación del principio en estudio, se limitó a referir el proceso en virtud del cual se realiza el tratamiento, así como los datos personales a tratar, es importante precisar que el responsable tenía que identificar la forma como el tratamiento propuesto no actualizaba alguno de los tres supuestos:

- Que el tratamiento se efectuara por medios engañosos o fraudulentos: aquéllos que el responsable utilice para tratar los datos personales con dolo, mala fe o negligencia,
- Que el responsable omitiera privilegiar los intereses del titular, esto es, cuando existan indicios de que el tratamiento de datos personales que efectúa diera lugar a una discriminación o trato injusto o arbitrario contra éste y no haga o efectúe acciones para contrarrestarlo, y
- Que el tratamiento no sentara las bases para crear en el titular una expectativa razonable de privacidad.

Aunado a lo anterior, no debe perderse de vista que, debido a las características de los datos biométricos, que consiste en el reconocimiento facial en el caso que nos ocupa, dentro de las cuales se encuentra que estos son únicos, ya que no existen dos biométricos con las mismas características, distinguiéndonos así de otras personas, estos sólo pueden recopilados a través de su titular. En ese sentido, se presumiría que los medios de obtención de éstos no serían por medios engañosos o fraudulentos al ser proporcionados por el propio titular, siempre y cuando, se obtengan conforme al fin para los cuales están siendo recabados y se le haga saber al titular a través del aviso de privacidad correspondiente. Últimas circunstancias que este Instituto no advierte que se encuentren claramente establecidas en los avisos de privacidad remitidos.

En virtud de lo anterior, se realizan las recomendaciones siguientes:

Recomendaciones en torno al principio de lealtad

Clave	Recomendaciones
AIFA_LE_001	En atención a la expectativa razonable de privacidad referente a la confianza que el titular ha depositado en el responsable respecto a que sus datos personales sean tratados conforme a lo señalado en el aviso de privacidad, se recomienda que, a través de éste, se precise en cada caso, cuáles son los medios de obtención de los datos personales, atendiendo las recomendaciones efectuadas en torno a ese principio.
AIFA_LE_002	Se sugiere que, en caso de que se considere mantener diversos avisos de privacidad respecto al Sistema de Procesamiento, se recomienda hacer homologar que se trata del mismo tratamiento de datos personales y las mismas finalidades de tratamiento.

AIFA_LE_003	Se sugiere, cumplir con las recomendaciones emitidas en el apartado de derechos ARCO con el objetivo de generar una expectativa razonable de privacidad en los titulares.
AIFA_LE_004	Se sugiere que, además de las recomendaciones efectuadas en el principio de información y en el apartado de derechos ARCO, que se privilegie que los particulares tengan certeza de los elementos suficientes para conocer los datos que serán objeto de tratamiento de datos personales, los periodos de conservación y la destrucción después de que culminen los periodos de conservación respectivos.
AIFA_LE_005	Se sugiere considerar que, la posibilidad de que, de acuerdo a los diferentes perfiles de los titulares de datos personales, se considere que podrían requerir el acceso al PDE de forma posterior a las 24 horas siguientes a la salida del vuelo respectivo.
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]

1.4. Principio de consentimiento

Los artículos 20, 21 y 22 de la Ley General, 12, 13, 14, 15, 16, 17, 18, 19 y 20 de los Lineamientos generales de los cuales se desprende que el responsable está obligado a obtener el consentimiento del titular, ya sea en su modalidad expresa o tácita, de manera previa al tratamiento de sus datos personales, salvo que se actualice alguna de las causales de excepción previstas en el artículo 22 de la Ley General:

Se eliminan 16 lineas, con fundamento en el artículo 110, fracción I de la LFTAIP; Décimo séptimo de los lineamientos Generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas, en relación con el artículo 5, fracción VI de la Ley de Seguridad Nacional; 47, Bis 4 de la Ley de Aviación Civil, 46 y 47 de la Ley de Aeropuertos y 152 del Reglamento de Aeropuertos.

I. Cuando una ley así lo disponga debiendo dichos supuestos ser acordes con las bases, principios y disposiciones establecidos en la Ley General, en ningún caso podrán contravenirla.
II. Cuando se realicen transferencias de datos personales entre responsables para el ejercicio de facultades propias, compatibles o análogas con la finalidad que motivó el tratamiento de los datos personales.
III. Cuando exista una orden judicial, resolución o mandato fundado y motivado de autoridad competente.
IV. Para el reconocimiento o defensa de derechos del titular ante autoridad competente.
V. Cuando los datos personales se requieran para ejercer un derecho o cumplir obligaciones derivadas de una relación jurídica entre el titular y el responsable.
VI. Cuando exista una situación de emergencia que potencialmente pueda dañar a un individuo en su persona o bienes.
VII. Cuando los datos personales sean necesarios para la prevención, diagnóstico, o la prestación de asistencia sanitaria.
VIII. Cuando los datos personales figuren en fuentes de acceso público.
IX. Cuando los datos personales se sometan a un procedimiento previo de disociación.
X. Cuando el titular sea una persona reportada como desaparecida en los términos de la ley en la materia.

Para tal efecto, el consentimiento del titular debe caracterizarse por ser:

- **Libre:** sin que medie error, mala fe, violencia o dolo que puedan afectar la manifestación de voluntad del titular.
- **Específico:** referido a finalidades concretas, lícitas, explícitas y legítimas que justifiquen el tratamiento de los datos personales.
- **Informado:** que el titular tenga conocimiento del aviso de privacidad previo al tratamiento de sus datos personales.

Por regla general, será válido el consentimiento tácito del titular para cualquier tratamiento de datos personales, salvo que una ley exija que la voluntad del titular se manifieste expresamente.

La solicitud del consentimiento debe ser concisa e inteligible, estar redactada en un lenguaje claro y sencillo acorde con el perfil del titular y, cuando se refiera a diversos asuntos ajenos a la protección de datos personales, presentarse de tal forma que se distinga claramente de dichos asuntos. Lo anterior, en caso de que se requiera el consentimiento del titular para el tratamiento de sus datos personales.

Asimismo, el responsable está obligado a obtener el consentimiento del titular, de manera previa, cuando se recaben los datos personales directamente del titular y se requiera su consentimiento.

Cuando se recaben los datos personales indirectamente del titular y se requiera su consentimiento, el responsable tiene prohibido tratar los datos personales hasta que cuente con el consentimiento del titular.

Sobre el particular, el AIFA en la Evaluación de impacto, refirió lo siguiente con relación a dicho principio:

> ***"...Descripción de sistemas y plataformas que componen el sistema de procesamiento de pasajeros:***
> *[...]*
> *Existen ciertos requisitos para proceder a realizar un enrolamiento biométrico:*
> ***1. Consentimiento de uso de datos personales (a través de los avisos de privacidad)***
> *[...]*
> ***d. Aplicación Móvil y SDK, vb MobileID™ de Vision-Box.***
> *[...]*
> *Para realizar el registro o enrolamiento en la aplicación móvil, el pasajero deberá proporcionar la siguiente información:*
> • ***Consentimiento de uso de datos personales.***
> • *Documento de viaje: pasaporte electrónico.*
> • *Pase de Abordar.*
> • *Captura de imagen del rostro ("Selfie").*
> *[...]*
> ***V. Categorías de los titulares.***
> *El sistema se definió y quedó configurado para no procesar biométricamente a pasajeros menores de edad. Para menores de edad se realizará el procedimiento tradicional (proceso no biométrico).*
> *Para el ingreso al área estéril, un agente de seguridad del AIFA realizará la verificación de su identidad. Para el proceso de abordaje, un agente de la aerolínea realizará la validación.*
> ***Todos los pasajeros mayores de edad que cuenten con su pase de abordar y documento de identificación oficial podrían realizar el registro biométrico, si se cuenta con su consentimiento.***
> *El sistema no discrimina, porque no está configurado para clasificar o identificar a un pasajero ya sea por origen étnico o racial; género; estado de salud; preferencia sexual; nivel de instrucción; condición socioeconómica; ni limitaciones físicas.*
> *Las personas elegibles son aquellas personas que pueden realizar un registro biométrico dentro de la solución de procesamiento biométricos de pasajeros.*
> *Existen algunos requisitos para que un pasajero pueda registrarse biométricamente:*
> • ***El pasajero debe proveer su consentimiento para el uso de sus datos personales a través de los avisos de privacidad.***

• El pasajero deberá proveer su documento de identidad (Pasaporte electrónico, pasaporte no electrónico o INE, según la fuente de registro biométrico).
• El pasajero deberá estar documentado en un vuelo. Deberá poseer un Pase de Abordar válido.
• Se deberá poder capturar una imagen del rostro (fotografía).
• El pasajero deberá ser mayor de edad (configuración actual de la plataforma vb orchestraTM).
[...]
b) Proceso de registro en el quiosco de autoservicio (CUSS) del AIFA.
1. El pasajero realiza una reservación con la aerolínea.
2. El pasajero ingresa a la aplicación de la aerolínea (DCS) en el quiosco de autoservicio.
3. La aerolínea genera el pase de abordar.
4. El pasajero imprime el pase de abordar en el Quiosco de autoservicio del AIFA.
5. En pantalla se muestra la solicitud de consentimiento de enrolamiento biométrico.
6. El usuario acepta los términos del aviso de privacidad.
[...]
c) Proceso de registro en el mostrador de documentación (CUPPS) y luego realiza registro biometrico en el vDesk del AIFA.
1. El pasajero reserva un vuelo con la aerolínea.
2. El usuario se presenta en el mostrador con una identificación oficial.
3. El agente de la aerolínea valida la coincidencia de la foto en el documento de identificación con el pasajero, de manera visual.
4. La aerolínea registra al pasajero e imprime el pase de abordar.
5. El personal de la aerolínea invita al pasajero a enrolarse en el sistema de procesamiento biométrico.
6. El pasajero acepta participar en el enrolamiento facial.
7. El agente de la aerolínea inicia proceso.
8. El pasajero deberá escoger el idioma de su preferencia (inglés o español).
9. Se muestra en pantalla el aviso de privacidad relativo al procesamiento de datos.
10. El pasajero otorga su consentimiento para el procesamiento de sus datos.
11. El agente de la aerolínea escanea el pase de abordar.
12. Se envían los datos por protocolo AIDX a través de la red local del AIFA.
13. Se almacena los datos en el Data Center del AIFA.
14. Se envía un mensaje de solicitud de escaneo de documento.
[...]
Nota: En caso de que el pasajero no de su consentimiento para realizar el enrolamiento biométrico podrá realizar su procesamiento e identificación (en el área de pre-seguridad y abordaje) de la forma tradicional, presentando su pase de abordar [...]"

Por su parte, en la respuesta de requerimiento de información adicional, se señaló lo siguiente:

[“…]e. Aplicación móvil, que integra el SDK, vb MobileID™ de Vision-Box.
[…]
Para realizar el registro o enrolamiento en la aplicación móvil, el pasajero deberá proporcionar la siguiente información:
- ***Consentimiento de uso de datos personales.***
- *Documento de viaje: pasaporte electrónico.*
- *Pase de Abordar.*
- *Captura de imagen del rostro (“Selfie”).*

[…]
Con fundamento en el Art. 65 se obtendrá el consentimiento expreso del titular a través de los avisos de privacidad que se darán a conocer por medio de los 3 puntos de enrolamiento del sistema.
[…]
Además de lo ya mencionado, en los avisos de privacidad (simple e integral) se ve reflejada la obtención del consentimiento expreso del particular, así como las finalidades por las cuales se recaban los datos, así como las transferencias que para el procesamiento de pasajeros se requieran, lo anterior en cumplimiento a lo que dispone el último párrafo del artículo 21 de la LGTAIP, que expresa que tratándose de datos personales sensibles el responsable deberá obtener el consentimiento expreso y por escrito del titular para su tratamiento, a través de mecanismos como el de autenticación que se establezca.
[…]
De conformidad con los artículos 26, 27 y 28 de la ley general de datos, referente al principio de información, si bien, se remiten los avisos de privacidad en sus diversas modalidades (integral y simplificado) ***y se indica que estos se pondrán en disposición a través de la pantalla, no se indica el tipo de consentimiento requerido en función de los datos personales a tratar ni forma de obtención, por lo que, se solicita indicar con exactitud lo mencionado, además de precisar si existieran medios adicionales al electrónico, como son formatos físicos, ópticos, sonoros, visuales o a través de cualquier otra tecnología que permita su eficaz comunicación; Así como si aparecen en el “sistema de procesamiento de pasajeros”.***

“En la página web será publicado el procedimiento de enrolamiento para conocimiento de los particulares, como un ejercicio del principio de información.
El tipo de consentimiento es expreso y es recabado directamente del titular a través de medios electrónicos de manera digital al llevar a cabo el proceso de registro biométrico; ya que, para poder realizar el enrolamiento, es requisito

aceptar el aviso de privacidad en cualquiera de las tres modalidades de registro (App, Quiosco de Autoservicio y Vdesk) a través de una pantalla táctil. En caso de no ser aceptado, se dará por finalizado el proceso de registro y realizara el abordaje de manera tradicional [...]"

En este sentido a continuación se emitirán algunos hallazgos y consideraciones advertidas de manera particular conforme a la información proporcionada por parte del AIFA, para lo cual resulta pertinente señalar que con relación al tipo de datos que se pretende recabar, tal y como ha quedado precisado con anterioridad principalmente se destacan los datos biométricos, el género y la nacionalidad, los cuales, de acuerdo a su contexto, pudieran ser considerados datos sensibles.

Bajo este supuesto, es importante reiterar que en términos del artículo 7 de la Ley General, por regla general no podrán tratarse datos personales sensibles, salvo que se cuente con el consentimiento expreso de su titular o en su defecto, se trate de los casos establecidos en el artículo 22 de dicha Ley.

Asimismo, de igual forma el último párrafo de la Ley General, refiere que tratándose de datos personales sensibles el responsable deberá obtener el consentimiento expreso y por escrito del titular para su tratamiento, a través de su firma autógrafa, firma electrónica o cualquier mecanismo de autenticación que al efecto se establezca, salvo en los casos previstos en el artículo 22 de la Ley, mismo que ya fue referenciado en líneas precedentes, no advirtiéndose con base en la información proporcionada por el AIFA, se pudiera acreditar algunas de las causales de excepción al consentimiento.

De igual manera con relación al tratamiento de datos personales sensibles, el artículo 53 de los Lineamientos Generales, se señala que el responsable no podrá llevar a cabo tratamientos de datos personales que tengan como efecto la discriminación de los titulares por su origen étnico o racial, su estado de salud presente, pasado o futuro, su información genética, sus opiniones políticas, su religión o creencias filosóficas o morales y su preferencia sexual, con especial énfasis en aquéllos automatizados.

Es por ello que, en atención a lo antes referido en términos de ley y al tipo de datos, el consentimiento deberá de ser expreso y por escrito por parte de las y los titulares.

No obstante, lo anterior, deberá de considerar que pueden existir finalidades específicas para las que no es necesario recabar el consentimiento del titular como puede ser aquella que se den derivado de la existencia de una orden judicial, resolución o mandato fundado y motivado de autoridad competente.

Por lo que, a continuación, se harán las precisiones en torno a las tres modalidades mediante las cuales se pretende efectuar el registro del enrolamiento y el principio de consentimiento, conforme a lo siguiente:

Es importante señalar que en la evaluación que nos ocupa, se señala que **el pasajero debe proveer su consentimiento para el uso de sus datos personales a través de los avisos de privacidad.**

Mostrador convencional CUPPS-VDesk
Conforme a lo antes señalado en cuanto a esta modalidad conforme al proceso citado se muestra en pantalla el aviso de privacidad relativo al procesamiento de datos y el pasajero otorga su consentimiento para el procesamiento de sus datos, con lo cual si bien es cierto se entendería se está obteniendo el consentimiento expreso por parte de las y titulares, de acuerdo al contexto de los datos personales a tratar no se advierte se obtenga el consentimiento por escrito.

Aplicación móvil
De igual manera que en mostrador, se advierte que se pretende recabar el consentimiento a través del aviso de privacidad respectivo, a través del aplicativo móvil, en donde el pasajero deberá proporcionar el Consentimiento de uso de datos personales, con lo cual si bien es cierto se entendería se está obteniendo el consentimiento expreso por parte de las y titulares, de acuerdo al contexto de los datos personales a tratar no se advierte se obtenga el consentimiento por escrito.

Quiosco de autoservicio - CUSS.
Asimismo, con relación a la presente modalidad, se señala que en pantalla se muestra la solicitud de consentimiento de enrolamiento biométrico y el usuario acepta los términos del aviso de privacidad, con lo cual si bien es cierto se entendería se está obteniendo el consentimiento expreso por parte de las y titulares, de acuerdo al contexto de los datos personales a tratar no se advierte se obtenga el consentimiento por escrito.

Es importante destacar, que se advierte de igual manera se pretende conforme al inventario de datos personales, el tratamiento del nombre del vendedor, por lo que en este supuesto de igual manera se tendría que garantizar se obtenga el consentimiento de dicho titular.

Debido a lo anterior, se realizan las recomendaciones siguientes:

Recomendaciones en torno al principio de consentimiento

Clave	Recomendación

AIFA_Co_001	Se recomienda verificar y definir el tipo de consentimiento que se requiere, según las categorías de datos personales que se vayan a tratar o las disposiciones normativas que regulen el tratamiento.
AIFA_Co_002	Se recomienda habilitar los mecanismos necesarios para solicitar el consentimiento expreso y por escrito por parte de las y los titulares de los datos personales en términos de la normatividad aplicable, así como documentar su obtención, tomando en consideración los medios digitales que se emplean en el caso de la app y el quiosco. Lo anterior, tomando como referencia las diferentes modalidades con relación al tratamiento de datos personales entre los cuales se encuentran datos biométricos en su carácter de datos personales sensibles.

1.5. Principio de calidad

Los artículos 23 y 24 de la Ley General establecen lo siguiente:

*"**Artículo 23**. El responsable 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.*

Se presume que se cumple con la calidad en los datos personales cuando éstos son proporcionados directamente por el titular y hasta que éste no manifieste y acredite lo contrario.

Cuando los datos personales hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas en el aviso de privacidad y que motivaron su tratamiento conforme a las disposiciones que resulten aplicables, deberán ser suprimidos, previo bloqueo en su caso, y una vez que concluya el plazo de conservación de los mismos.

Los plazos de conservación de los datos personales no deberán exceder aquéllos que sean necesarios para el cumplimiento de las finalidades que justificaron su tratamiento, y deberán atender a las disposiciones aplicables en la materia de que se trate y considerar los aspectos administrativos, contables, fiscales, jurídicos e históricos de los datos personales.

***Artículo 24.** El responsable deberá establecer y documentar los procedimientos para la conservación y, en su caso, bloqueo y supresión de los datos personales que lleve a cabo, en los cuales se incluyan los periodos de conservación de los mismos, de conformidad con lo dispuesto en el artículo anterior de la presente Ley.*

En los procedimientos a que se refiere el párrafo anterior, el responsable deberá incluir mecanismos que le permitan cumplir con los plazos fijados para la supresión de los datos personales, así como para realizar una revisión periódica sobre la necesidad de conservar los datos personales."

Los artículos 23 y 24 de la Ley General, 21 y 23 de los Lineamientos generales, de los cuales se desprende que el responsable tiene la obligación de adoptar las medidas necesarias para mantener exactos, completos, correctos y actualizados los datos personales que serán

tratados, de tal manera que no se altere la veracidad de éstos y que correspondan con la realidad del titular."

Asimismo, los artículos 21, 22 y 23 de los Lineamientos generales prevén lo siguiente:

*"**Principio de Calidad***

***Artículo 21.** Para efectos del artículo 23 de la Ley General y los presentes Lineamientos generales, se entenderá que los datos personales son:*

***I.** Exactos y correctos: cuando los datos personales en posesión del responsable no presentan errores que pudieran afectar su veracidad;*

***II.** Completos: cuando su integridad permite el cumplimiento de las finalidades que motivaron su tratamiento y de las atribuciones del responsable, y*

***III.** Actualizados: cuando los datos personales responden fielmente a la situación actual del titular.*

Presunción de calidad de los datos personales cuando se obtienen indirectamente del titular

***Artículo 22.** Cuando los datos personales fueron obtenidos indirectamente del titular, el responsable deberá adoptar medidas de cualquier naturaleza dirigidas a garantizar que éstos responden al principio de calidad, de acuerdo con la categoría de datos personales y las condiciones y medios del tratamiento.*

Supresión de los datos personales

***Artículo 23.** En la supresión de los datos personales a que se refiere el artículo 23, párrafo tercero de la Ley General, el responsable deberá establecer políticas, métodos y técnicas orientadas a la supresión definitiva de éstos, de tal manera que la probabilidad de recuperarlos o reutilizarlos sea mínima.*

En el establecimiento de las políticas, métodos y técnicas a que se refiere el párrafo anterior, el responsable deberá considerar, al menos, los siguientes atributos y el o los medios de almacenamiento, físicos y/o electrónicos en los que se encuentren los datos personales:

***I. Irreversibilidad:** que el proceso utilizado no permita recuperar los datos personales;*

***II. Seguridad y confidencialidad:** que en la eliminación definitiva de los datos personales se consideren los deberes de confidencialidad y seguridad a que se refieren la Ley General y los presentes Lineamientos generales, y*

***III. Favorable al medio ambiente:** que el método utilizado produzca el mínimo de emisiones y desperdicios que afecten el medio ambiente."*

De lo anterior se desprende que el responsable tiene la obligación de adoptar las medidas necesarias para mantener exactos, completos, correctos y actualizados los datos personales que serán tratados, de tal manera que no se altere la veracidad de éstos y que correspondan con la realidad del titular.

Se entiende que los datos personales son:

- Exactos y correctos: cuando los datos personales en posesión del responsable no presentan errores que pudieran afectar su veracidad.
- Completos: cuando su integridad permite el cumplimiento de las finalidades que motivaron su tratamiento y de las atribuciones del responsable.
- Actualizados: cuando los datos personales responden fielmente a la situación actual del titular.

Se presume el cumplimento del principio de calidad cuando los datos personales sean obtenidos de manera directa del titular. De lo contrario, si los datos personales son obtenidos de manera indirecta, el responsable está obligado a adoptar medidas de cualquier naturaleza dirigidas a garantizar que éstos responden al principio de calidad, de acuerdo con la categoría de datos personales y las condiciones y medios del tratamiento.

Asimismo, el responsable tiene la obligación de:

- Suprimir los datos personales tratados una vez que dejen de ser necesarios para el cumplimiento de las finalidades que motivaron su utilización.
- Establecer y documentar los procedimientos para la conservación y, en su caso, bloqueo y supresión de los datos personales que serán utilizados. En la definición de los plazos de conservación de los datos personales se deberán considerar los valores administrativos, contables, fiscales, jurídicos e históricos que pudieran llegar a tener éstos.
- Establecer políticas, métodos y técnicas orientadas a la supresión definitiva de los datos personales, de tal manera que la probabilidad de recuperarlos o reutilizarlos sea mínima. Para ello deberá considerar los siguientes factores:
  - Irreversibilidad: que el proceso utilizando no permita recuperar los datos personales;
  - Seguridad y confidencialidad: que en la eliminación definitiva de los datos personales se consideren los deberes de confidencialidad y seguridad.
  - Favorable al medio ambiente; que el método utilizado produzca el mínimo de emisiones y desperdiciados que afecten el medio ambiente.

Al respecto, el AIFA manifestó en la evaluación de impacto, lo siguiente:

> *"El sistema cuenta con los mecanismos para mantener los datos personales exactos, completos, correctos y actualizados a través de procesos de validación, los mismos que constan en el documento Experiencia sin contacto con tecnología biométrica, Gestión de Datos Personales, Solución Biométrica, 2.2 Puntos de Validación o Verificación de Identidad Biométrica.*
>
> ...
>
> ***III. Los plazos de conservación o almacenamiento de los datos personales.***
> *Descritos en los numerales V Bloqueo y VI Cancelación o supresión de datos personales, del Ciclo de Vida dentro de este documento.*

V. Bloqueo de datos personales (Desactivación).

- Plataforma de gestión biométrica Vision Box vb orchestra™:

Los datos almacenados se usan dentro de la plataforma orchestra únicamente para:

o Identificar al pasajero dentro de la plataforma orchestra.

o Intercambiar los datos para validar la elegibilidad del pasajero en puertas de pre-seguridad y abordaje.

Después de 24 horas posteriores a la fecha de la salida del vuelo, se ejecuta una acción de borrado, de manera automática, de todos los PDE almacenados en las Galerías de la solución biométrica. Esto se realiza con el objetivo de asegurar el borrado de los datos de los pasajeros.

El tiempo de permanencia de la información en el Data Center en referencia es configurable.

- Aplicación móvil del AIFA

No se almacenan datos.

- Quioscos de Autoservicio (CUSS)

No se almacenan datos.

- Mostradores de documentación (Enrolamiento asistido) CUPPS y Vdesk

No se almacenan datos.

- E-Gate Pre-seguridad

No se almacenan datos.

- E-Gate Abordaje

No se almacenan datos.

- Sistema de Validación de Pasajeros de Amadeus (APV)

No se almacenan datos.

- Sistema Aeroportuario de Uso Común (ACUS)

No se almacenan datos.

VI. Cancelación o supresión de datos personales.

Si un pasajero ha realizado su registro biométrico, una vez que pase por las E-Gate de Pre-Seguridad, sus datos se suprimirán de la Galería de Pre Seguridad. De igual manera, una vez que el pasajero pasa por las E-Gate de Abordaje, sus datos se suprimirán de la Galería de Abordaje y de la base de datos.

Después de 24 horas posteriores a la fecha de la salida del vuelo, se ejecuta una acción de borrado, de manera automática, de todos los PDE almacenados en las Galerías de la solución biométrica. Esto se realiza con el objetivo de asegurar el borrado de los datos de los pasajeros, debido a que podrían presentarse los siguientes casos:

o Que el pasajero no ingrese al área estéril del aeropuerto o no realice el abordaje.

o Que el pasajero use el procedimiento de pre-seguridad de manera tradicional, con la asistencia de un agente, presentando el pase de abordar de forma física.

o Que el pasajero use el procedimiento de abordaje tradicional, presentando el pase de abordar de forma física.

o Que el vuelo sea suspendido.

o Que exista requerimiento de las autoridades (transporte de drogas ilegales, casos de ebriedad o bajo el influjo de estupefacientes, psicotrópicos o enervantes, otros).

De acuerdo con el Artículo 23 de la LGPDPPSO cuando los datos personales hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas en los avisos de privacidad y que motivaron su tratamiento conforme a las disposiciones que resulten aplicables, deberán ser suprimidos, previo bloqueo en su caso, y una vez que concluya el plazo de conservación de los mismos.

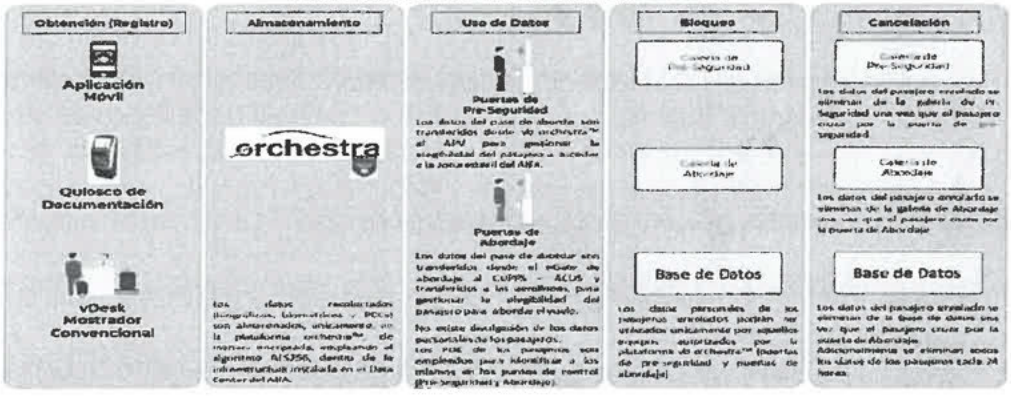
Por lo que en la operación inicial del Sistema de Procesamiento de Pasajeros del AIFA el plazo señalado de 24 horas máximo para el borrado de los datos personales cumple con las finalidades que justificaron su tratamiento.

Como medidas adicionales de seguridad y confidencialidad y según lo establece el Artículo 55 de la mencionada Ley, en este caso el ejercicio de los derechos ARCO no sería procedente porque los datos personales no se encontrarán en posesión del responsable.

El borrado en el plazo mencionado de 24 horas, garantizará la correcta funcionalidad del sistema durante los procesos internos de consulta, ya que una cantidad alta de registros pudiera resultar en afectaciones al flujo de los datos y a la integridad del sistema, aunado a un costo desproporcionado por almacenamiento de datos no inherentes a la finalidad de cada PDE. La certeza en cuanto al punto anterior la tendrá el operador del sistema en cuanto inicie su operación con tráfico real de pasajeros, independientemente de las figuras teóricas que describe la literatura, fichas técnicas y manuales de funcionamiento.

Una vez que se tengan figuras reales sobre los flujos de datos, el comportamiento del sistema, y para garantizar los derechos ARCO de los titulares se podría analizar, validar y ampliar el período de ciclo de vida del tratamiento de los datos personales en el Sistema de Procesamiento de Pasajeros del AIFA.

Ciclo de Vida de los Datos Personales



Resumen del Ciclo de Vida de los Datos Personales

Para el proceso **no biométrico** no se almacena información en la Base de Datos del AIFA.

[…]"

Por otro lado, en la respuesta al requerimiento de información adicional, se indicó lo siguiente:

> *"Sobre las pruebas de calidad, vulnerabilidad y estrés, se detalla lo siguiente: A. Pruebas de calidad, se llevaron a cabo durante el mes de Julio 2022, donde se validó cada una de las funcionalidades de los diferentes equipos y sistemas, siendo completadas de manera satisfactoria. El detalle se incluye en el Anexo 13."*

Por su parte, en el Anexo 2 "Experiencia sin contacto" se indica lo siguiente:

> *"1.7.1 Calidad de los datos Los datos utilizados en vb orchestra™ se extraen de los documentos de viaje, del pase de abordar y del pasajero, y el PDE se extrae de los sistemas y bases de datos existentes dentro de la plataforma vb orchestra™, y con esto se salvaguarda la calidad de los datos."*

Una vez expuesto lo anterior, se advierte que la obtención de los datos personales se lleva a cabo a través de:

- Quioscos de autoservicio – CUSS.
- Mostradores de documentación CUPPS-Vdesk.
- Aplicación móvil AIFA.

En este sentido, de acuerdo con el artículo 23 de la Ley General se presume que se atiende la calidad en los datos personales cuando éstos son proporcionados directamente por el titular y hasta que éste no manifieste y acredite lo contrario, por lo cual, se advierte que la obtención de los datos personales será directamente de los titulares a través de medios electrónicos como son los quioscos de autoservicio – CUSS y la app.

Por lo cual, se presume que el tratamiento de datos personales que será llevado a cabo con motivo de la implementación del Sistema de Procesamiento a través de los quioscos de autoservicio – CUSS y la app, contiene características bajo las cuales se puede determinar que los datos personales serán tratados bajo el principio de calidad, al ser estos proporcionados de manera directa por los titulares y el medio establecido para tal fin.

No obstante, se indica en la evaluación de impacto, por lo que hace al medio de obtención de los mostradores de documentación CUPPS-Vdesk serán en los mostradores de las diferentes aerolíneas en las cuales los titulares podrán realizar el enrolamiento biométrico con asistencia de personal de la aerolínea.

Por lo anterior y en el entendido de que las aerolíneas pudieran constituirse como terceros responsables, se pudiera estar ante un medio de obtención de los datos personales de manera indirecta ya que se realiza a partir del personal de las aerolíneas y no así del personal del AIFA, no

obstante, en la misma evaluación se indica que es el AIFA es quien implementa y proporciona la tecnología Vdesk para que los mostradores convencionales puedan realizar el registro biométrico, así como la plataforma ACUS, vía el APV, como el componente tecnológico de la solución de Procesamiento de Pasajeros que permite la integración entre CUSS; CUPPS de documentación y abordaje; E-gates y los sistemas de las aerolíneas.

De esta manera, se advierte que, para el cumplimiento de las finalidades que persigue el Sistema de procesamiento, el AIFA es quien lo implementa y proporciona a las aerolíneas la tecnología necesaria para permitir el flujo ininterrumpido para el acceso de los pasajeros para pasar a los filtros de pre-seguridad y realizar el embarque a la aeronave de manera rápida y segura por lo cual, es quien decide los medios mediante el cual se llevará a cabo el tratamiento o tratamientos de datos personales para tal fin.

En este sentido, se advierte que si bien, la aerolínea es quien recaba los datos personales de los titulares a través de la tecnología Vdesk, el AIFA es el responsable de esta tecnología, su operación y funcionamiento, por lo que pudiera estarse ante un supuesto en el que la aerolínea funge como encargado del AIFA, en términos de lo establecido en el artículo 3, fracción XV de la Ley General puesto que el registro biométrico es realizado a cargo del AIFA toda vez que se trata de una medida implementada por el aeropuerto.

Por lo cual, en tal supuesto se estaría ante una obtención de datos personales de manera personal y directa en virtud de que el titular proporciona los datos personales al responsable o a la persona física designada por el responsable, con la presencia física de ambos y directa al ser proporcionada a través del medio electrónico Vdesk y por lo tanto determinar que los datos personales serán tratados bajo el principio de calidad.

Ahora bien, por lo que hace a las condiciones para constituir las características de los datos como exactos, correctos, completos y actualizados se advierte lo siguiente:

Respecto a la característica de ser exactos y correctos, establecido artículo 21, fracción I de los Lineamientos generales, al ser datos personales proporcionados directamente por los usuarios del Sistema de procesamiento, los mismos no pudieran presentar errores que pudieran afectar su veracidad puesto que sus titulares son los que capturan la información.

Sin embargo, es preciso indicar que, si bien se indicó que se preserva la calidad de los datos personales en el Sistema de Procesamiento, de acuerdo con lo establecido en el Anexo 2, antes referido, puesto que se extraen de los documentos de viaje, del pase de abordar y del pasajero, es importante señalar que en la evaluación de impacto en el procesamiento de la obtención de los

datos a través de los mostradores de documentación CUPPS-Vdesk se indica que "*El agente valida visualmente que la identificación proporcionada corresponda al pasajero y procede con el escaneo del documento*" y posteriormente se envían los datos correspondientes tomados del pase de abordar y de la identificación del pasajero a la plataforma de vb orchestra.

Por lo cual, se observa que el AIFA señala la preservación de la calidad de los datos personales por la extracción de los documentos presentados, sin embargo, es importante verificar que en dicha parte del procedimiento se esté reflejando la realidad de la situación de su titular, es decir, que sean verdaderos o fieles a efecto de que sean exactos y que sean pertinentes, es decir, que correspondan efectivamente al titular.

Asimismo, es importante traer a colación una de las consideraciones establecidas en el análisis de las obligaciones para la atención de solicitudes de derechos ARCO, respecto de que no se podrá ejercer ninguno de los derechos ARCO debido al plazo para su eliminación y la encriptación de los datos. Al respecto, en el caso particular del derecho de rectificación, es importante señalar que tal situación puede impactar en las características de los datos personales sobre su exactitud, pertinencia y actualización, toda vez que ante un posible supuesto en el que los datos personales de los titulares sean incorrectos, no se tiene un mecanismo o solución mediante el cual el titular puede rectificarlos y con ello garantizar que son fieles a su situación, que corresponden al titular y que están actualizados al día.

Por lo que hace a la obligación de los responsables de establecer plazos de conservación de los datos personales, los cuales no deberán exceder aquéllos que sean necesarios para el cumplimiento de las finalidades que justificaron su tratamiento, asimismo deberán atender las disposiciones aplicables en la materia de que se trate y considerar los aspectos administrativos, contables, fiscales, jurídicos e históricos de los datos personales, de conformidad a lo dispuesto en el artículo 23 de la Ley General, es preciso traer a colación que el AIFA, en su evaluación de impacto señaló que los datos que serán almacenado en la plataforma vb orchestra serán borrados de manera automática después de 24 horas posteriores a la fecha de la salida del vuelo.

Si bien se indica el momento en el cual se eliminarán los datos personales almacenados en el Sistema de Procesamiento, lo cierto es que no se establece un plazo de conservación exacto, puesto que no se brinda información sobre si existe una limitante de tiempo para que los titulares pueden enrolarse biométricamente a través de la app como el quiosco, es decir, si se cuenta con alguna configuración específica que impida a los titulares enrolarse tiempo antes de su día de vuelo y en caso de que no, establecer el tiempo previo en el que pueden realizar este registro biométrico, lo anterior, a efecto de establecer el tiempo posible de almacenamiento y los plazos de conservación de los datos personales.

De igual forma, es importante señalar que los plazos de conservación no deben exceder el tiempo estrictamente necesario para llevar a cabo las finalidades que justificaron el tratamiento, ni aquél que se requiera para cumplir con:

- Las disposiciones legales establecidas en la Ley General de Archivos.
- Las disposiciones aplicables en la materia de que se trate.
- Los aspectos administrativos, contables, fiscales, jurídicos e históricos de la información.
- El periodo de bloqueo.

En cuanto a la obligación del responsable de suprimir, previo bloqueo en su caso, los datos personales cuando dejen de ser necesarios para su finalidad, es importante señalar que el Anexo 2 "Experiencia sin contacto" se indicó lo siguiente:

> *"Sobre la plataforma vb orchestra™ es posible activar configuraciones personalizadas, que corresponden al tratamiento de los datos personales que por instrucción del Controlador de Datos son configuradas en la plataforma para el procesamiento de los datos*

De lo anterior es importantes señalar que tanto en la evaluación como en el documento antes referido se advierte la posibilidad de que extender el plazo de 24 horas que se señala para el borrado de la información, puesto que se advierte que el sistema de vb orchestra tiene una configuración para personalizar el borrado, por lo cual se advierte no sólo una inconsistencia del plazo que define el AIFA, sino también una situación que pudiera ser desleal para los titulares toda vez que está abierta a discreción de quien tenga el acceso a esta configuración, de que sus datos sean almacenados más tiempo del establecido en los plazos de conservación.

Adicionalmente, el AIFA señala que habrá un borrado de los datos contenidos en la plataforma vb orchestra sin embargo no se manifiesta sobre el borrado en el resto de los elementos que conforman el Sistema de Procesamiento, particularmente en la tecnología de Amadeus.

Si bien, el AIFA explica en su evaluación de impacto que los datos personales sólo se almacenarán en la plataforma vb orchestra, lo cierto es que en el Anexo denominado ITP-043-02 Apollo Anexo A pag. 31-74 se advirtió como una de las características mínimas del quiosco de autoservicio CUSS:

> *"**11. Lector Biométrico***
> *Debe permitir el enrolamiento del pasajero permitiendo agilizar los procesos desde el check-in hasta el abordaje, almacenando la información en la AODB."*

Por su parte, el Anexo Apollo anexo A des. tec. pag. 1-30 se establece lo siguiente sobre el AODB:

> *"3.1 Base de datos de operaciones aeroportuarias (AODB)*
> ...

A. Base de datos.
La base de datos de operación Amadeus AODB está diseñada para administrar los datos de losmovimientos de los vuelos, desde la fase de planificación hasta la operación diaria, así como el archivo de todas las transacciones de datos. Para ofrecer una solución independiente del hardware, todo el software está basado en Java.
Luego de completarse un día de vuelos, los datos se almacenarán en un archivo de datos independiente. Este archivo de datos se llama Amadeus DAR. Los datos archivados se encuentran disponibles para el procesamiento comercial de datos y la posterior evaluación de estos."

Por lo anterior, es posible observar que Amadeus y Apollo tiene implementada una base de datos de operación aeroportuaria por sus siglas AODB, en la cual se almacenarán, entre otros, la información del enrolamiento biométrico de los pasajeros para, posteriormente, almacenarse en otra base de datos denominada Amadeus DAR.

De esta manera, el borrado que alude el AIFA en su evaluación de impacto no considera los datos personales que pudieran ser recolectados y almacenados en bases de datos de Amadeus y Apollo a través del resto de los elementos que conforman el Sistema de Procesamiento, sin incluir la plataforma vb orchestra, es decir, sólo se informa sobre el borrado que se hace a ésta última plataforma sin pronunciarse sobre el borrado en el resto del sistema, lo cual es factible por las características de función que pudo advertirse en los anexos antes citados y que aportan información contraria a lo indicado por el AIFA sobre que sólo se almacenan datos en la plataforma vb orchestra.

Por lo tanto, es imprescindible establecer políticas, métodos y técnicas orientadas a la supresión definitiva de los datos personales de todo el Sistema de Procesamiento, no sólo de la plataforma vb orchestra, considerando los atributos de irreversibilidad; seguridad y confidencialidad y favorable al medio ambiente.

Finalmente, es importante señalar que en la evaluación e impacto en el apartado denominado "VI. Cancelación o supresión de datos personales." se señala lo siguiente:

"[…]
Después de 24 horas posteriores a la fecha de la salida del vuelo, se ejecuta una acción de borrado, de manera automática, de todos los PDE almacenados en las Galerías de la solución biométrica. Esto se realiza con el objetivo de asegurar el borrado de los datos de los pasajeros, debido a que podrían presentarse los siguientes casos:
Que el pasajero no ingrese al área estéril del aeropuerto o no realice el abordaje.
Que el pasajero use el procedimiento de pre-seguridad de manera tradicional, con la asistencia de un agente, presentando el pase de abordar de forma física.

Que el pasajero use el procedimiento de abordaje tradicional, presentando el pase de abordar de forma física.
Que el vuelo sea suspendido.
Que exista requerimiento de las autoridades (transporte de drogas ilegales, casos de ebriedad o bajo el influjo de estupefacientes, psicotrópicos o enervantes, otros)
[...]"

[Énfasis añadido]

Por consiguiente, es posible observar que el borrado de los datos personales está sujeto no sólo a las 24 horas posteriores a la fecha de la salida del vuelo, sino a la posibilidad de que exista un requerimiento de las autoridades, por lo tanto, la limitante de 24 horas que se alude para el borrado de la información resulta insuficiente ante dicha finalidad que pudiera ocurrir posteriormente a las 24 horas que se establecen, lo cual no permitiría al AIFA cumplir con tales peticiones ya que la información no estaría disponible.

Por lo cual, se advierte una serie de inconsistencias sobre el plazo que se ha establecido para el borrado, incluido que no se estipuló un periodo de bloqueo conforme lo establece la Ley General, principalmente si el borrado sí se efectúa de manera correcta o se queda información de los titulares en posesión del AIFA para finalidades, en este caso de seguridad, inclusive de seguridad nacional, que no son del todo esclarecidas.

En función de lo anterior, se realizan las recomendaciones siguientes:

Recomendaciones en torno al principio de calidad

Clave	Recomendación
AIFA_CA_ 001	En el procedimiento de obtención de datos a través de los mostradores de documentación CUPPS-Vdesk en el que el agente valida visualmente que la identificación proporcionada corresponde al pasajero y procede con el escaneo del documento en el sistema, se recomienda verificar e implementar medidas que permitan garantizar que la información del titular que se está capturando sea verdadera y fiel a su situación a efecto de que sean exactos y pertinentes para que correspondan efectivamente al titular.
AIFA_CA_ 002	Se recomienda establecer medidas para que los datos personales se corrijan o completen, en las distintas bases de datos que estén a cargo del AIFA.
AIFA_CA_003	En atención a lo examinado, y en correspondencia con lo establecido en el apartado de derechos ARCO, se sugiere establecer mecanismos que acrediten las modificaciones que realicen los titulares con relación a su derecho de rectificación, como pudiera ser, a manera de orientación, la

	relación de constancias sobre las rectificaciones realizadas, sólo en los casos en que la misma haya sido procedente.
AIFA_CA_004	Se recomienda establecer los plazos de conservación de los datos personales considerando el límite de tiempo para que los titulares puedan enrolarse biométricamente a través de la app como el quiosco antes de su día de vuelo. Asimismo, deberá ser congruente con los plazos de conservación establecidos en los instrumentos de clasificación archivística y considerar un periodo de bloqueo.
AIFA_CA_005	Se recomienda que, al establecer un periodo de bloqueo se consideren las disposiciones legales establecidas en la Ley General de Archivos y las disposiciones aplicables en la materia de que se trate, los aspectos administrativos, contables, fiscales, jurídicos e históricos de la información.
AIFA_CA_006	Se recomienda considerar para el establecimiento del plazo de conservación, periodo de bloqueo y supresión, en caso de ser aplicable y constituirse como otra finalidad del tratamiento, el supuesto de requerimientos de las autoridades ante situaciones de transporte de drogas ilegales, casos de ebriedad o bajo el influjo de estupefacientes, psicotrópicos o enervantes, otros, así como de temas de seguridad.
AIFA_CA_007	Se recomienda elaborar los procedimientos para la conservación y supresión de los datos personales, así como documentarlos, considerando que podrán ser los establecidos en materia de archivos, si a través de los mismos se puede cumplir con la obligación prevista en la Ley General.
AIFA_CA_008	Se recomienda establecer la documentación que permita al responsable demostrar que los datos personales han sido suprimidos en atención a una solicitud de ejercicio del derecho de cancelación.
[redacted]	[redacted]
AIFA_CA_010	Se sugiere tener en cuenta que el PDE, además de contar con datos personales, debe encontrarse previsto en el Catálogo de Disposición Documental, sujetándose a las previsiones previstas en la LGA, para que los titulares conozcan los periodos de conservación, además de las recomendaciones en torno al principio de calidad.

Se eliminan 7 lineas, con fundamento en el artículo 110, fracción I de la LFTAIP; Décimo séptimo de los lineamientos Generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas, en relación con el artículo 5, fracción VI de la Ley de Seguridad Nacional; 47, Bis 4 de la Ley de Aviación Civil, 46 y 47 de la Ley de Aeropuertos y 152 del Reglamento de Aeropuertos.

1.5.1. Técnicas a utilizar para garantizar el borrado seguro de los datos personales

En particular, sobre el mecanismo de borrado seguro la Ley General menciona lo siguiente:

*"**Artículo 23.***
[...]

Cuando los datos personales hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas en el aviso de privacidad y que motivaron su tratamiento conforme a las disposiciones que resulten aplicables, deberán ser suprimidos, previo bloqueo en su caso, y una vez que concluya el plazo de conservación de los mismos."

Por su parte, los Lineamientos generales indican que:

*"**Supresión de los datos personales***
***Artículo 23.** En la supresión de los datos personales a que se refiere el artículo 23, párrafo tercero de la Ley General, el responsable deberá establecer políticas, métodos y técnicas orientadas a la supresión definitiva de éstos, de tal manera que la probabilidad de recuperarlos o reutilizarlos sea mínima.*

En el establecimiento de las políticas, métodos y técnicas a que se refiere el párrafo anterior, el responsable deberá considerar, al menos, los siguientes atributos y el o los medios de almacenamiento, físicos y/o electrónicos en los que se encuentren los datos personales:

- ***I. Irreversibilidad:** que el proceso utilizado no permita recuperar los datos personales;*
- ***II. Seguridad y confidencialidad:** que en la eliminación definitiva de los datos personales se consideren los deberes de confidencialidad y seguridad a que se refieren la Ley General y los presentes Lineamientos generales, y*
- ***III. Favorable al medio ambiente:** que el método utilizado produzca el mínimo de emisiones y desperdicios que afecten el medio ambiente."*

En el mismo sentido, las Disposiciones Administrativas, en su artículo 18 señalan que el responsable deberá describir y representar cada una de las fases de la política pública, programa, sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología que implique un tratamiento intensivo o relevante de datos personales, especificando el ciclo de vida de éstos a partir de su obtención, aprovechamiento, explotación, almacenamiento, conservación o cualquier otra operación, realizada hasta la supresión de los mismos, en particular la fracción IV establece:

*"**IV.** Las técnicas a utilizar para garantizar el borrado seguro de los datos personales."*

En esta tesitura, conforme a lo señalado en la Evaluación de impacto con relación a las técnicas del borrado seguro, se especificó lo siguiente:

"IV. Las técnicas a utilizar para garantizar el borrado seguro de los datos personales.
El método de borrado es un método estándar y se describe en el punto VI Cancelación o supresión de datos personales, del Ciclo de Vida.

La solución vb orchestraTM cuenta con la certificación Privacy-by-Design. Donde, uno de los siete principios fundamentales de la Privacidad por Diseño conocido como la "Privacidad como la configuración predeterminada" establece: "La información personal se conservará solo el tiempo que sea necesario para cumplir con los propósitos establecidos y luego se destruirá de forma segura".

Técnicamente, vb orchestraTM, hace uso de las capacidades nativas de las funciones de eliminación de datos de Microsoft Windows del motor de base de datos SQL (DELETE Comando-SQL), que permiten borrar y eliminar de forma segura la información de las bases de datos y dispositivos de almacenamiento. Adicionalmente, Vision-Box, bajo los lineamientos de la certificación ISO 27001, garantiza que aplica los controles de seguridad al crear, manejar y eliminar información personal, asegurando que seguimos los procesos definidos por el Estándar Internacional.

No se tiene contemplado la implementación de un software para futuro borrado de datos personales ya que en la actualidad la solución cuenta con un proceso y políticas de acceso y borrado seguro de los datos personales".

Por su parte, en el desahogo del requerimiento de información adicional, se refirió lo siguiente:

"• En ese sentido, se solicita remitir la documentación de los procedimientos para la conservación y, en su caso, bloqueo y supresión de los datos personales definiendo el periodo de conservación de los mismos. por lo tanto, cuál se sugiere identificar las obligaciones, en su caso, a los que el responsable como sujeto obligado se encuentra constreñido de la conservación y plazos de conservación establecidos de la información. Después de 24 horas posteriores a la fecha de la salida del vuelo, se ejecuta una acción de borrado seguro de manera automática, debido a que podrían presentarse los siguientes casos:

o Que el pasajero no ingrese al área estéril del aeropuerto o no realice el abordaje.

o Que el pasajero use el procedimiento de pre-seguridad de manera tradicional, con la asistencia de un agente, presentando el pase de abordar de forma física.

o Que el pasajero use el procedimiento de abordaje tradicional, presentando el pase de abordar de forma física.

o Que el vuelo sea suspendido.

o Que exista requerimiento de las autoridades (transporte de drogas ilegales, casos de ebriedad o bajo el influjo de estupefacientes, psicotrópicos o enervantes, otros).

El borrado seguro consiste en la eliminación de datos de Microsoft Windows del motor de base de datos SQL (DELETE Comando-SQL), que permiten borrar y eliminar de forma segura la información de las bases de datos y dispositivos de almacenamiento."

[...]

16. Con fundamento en el artículo 14 fracción III 18 fracción IV de las disposiciones administrativas, se solicita la siguiente información:

Se requiere información sobre la metodología y técnicas de para el borrado seguro de datos personales implementadas en las bases de datos que se encuentran en la infraestructura del AIFA, ya que la documentación presentada no incluye información respecto al borrado de los

datos personales que se describe tiene lugar en bases de datos denominadas galerías de pre-registro, de abordaje y de registros biométricos.
La técnica utilizada para garantizar el borrado seguro de los datos personales es la solución vb orchestraTM cuenta con la certificación Privacy-by-Design. donde, uno de los siete principios fundamentales de la Privacidad por Diseño conocido como la "Privacidad como la configuración predeterminada" establece:
"La información personal se conservará solo el tiempo que sea necesario para cumplir con los propósitos establecidos y luego se destruirá de forma segura". Técnicamente, vb orchestraTM, hace uso de las capacidades nativas de las funciones de eliminación de datos de Microsoft Windows del motor de base de datos SQL (DELETE Comando-SQL), que permiten borrar y eliminar de forma segura la información de las bases de datos y dispositivos de almacenamiento. Adicionalmente, Vision-Box, bajo los lineamientos de la certificación ISO 27001, garantiza que aplica los controles de seguridad al crear, manejar y eliminar información personal, asegurando que seguimos los procesos definidos por el Estándar Internacional. En este sentido, es necesario incluir la documentación que identifique la consideración de la implementación de borrado seguro de los datos personales que son transferidos a los sistemas provistos por AMADEUS y ORCHESTRA. Debido a la naturaleza del sistema y que Amadeus no realiza almacenamiento de datos personales, se da cumplimiento con el borrado seguro desde la plataforma de VBOrchestra."

Conforme a lo anteriormente expuesto, se desprende que el AIFA manifestó esencialmente sobre el borrado seguro:

- Que la solución vb orchestraTM cuenta con la certificación Privacy-by-Design, que comprende siete principios fundamentales entre los cuales se señala que la información personal se conservará solo el tiempo que sea necesario para cumplir con los propósitos establecidos y luego se destruirá de forma segura,
- Por lo que desde una visión técnica, vb orchestraTM, hace uso de las capacidades nativas de las funciones de eliminación de datos de Microsoft Windows del motor de base de datos SQL (DELETE Comando-SQL), que permiten borrar y eliminar de forma segura la información de las bases de datos y dispositivos de almacenamiento,
- Adicionalmente, Vision-Box, bajo los lineamientos de la certificación ISO 27001, garantiza que aplica los controles de seguridad al crear, manejar y eliminar información personal, asegurando que seguimos los procesos definidos por el Estándar Internacional,
- Que después de 24 horas posteriores a la fecha de la salida del vuelo, se ejecuta una acción de borrado seguro de manera automática, debido a que podrían presentarse los siguientes casos: que el pasajero no ingrese al área estéril del aeropuerto o no realice el abordaje, use el procedimiento de pre-seguridad de manera tradicional, con la asistencia de un agente, presentando el pase de abordar de forma física o bien siga el procedimiento de abordaje tradicional, presentando el pase de abordar de forma física. Además de que el vuelo sea

suspendido o exista requerimiento de las autoridades (transporte de drogas ilegales, casos de ebriedad o bajo el influjo de estupefacientes, psicotrópicos o enervantes, otros),

- Que no tiene contemplado la implementación de un software para futuro borrado de datos personales ya que en la actualidad la solución cuenta con un proceso y políticas de acceso y borrado seguro de los datos personales,
- Que el borrado seguro consiste en la eliminación de datos de Microsoft Windows del motor de base de datos SQL (DELETE Comando-SQL), que permiten borrar y eliminar de forma segura la información de las bases de datos y dispositivos de almacenamiento."
- Adicionalmente, Vision-Box, bajo los lineamientos de la certificación ISO 27001, garantiza que aplica los controles de seguridad al crear, manejar y eliminar información personal, asegurando que seguimos los procesos definidos por el Estándar Internacional, y
- Señaló que debido a la naturaleza del sistema y que Amadeus no realiza almacenamiento de datos personales, se da cumplimiento con el borrado seguro desde la plataforma de VBOrchestra.

Al respecto, es oportuno recordar que, conforme a la Guía de Borrado Seguro emitida por este Instituto, dicho borrado es la medida de seguridad mediante la cual se establecen métodos y técnicas para la eliminación definitiva de los datos personales, de modo que la probabilidad de recuperarlos sea mínima. En ese sentido, los beneficios de aplicarlo son:

- Eliminar adecuadamente los medios de almacenamiento en desuso representa una medida de seguridad efectiva para minimizar las fugas y/o el mal uso de los datos personales por parte de una persona mal intencionada, o no autorizada,
- Se optimizan los espacios y los procesos, en particular con la eliminación periódica de los denominados "archivos muertos", y
- Se previenen las afectaciones económicas y de imagen debido a multas, compensación de daños y pérdida de clientes e inversionistas.

En ese sentido, el documento aludido establece que para el caso de información que existe en medios electrónicos, deben preferirse aquellos métodos que destruyan el almacenamiento o bien aplicar métodos lógicos, que implican la sobreescritura o modificación del contenido del medio de almacenamiento electrónico, incluyéndose en estos la magnetización, la sobreescritura o el cifrado.

La desmagnetización implica exponer los dispositivos de almacenamiento a un campo magnético a través de un dispositivo denominado desmagnetizador que altera directamente el contenido de información y no al medio de almacenamiento en sí mismo; por lo que es posible que el hardware donde se encuentra la información se vuelva inoperable, en consecuencia, es recomendable aplicar este método si no se volverá a utilizar el medio de almacenamiento.

La sobreescritura implica sobrescribir todas las ubicaciones de almacenamiento utilizables en un medio de almacenamiento, es decir, se trata de escribir información nueva en la superficie de almacenamiento, en el mismo lugar que los datos existentes, utilizando herramientas de software.

El método más simple consiste en realizar una sola sobreescritura, y para implementar una mayor seguridad se pueden efectuar múltiples sobreescrituras o "pasadas" con variaciones en los caracteres grabados al medio de almacenamiento, esto para borrar un archivo o carpeta específica, sin necesidad de alterar o detener la operación de todo un medio de almacenamiento o equipo de cómputo.

Al respecto, primero, se identifica que la información se encuentra centralizada y operada en una infraestructura, que esta información puede ser de dos naturalezas biométrica en el PDE o no biométrica en el BCBP y que, es procesada en dos momentos, al ingresar a pre-seguridad y a abordaje, no es posible identificar si se tienen bases de datos temporales para cada área señalada o en qué momento ocurre el borrado de datos biométricos y no biométricos dentro de cada proceso, específicamente se hace énfasis en la eliminación de datos no biométricos ya que, la descripción proporcionada por el AIFA determina el borrado del PDE sin especificar qué ocurre con los datos registrados a partir del BCBP.

Este Instituto advirtió la mención de que los datos en las galerías de preseguridad y abordaje serían eliminados, lo cierto es que no se señala específicamente la técnica aplicable para esos casos.

Por otro lado, no se identifica en el ciclo de vida de datos cómo ocurrirá el borrado de perfil de usuario que haya ingresado sus documentos digitalizados desde un dispositivo y su fotografía ya que, el borrado que se menciona refiere al pase del pasajero entre dos áreas dentro del aeropuerto, dejando de lado el tratamiento de los datos adicionales que son proporcionados durante el registro del usuario desde el aplicativo, mostrador o quiosco, siendo la obtención de los datos el mecanismo para ejercer el derecho de Cancelación de datos para el elemento biométrico del sistema de tratamiento, es decir, describiendo la eliminación de perfiles desde el dispositivo del usuario a través de la app móvil o desde el mostrador o quiosco, según lo requiera el usuario.

Adicionalmente, el AIFA expresa que técnicamente, vb orchestraTM, hace uso de las capacidades nativas de las funciones de eliminación de datos de Microsoft Windows del motor de base de datos SQL (DELETE Comando-SQL), que permiten borrar y eliminar de forma segura la información de las bases de datos y dispositivos de almacenamiento.

Al respecto, este Instituto advierte que el uso del comando DELETE en un Query no puede ser considerado un método de borrado seguro ya que es necesario conocer los parámetros en que se

ejecuta dicho Query, identificando fehacientemente que no hay un comando que deshaga la instrucción del comando anterior, como lo pudiera ser un Rollback transaction. Por lo que, no se presentaron elementos que demuestren la ejecución de un borrado seguro de información a nivel implementación de base datos.

De esta manera, para cumplir con el borrado seguro de información, es necesario que el método o estándar implementado brinde la evidencia de la realización de una destrucción de activo primario (dato personal a nivel software) o activo de apoyo (hardware y/o software) lo cual daría garantía de la ejecución de un correcto borrado de datos personales.

Finalmente, este Instituto advierte la frecuente remisión a instrumentos normativos que no son aplicables en el territorio nacional como el RGPD, esto sin señalar como el método de borrado establecido podría ser considerado de esa manera bajo los parámetros señalados a lo largo de la presente exposición.

En función de lo anterior, se realizan las recomendaciones siguientes:

Recomendaciones en torno al borrado seguro

Clave	Recomendación
AIFA_TB_ 001	Se sugiere establecer métodos de borrado a nivel de base de datos que cumplan con los criterios mínimos para evitar la recuperación de la información.
AIFA_TB_002	Se sugiere apegarse a la normatividad aplicable en los Estados Unidos Mexicanos para la implementación de métodos de borrado seguro.
AIFA_TB_003	Se sugiere que el método o estándar implementado brinde la evidencia de la realización de una destrucción de activo primario (dato personal a nivel software) o activo de apoyo (hardware y/o software) lo cual daría garantía de la ejecución de un correcto borrado de datos personales, identificando el servidor público que intervino y el momento en que se realizó.
AIFA_TB_004	Se sugiere que en el ciclo de vida de datos se identifique y documente cómo ocurrirá el borrado de perfil de usuario que haya ingresado sus documentos digitalizados desde un dispositivo y su fotografía.
AIFA_TB_005	Se sugiere que, respecto a la evidencia de borrado, pueda identificarse con precisión cuando se eliminaron las galerías de preseguridad y abordaje, así como el método adoptado.
AIFA_TB_006	Se sugiere, en seguimiento a las recomendaciones sobre los derechos ARCO, que al momento de obtener los datos se especifique el mecanismo para ejercer el derecho de Cancelación de datos en el elemento biométrico

	del sistema de tratamiento, es decir, describiendo la eliminación de perfiles desde el dispositivo del usuario a través de la app o desde el mostrador o quiosco, según lo requiera el usuario.

1.6. Principio de proporcionalidad

El artículo 25 de la Ley General establece lo siguiente:

> ***"Artículo 25.*** *El responsable sólo deberá tratar los datos personales que resulten adecuados, relevantes y estrictamente necesarios para la finalidad que justifica su tratamiento."*

A su vez, los artículos 24 y 25 de los Lineamientos Generales señalan lo siguiente:

> ***"Principio de proporcionalidad***
> ***Artículo 24.*** *En términos del artículo 25 de la Ley General y los presentes Lineamientos generales, se entenderá que los datos personales son adecuados, relevantes y estrictamente necesarios cuando son apropiados, indispensables y no excesivos para el cumplimiento de las finalidades que motivaron su obtención, de acuerdo con las atribuciones conferidas al responsable por la normatividad que le resulte aplicable."*
>
> ***Criterio de minimización***
> ***"Artículo 25.*** *El responsable deberá realizar esfuerzos razonables para limitar los datos personales tratados al mínimo necesario, con relación a las finalidades que motivan su tratamiento."*

De las disposiciones citadas, se observa que el responsable está obligado a recabar y utilizar los datos personales que resulten estrictamente necesarios y pertinentes para los objetivos que persigue, de acuerdo con las atribuciones conferidas al responsable por la normatividad que le resulte aplicable, así como realizar esfuerzos razonables para limitar los datos personales tratados al mínimo necesario, con relación a las finalidades que motivan su tratamiento.

Al respecto, en en la Evaluación de impacto el AIFA manifestó lo siguiente:

> ***"V. Categorías de los titulares.***
> *El sistema se definió y quedó configurado para no procesar biométricamente a pasajeros menores de edad. Para menores de edad se realizará el procedimiento tradicional (proceso no biométrico).*
> *[...]*
> *• El pasajero deberá proveer su documento de identidad (Pasaporte electrónico, pasaporte no electrónico o INE, según la fuente de registro biométrico).*
> *• El pasajero deberá estar documentado en un vuelo. Deberá poseer un Pase de Abordar válido.*
> *• Se deberá poder capturar una imagen del rostro (fotografía).*

• *El pasajero deberá ser mayor de edad (configuración actual de la plataforma vb orchestraTM)*

VI. Datos personales que serán objeto de tratamiento.



Se eliminan 39 lineas, con fundamento en el artículo 110, fracción I de la LFTAIP; Décimo séptimo de los lineamientos Generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas, en relación con el artículo 5, fracción VI de la Ley de Seguridad Nacional; 47, Bis 4 de la Ley de Aviación Civil, 46 y 47 de la Ley de Aeropuertos y 152 del Reglamento de Aeropuertos.

Instituto Nacional de
Transparencia,
Acceso a la Información y
Protección de Datos Personales

[redacted]



Se eliminan 45 lineas, con fundamento en el artículo 110, fracción I de la LFTAIP; Décimo séptimo de los lineamientos Generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas, en relación con el artículo 5, fracción VI de la Ley de Seguridad Nacional; 47, Bis 4 de la Ley de Aviación Civil, 46 y 47 de la Ley de Aeropuertos y 152 del Reglamento de Aeropuertos.

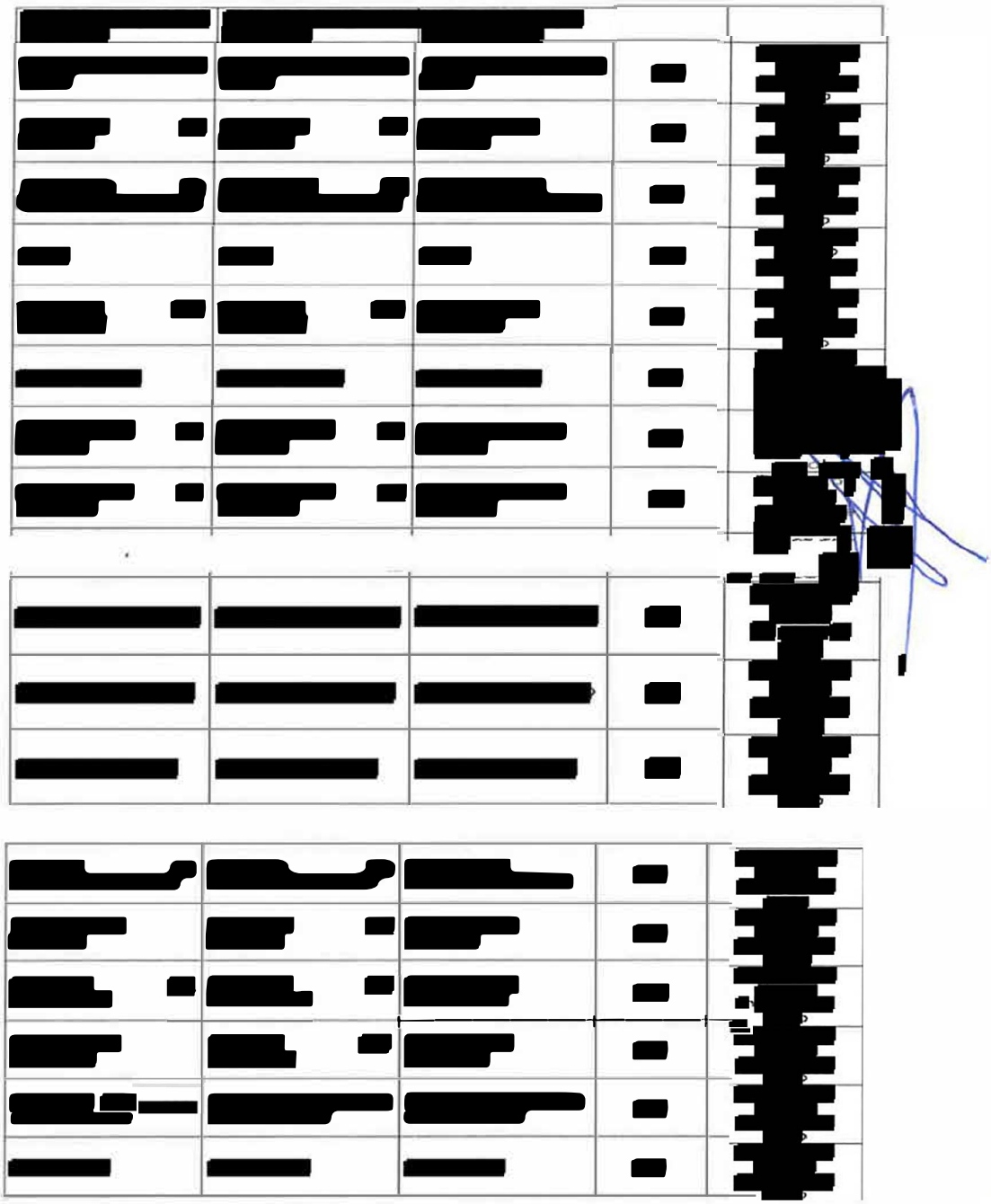




Se eliminan 37 lineas, con fundamento en el artículo 110, fracción I de la LFTAIP; Décimo séptimo de los lineamientos Generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas, en relación con el artículo 5, fracción VI de la Ley de Seguridad Nacional; 47, Bis 4 de la Ley de Aviación Civil, 46 y 47 de la Ley de Aeropuertos y 152 del Reglamento de Aeropuertos.

Instituto Nacional de
Transparencia,
Acceso a la Información y
Protección de Datos Personales

[redacted]



Se eliminan 53 lineas, con fundamento en el artículo 110, fracción I de la LFTAIP; Décimo séptimo de los lineamientos Generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas, en relación con el artículo 5, fracción VI de la Ley de Seguridad Nacional; 47, Bis 4 de la Ley de Aviación Civil, 46 y 47 de la Ley de Aeropuertos y 152 del Reglamento de Aeropuertos.

Durante el proceso de registro/enrolamiento biométrico no se crea una dupla usuario/contraseña para el pasajero o titular de los datos personales.
El PDE que se crea dentro de la plataforma vb orchestra es utilizado para la identificación del pasajero en los puntos de validación de identidad (pre-seguridad y abordaje). El PDE es un identificador digital único de cada pasajero, contenido dentro de la plataforma vb orchestra TM."

Asimismo, se manifestó lo siguiente:

a) Quioscos de autoservicio (CUSS)
Los datos que se reciben del quiosco son los siguientes:

Datos del dispositivo (quiosco)
1. Nombre del dispositivo
2. Tipo de Dispositivo
3. Nombre del aeropuerto
4. Número de Terminal
5. Código de Aerolínea
6. Vendedor
7. Horario

Datos del documento del pasajero (Pasaporte electrónico)
1. Nombre completo
2. Fecha de nacimiento
3. País de Nacionalidad
4. Género
5. Tipo de documento
6. Número de documento
7. País de emisión de documento
8. Fecha de expiración del documento

Datos del Pase de Abordar
1. Tipo de Código de Barra
2. Formato de Código
3. Indicador de Ticket Electrónico
4. RAW
5. Nombre del Pasajero
6. Código PNR
7. Aeropuerto de Origen
8. Aeropuerto de Destino
9. Código del Carrier
10. Número de Vuelo
11. Fecha del Vuelo
12. Código de Compartimiento
13. Número de Asiento
14. Número de Secuencia
15. Estatus del Pasajero
16. Número Serial del Documento
17. Leg Order

Datos de la fotografía
1. Foto (vector)
2. Id de la cámara

b) Mostradores de documentación CUPPS-Vdesk.

Los datos que se reciben del Mostrador de documentación (CUPPS) a través del VDESK son los siguientes:

Datos del dispositivo

1. Nombre del dispositivo (VDESK)
2. Tipo de Dispositivo
3. Nombre del aeropuerto
4. Número de Terminal
5. Código de Aerolínea
6. Vendedor
7. Horario

Datos del documento del pasajero (INE)

1. Nombre completo
2. Número de documento
3. País de Nacionalidad
4. Fecha de Validez del documento
5. Género

Datos del documento del pasajero (Pasaporte no electrónico)

1. Nombre completo
2. Número de pasaporte
3. País de Emisión
4. País de Nacionalidad
5. Fecha de validez del documento
6. Fecha de Nacimiento
7. Género

Datos del documento del pasajero (Pasaporte electrónico)

1. Fecha de Nacimiento
2. Número de documento
3. Nombre completo
4. País de Nacionalidad
5. País de Emisión
6. Fecha de Validez del documento
7. Género

Datos del Pase de Abordar

1. Tipo de Código de Barra
2. Formato de Código
3. Indicador de Ticket Electrónico
4. RAW
5. Nombre del Pasajero
6. Código PNR
7. Aeropuerto de Origen
8. Aeropuerto de Destino
9. Código del Carrier
10. Número de Vuelo
11. Fecha del Vuelo
12. Código de Compartimiento
13. Número de Asiento
14. Número de Secuencia
15. Estatus del Pasajero
16. Número Serial del Documento
17. Leg Order

Datos de la fotografía

1. Foto (vector)
2. Id de la cámara

c) Aplicación móvil AIFA.
Los datos leídos del ***pasaporte electrónico para el procesamiento del pasajero son los siguientes:***
1. Nombre completo
2. Fecha de nacimiento
3. País de Nacionalidad
4. Género
5. Tipo de Documento
6. Número de documento
7. País de emisión de documento
8. Fecha de expiración del documento
9. Foto del chip del pasaporte
10. Foto capturada por el dispositivo móvil (vector)

Datos del Pase de Abordar
1. Tipo de Código de Barra
2. Formato de Código
3. Indicador de Ticket Electrónico
4. RAW
5. Nombre del Pasajero
6. Código PNR
7. Aeropuerto de Origen
8. Aeropuerto de Destino
9. Código del Carrier
10. Número de Vuelo
11. Fecha del Vuelo
12. Código de Compartimiento
13. Número de Asiento
14. Número de Secuencia
15. Estatus del Pasajero
16. Número Serial del Documento
17. Leg Order

d) Modo no biométrico.
Los datos que se obtienen del ***pase de abordar son los siguientes****:*
1. Tipo de Código de Barra
2. Formato de Código
3. Indicador de Ticket Electrónico
4. RAW
5. Nombre del Pasajero
6. Código PNR
7. Aeropuerto de Origen
8. Aeropuerto de Destino
9. Código del Carrier
10. Número de Vuelo
11. Fecha del Vuelo
12. Código de Compartimiento
13. Número de Asiento
14. Número de Secuencia
15. Estatus del Pasajero
16. Número Serial del Documento
17. Leg Order

Por su parte, en el desahogo del requerimiento de información adicional se señaló lo siguiente con relación al cumplimiento de este principio:

> *"En la página web será publicado el procedimiento de enrolamiento para conocimiento de los particulares, como un ejercicio del principio de información. De conformidad con el artículo 25 de la ley general de datos, referente al principio de proporcionalidad, si bien, se identifican los datos personales requeridos para cada finalidad, hoy se solicita indicar los esfuerzos razonables y que se han realizado para limitar los datos personales tratados al mínimo*

necesario, con relación a la finalidad que motiva su tratamiento. así mismo, indicar las razones y justificaciones por las cuales se determina que los datos personales tratados son adecuados, relevantes y estrictamente necesarios, de conformidad con el artículo 24 de los lineamientos generales.

En relación con la finalidad definida del tratamiento de los datos guarda relación únicamente con el procesamiento y abordaje de los usuarios, el hecho de guardarlos por un tiempo mayor incluso, podría considerarse como un incumplimiento al criterio de minimización señalado en el artículo 25 de los lineamientos.

Cabe mencionar que La solución de gestión de identidades Vision-Box, vb orchestra™, cuenta con la certificación "Privacy by Design (PbD)". Esto significa que los datos personales de los pasajeros (biográficos y biométricos) serán gestionados por una plataforma de software que fue diseñada con la máxima protección y privacidad y con un riesgo minimizado de fuga.

El PbD se encuentra apegado a las regulaciones de gestión de datos personales, incluidas las regulaciones GDPR (General Data Protection Regulation) de la Unión Europea, también se tienen en cuenta al diseñar la plataforma Orchestra. General Data Protection Regulation o, en español, Reglamento General de Protección de Datos teniendo como principio de implementación la Minimización de datos, así como en el propósito delimitado de recolectar datos personales adecuados y relevantes para la finalidad.

Con relación a la "expectativa razonable de privacidad; en el que se confirme que el tratamiento no da lugar a discriminación o trato injusto orbitario en contra del titular, por lo cual, deberá señalar las razones que se consideren sustenta en el cumplimiento de este principio por parte del responsable."

Al respecto, se trae a colación lo manifestado en el "Anexo 1. Glosario" de la evaluación de impacto, que señala:

***PNR**: Passenger Name Record (Registro de Nombre del Pasajero)*

***Código del Carrier:** Código identificador de la aerolínea. (IATA: dos letras, OACI: tres letras).*

***Código PNR:** Número de 10 dígitos generado automáticamente por la reserva de boleto de avión. Sirve de clave única para localizar los datos de cualquier viaje*

***Foto del chip:** Foto del pasajero contenida en el chip digital del pasaporte electrónico, grabada desde el momento de emisión del documento.*

***Leg Order**: Segmento de vuelo. Dato asociado al vuelo.*

***RAW:** Cadena de caracteres que conforman algunos de los datos que se comparten en el pase de abordar.*

Es importante señalar que, dentro de la documentación que se solicita, la misma conlleva a más información, como es el caso del PNR, en ese sentido, se tiene que dentro de la evaluación de impacto, en el "Anexo 6 PROTOCOLOS" por el AIFA, se encuentra el documento denominado "INTERNATIONAL AIR TRANSPORT ASSOCIATION" (AITA, por sus siglas en inglés), dicha asociación emitió el documento denominado "Guidelines on Passenger Name Record (PNR)

Data[55]" que si bien no se hizo de conocimiento durante el desarrollo de la evaluación, al obrar en fuente de acceso público, se trae a colación, únicamente con la finalidad de conocer los datos que se recopilan en el PNR que son: las reservas realizadas que puede incluir nombre, itinerario e indicador de boleto, cambios en asientos, preferencias de comida y servicios adicionales solicitados, información de salud, información sobre "menores no acompañados", solicitudes de asistencia, entre otros.

En ese sentido, el tratamiento de dicha información debe realizarse en atención al marco que lo regula y en su caso considerar si la recolección de dicha datos es pertinente en el tratamiento del sistema de pasajeros, atendiendo al criterio de minimización, considerando la protección de datos personales, el derecho a la no discriminación, así como a la privacidad.

El uso del PNR también guarda una importancia para las autoridades estatales, pues del análisis de dichos datos, pueden obtenerse herramientas útiles para la lucha, prevención, investigación o enjuiciamiento contra el terrorismo y la delincuencia grave, y precisamente en la utilidad de esta información es en la que se ha basado los periodos para su conservación por parte de múltiples Estados, pues debe de encontrarse disponible para garantizar que las investigaciones puedan llevarse a cabo de manera completa e integra para cumplir con los fines de impartición de justicia.

Establecido lo anterior, debe recordarse que, al analizar el principio de finalidad, este Instituto identificó que si bien existen múltiples fuentes de obtención de datos personales lo cierto es que integran el Sistema de Procesamiento, y tienen el mismo objetivo, también es cierto que las vías de obtención son diferentes, en ese sentido se tiene que las finalidades del sistema en general son las siguientes:

- Crear y realizar el registro biométrico (enrolamiento biométrico) del pasajero mediante un token digital denominado PDE.
- Almacenar los datos personales del pasajero dentro de la plataforma vb orchestra.
- Identificar y validar biométricamente a los pasajeros en los puntos de validación desde el ingreso a salas de última espera, hasta el abordaje a la aeronave.
- Validar la existencia de registros biométricos para pasar a los filtros de pre-seguridad y realizar el abordaje.
- Permitir el flujo ininterrumpido para el acceso de los pasajeros para pasar a los filtros de pre-seguridad y realizar el embarque a la aeronave de manera rápida y segura.
- Transferir datos a las aerolíneas para avisar que el pasajero ha abordado la aeronave.
- Permitir el paso de los pasajeros que no realizaron su registro biométrico.

---

[55] Disponible para su consulta en el vínculo: https://www.iata.org/contentassets/18a5fdb2dc144d619a8c10dc1472ae80/new_doc_9944_1st_edition_pnr.pdf, enlace consultado por última vez el 28/02/23.

- Fortalecer el proceso de seguridad mediante la identificación de pasajeros que ingresan a la zona de pre-seguridad y confirmar la validez del pase de abordar con las aerolíneas.
- Contar con información estadística del número de pasajeros que ingresan a los filtros de seguridad y realizan el abordaje mediante el uso de los E-gates (esta información no incluye datos personales).
- Validar que no exista un enrolamiento/registro previo del pasajero

En tanto, se desprende que, para cada uno de los tres medios de recepción de datos personales considerados en la evaluación de impacto, se efectúa el recabo en los siguientes términos:

Tipo de dato	Quioscos de autoservicio (CUSS)	Mostradores de documentación CUPPS-Vdesk	Aplicación móvil AIFA
Datos del dispositivo	1. Nombre del dispositivo	1. Nombre del dispositivo (VDESK)	No tiene correlativo.
	2. Tipo de Dispositivo	2. Tipo de Dispositivo	
	3. Nombre del aeropuerto	3. Nombre del aeropuerto	
	4. Número de Terminal	4. Número de Terminal	
	5. Código de Aerolínea	5. Código de Aerolínea	
	6. Vendedor	6. Vendedor	
	7. Horario	7. Horario	
Datos del documento del pasajero (Pasaporte electrónico)	1. Nombre completo	1. Nombre completo	1. Nombre completo
	2. Fecha de nacimiento	2. Fecha de Nacimiento	2. Fecha de nacimiento
	3. País de Nacionalidad	3. País de Nacionalidad	3. País de Nacionalidad
	4. Género	4. Género	4. Género
	5. Tipo de documento	No tiene correlativo	5. Tipo de Documento
	6. Número de documento	5. Número de documento	6. Número de documento

	7. País de emisión de documento	6. País de Emisión	7. País de emisión de documento
	8. Fecha de expiración del documento	7. Fecha de Validez del documento	8. Fecha de expiración del documento
	No tiene correlativo	No tiene correlativo	9. Foto del chip del pasaporte
	No tiene correlativo	No tiene correlativo	10. Foto capturada por el dispositivo móvil (vector)
Pasaporte no electrónico	No tiene correlativo	1. Nombre completo	No tiene correlativo
	No tiene correlativo	2. Número de pasaporte	No tiene correlativo
	No tiene correlativo	3. País de Emisión	No tiene correlativo
	No tiene correlativo	4. País de Nacionalidad	No tiene correlativo
	No tiene correlativo	5. Fecha de validez del documento	No tiene correlativo
	No tiene correlativo	6. Fecha de Nacimiento	No tiene correlativo
	No tiene correlativo	7. Género	No tiene correlativo
Credencial para votar	No tiene correlativo	1. Nombre completo	No tiene correlativo
	No tiene correlativo	2. Número de documento	No tiene correlativo
	No tiene correlativo	3. País de Nacionalidad	No tiene correlativo
	No tiene correlativo	4. Fecha de Validez del documento	No tiene correlativo
	No tiene correlativo	5. Género	No tiene correlativo
Datos del pase de abordar (Biométrico y no Biométrico, este último solo para Mostradores de	1. Tipo de Código de Barra	1. Tipo de Código de Barra	1. Tipo de Código de Barra
	2. Formato de Código	2. Formato de Código	2. Formato de Código
	3. Indicador de Ticket Electrónico	3. Indicador de Ticket Electrónico	3. Indicador de Ticket Electrónico
	4. RAW	4. RAW	4. RAW

documentación CUPPS-Vdesk)	5. Nombre del Pasajero	5. Nombre del Pasajero	5. Nombre del Pasajero
	6. Código PNR	6. Código PNR	6. Código PNR
	7. Aeropuerto de Origen	7. Aeropuerto de Origen	7. Aeropuerto de Origen
	8. Aeropuerto de Destino	8. Aeropuerto de Destino	8. Aeropuerto de Destino
	9. Código del Carrier	9. Código del Carrier	9. Código del Carrier
	10. Número de Vuelo	10. Número de Vuelo	10. Número de Vuelo
	11. Fecha del Vuelo	11. Fecha del Vuelo	11. Fecha del Vuelo
	12. Código de Compartimiento	12. Código de Compartimiento	12. Código de Compartimiento
	13. Número de Asiento	13. Número de Asiento	13. Número de Asiento
	14. Número de Secuencia	14. Número de Secuencia	14. Número de Secuencia
	15. Estatus del Pasajero	15. Estatus del Pasajero	15. Estatus del Pasajero
	16. Número Serial del Documento	16. Número Serial del Documento	16. Número Serial del Documento
	17. Leg Order	17. Leg Order	17. Leg Order
Datos de la fotografía	1. Foto (vector)	1. Foto (vector)	No tiene correlativo
	2. Id de la cámara	2. Id de la cámara	No tiene correlativo

Es importante señalar que entre los medios de recabo existen importantes diferencias, pues mientras en la aplicación móvil se encuentra los datos personales relacionados con el pasaporte electrónico y el pase de abordar, en el Quiosco y en el mostrador se requieren datos adicionales relacionados con el equipo desde el cual se obtuvieron los datos biométricos, así como los datos del vendedor.

Sobre los datos relacionados con el equipo desde el cual se toma la biometría, se desprende que esos equipos son aquellos descritos en la evaluación de impacto presentada que fueron instalados en el Aeropuerto Internacional Felipe Ángeles.

Sin embargo, este Instituto advirtió que el PDE tiene, entre otros, los datos del vendedor, esto sin especificar en qué consiste esa información, si contempla el nombre del vendedor, su clave única de registro de población, un número de empleado o alguna información que lo haga identificado o identificable, en este último caso considerando que podría particularizarse considerando que presta

sus servicios para un permisionario o aerolínea que presta sus servicios aéreos desde el Aeropuerto Internacional Felipe Ángeles.

Lo anterior es relevante, ya que, en cualquier caso, el AIFA no cuenta con el carácter de responsable del tratamiento respecto de la existencia de la relación laboral de ese vendedor con un permisionario o aerolínea, por lo que cualquier tratamiento que realice sobre cualquier dato personal de dichos titulares debe encontrarse justificado y previsto en un aviso de privacidad específico para tales efectos.

Sin embargo, este Instituto no advierte una finalidad que pueda justificar el tratamiento de datos personales diversos a los del titular que utiliza los servicios que proporcionar el responsable para facilitar el uso de las instalaciones aeroportuarias. Lo anterior, ya que esa facilitación no conlleva la necesidad de que datos personales de terceros sean tratados para ese uso, pues su objetivo es facilitar la revisión y abordaje de una persona que no es ese vendedor.

Por lo cual, respecto al dato del vendedor, se advierte podría constituir un tratamiento desproporcional de datos personales y con ello, afectar la vida íntima de un titular de datos personales ajeno de la que se realizó el enrolamiento biométrico.

Ahora bien, respecto a los datos recabados del pasaporte electrónico, este Instituto advierte que se obtienen de tal documento, mediante los tres medios de recabo, la siguiente información:

- Nombre completo,
- Número de pasaporte,
- País de Emisión,
- País de Nacionalidad,
- Fecha de validez del documento,
- Fecha de Nacimiento, y
- Género.

Sin embargo, para el caso de la aplicación móvil, se señala que se recaban tanto la foto del chip del pasaporte, así como el vector derivado de la foto capturada por el dispositivo móvil. El primero de los datos mencionados se encuentra presente en los datos personales recabados en los Quioscos como en el mostrador, junto con el ID del dispositivo desde el cual se recabó.

Sobre los datos biométricos, identificados con el vector derivado de la foto capturada por el dispositivo móvil, debe recordarse que existen disposiciones de OACI que permiten ese tratamiento, Sin embargo, ello no implica que a la par en el uso de datos biométricos pueda recabarse una amplitud de datos personales.

En ese sentido, resulta indispensable que a la par de los datos biométricos a tratar, se aplique un criterio de minimización consistente en precisar los datos mínimos indispensables para realizar una actividad sin afectarla. Resulta especialmente relevante el dato personal relacionado con el género, ya que principio no se advierte de las finalidades establecidas por OACI en el marco del Convenio de Chicago como podría ayudar a la búsqueda de esas finalidades.

Igualmente, este Instituto advierte que la Concesión del AIFA implica considerar que, en términos del artículo 146 de la Ley General del Sistema Nacional de Seguridad Pública[56] son instalaciones estratégicas, a los espacios, inmuebles, construcciones, muebles, equipo y demás bienes, destinados al funcionamiento, mantenimiento y operación de las actividades consideradas como estratégicas por la Constitución Política de los Estados Unidos Mexicanos, así como de aquellas que tiendan a mantener la integridad, estabilidad y permanencia del Estado Mexicano, en términos de la Ley de Seguridad Nacional.

Por su parte, en el artículo 5 de la Ley de Seguridad Nacional[57] se enlistan las que se consideran amenazas a la Seguridad Nacional, entre las cuales se localizan supuestos relacionados al espionaje, sabotaje, terrorismo, rebelión, traición a la patria, genocidio, interferencia extranjera en los asuntos nacionales que puedan implicar una afectación al Estado Mexicano; **actos tendentes a obstaculizar o bloquear operaciones militares o navales contra la delincuencia organizada**, delincuencia organizada; **la seguridad de la aviación**; personal diplomático; tráfico ilegal de materiales nucleares, de armas químicas, biológicas y convencionales de destrucción masiva; navegación marítima; inteligencia o contrainteligencia; infraestructura de carácter estratégico o indispensable para la provisión de bienes o servicios públicos, y actos ilícitos en contra del fisco federal.

En ese sentido, se desprende que el AIFA tiene la concesión para la explotación del Aeropuerto Internacional Felipe Ángeles, por ende, tiene a su cargo una instalación estratégica, ya que dicha instalación tiene como parte de sus funciones la prestación del servicio complementario de tráfico de pasajeros, lo cual es uno de los motivos por los que debe mantenerse la seguridad de la aviación, para permitir el transporte seguro de pasajeros y mercancías.

En ese sentido, el responsable señala que durante el proceso de registro/enrolamiento biométrico no se crea una dupla usuario/contraseña para el pasajero o titular de los datos personales. Para

[56] Publicada en el Diario Oficial de la Federación el 2 de enero de 2009, texto consolidado por la Cámara de Diputados del H. Congreso de la Unión en formato de documento portable, denominado como pdf por sus siglas en inglés, incorporando las diversas reformas de dicho ordenamiento jurídico en el sitio siguiente: https://www.diputados.gob.mx/LeyesBiblio/pdf/LGSNSP.pdf, enlace consultado por última vez el 28/02/2023.

[57] Publicada en el Diario Oficial de la Federación el 31 de enero de 2005, texto consolidado por la Cámara de Diputados del H. Congreso de la Unión en formato de documento portable, denominado como pdf por sus siglas en inglés, incorporando las diversas reformas de dicho ordenamiento jurídico en el sitio siguiente: https://www.diputados.gob.mx/LeyesBiblio/pdf/LSN.pdf, enlace consultado por última vez el 28/02/2023.

ello, se crea el PDE dentro de la plataforma vb orchestra es utilizado para la identificación del pasajero en los puntos de validación de identidad (pre-seguridad y abordaje), ello se constituye en un identificador digital único de cada pasajero, contenido dentro de la plataforma vb orchestra TM.

El AIFA indica que, con motivo de la finalidad definida del tratamiento de los datos, esto es, al guardar relación únicamente con el procesamiento y abordaje de los usuarios, el hecho de guardarlos por un tiempo mayor incluso podría considerarse como un incumplimiento al criterio de minimización señalado en el artículo 25 de los Lineamientos Generales.

Retomando la importancia del PNR, este Instituto advierte una doble utilidad de identificar a los pasajeros, en el presente caso mediante el PDE, la primera es de carácter comercial para conocer los gustos y preferencias de las personas que son transportadas, mientras que la segunda es de carácter de seguridad nacional, ya que permite identificar a las personas que se encuentran involucradas personas que en principio fueron pasajeros pero que realizaron o han realizado actos ilícitos graves o muy graves.

Lo anterior, ya que al ser un lugar de origen y destino pueden concurrir diferentes circunstancias que pueden requerir de la información recabada para tramitarse adecuadamente.

Por ejemplo, en la Ley de Aviación Civil se establece en su artículo 79 que los concesionarios deberán proveerse de equipos técnicos y de personal necesario para la prevención de accidentes e incidentes aéreos, además, en el diverso 80, se establece que la búsqueda y salvamento en accidentes de aeronaves civiles es de interés público y que los concesionarios estarán obligados a participar en las acciones que se lleven a cabo.

Ante la existencia de un accidente, la Secretaría de Infraestructura, Comunicaciones y Transportes, a través de la Comisión Investigadora y Dictaminadora de Accidentes, investigara dicho acontecimiento, esto mediante el ejercicio de atribuciones tales como la prevista en el artículo 81 Bis, fracciones III y VII, del ordenamiento en estudio, en la que se prevé que dicha instancia puede:

- Exigir la protección y preservación de los registros y documentos relacionados con el suceso, y
- Obtener todo tipo de evidencia y copias de cualquier documento relevante relativo al accidente o incidente, a las personas, empresas y equipos relacionados con el mismo, en particular, la formación y calificación de las personas, que hayan participado en el mantenimiento, despacho, servicio de control y seguimiento del vuelo, construcción o diseño, tripulación, control de la(s) aeronave(s) implicadas, así como demás información que el investigador considere relevante.

En el presente caso, se advierte que el AIFA pretende identificar a las personas mediante el registro biométrico de sus rasgos faciales, así como los datos obtenidos y existentes en el pasaporte electrónico.

También resulta oportuno considerar, respecto de los restantes datos personales que son materia de tratamiento al estar contenidos en el pasaporte electrónico, físico o la credencial para votar emitida por el Instituto Nacional Electoral, que el tratamiento de datos personales relacionados con la prestación de ese servicio complementario no implica que todos los datos personales existentes en tales documentos deban ser tratados para fines del tráfico de pasajeros.

Al respecto, es oportuno traer a colación lo señalado por la Suprema Corte de Justicia de la Nación respecto a la acción de inconstitucionalidad 82/2021 y su acumulada 86/2021 en la que se resolvió lo siguiente:

> ***"Décimo.*** *Los numerales 15, fracción XLII bis, 180 Ter, fracción VI, 180 Quáter, 180 Quintus, 180 Séptimus, último párrafo impugnados, violan las garantías de seguridad y legalidad jurídicas en relación con las técnicas de investigación contenidas en el artículo 16 constitucional, puesto que permiten acceder a datos biométricos sin control judicial.*
> *En términos del artículo 16 constitucional y 252 del Código Nacional de Procedimientos Penales, el requerimiento de datos biométricos exige que un Juez de control lo autorice, previa solicitud del Ministerio Público. No obstante, el artículo 180 Séptimus, último párrafo impugnado no alude a la necesidad de obtener ese control judicial para acceder a los datos biométricos contenidos en el PANAUT, sino que solo establece que, si las autoridades conforme a las leyes cuentan con facultades para requerir al IFT, podrán acceder al padrón, sin aclarar si será suficiente con que las leyes las autoricen en términos genéricos, o si se requerirá, además una orden judicial. Por ende, se transgrede el principio de seguridad jurídica y la legalidad en relación con las técnicas de investigación.*
> *Adicionalmente, no existe certeza sobre el número de personas que podrán acceder al padrón, no se define cómo será el acceso a los datos biométricos y a los restantes datos personales, si podrá accederse a todo el padrón o a los datos de solo una persona, ni los requisitos que deben contener los requerimientos de acceso a la información del Padrón cuando debiera exigirse demostrar que la persona respecto de la cual se solicita la información es sujeto de investigación por el delito de extorsión.*
> *Al respecto se recuerda que al resolver los casos C-293/12 y C-594/1, el Tribunal de Justicia de la Unión Europea declaró la invalidez de la Directiva 2006/24/CE, por no prever ningún criterio objetivo que permitiera limitar el número de personas que disponían de la autorización de acceso a los datos conservados ni garantías suficientes, que permitieran asegurar una protección eficaz de esos datos.*

Una vez establecido lo anterior, es oportuno considerar que para verificar la proporcionalidad en el tratamiento de datos personales debe corroborarse lo siguiente:

- **Que se persiga un fin válido.** Esta etapa del análisis presupone la idea de que no cualquier propósito puede justificar la limitación a un derecho fundamental, en este caso la protección de datos personales, pues los derechos fundamentales, ciertos bienes colectivos y bienes jurídicos garantizados como principios constitucionales, constituyen fines que legítimamente fundamentan la medida en el ejercicio de otros derechos.
- **Que la medida resulte idónea para satisfacer en alguna medida su propósito.** En esta etapa del escrutinio debe analizarse si la medida adoptada tiene, en términos fácticos, una relación de instrumentalidad con el fin, esto es, si es un medio apto para producir el fin perseguido. En este sentido, el examen de idoneidad presupone la existencia de una relación entre la intervención al derecho y el fin que persigue dicha afectación, siendo suficiente que la medida contribuya en algún modo y en algún grado a lograr el propósito que se busca.
- **Que la medida resulte necesaria.** El examen de necesidad implica corroborar en términos fácticos, en primer lugar, si existen otros medios igualmente idóneos para lograr los fines que se persiguen y, en segundo lugar, determinar si estas alternativas intervienen con menor intensidad el derecho fundamental afectado. Así, de encontrarse alguna medida alternativa que sea igualmente idónea para proteger el fin constitucional y que a su vez intervenga con menor intensidad al derecho, deberá concluirse que la medida elegida es desproporcional.
- **La proporcionalidad en estricto sentido.** Esta grada de la prueba consiste en efectuar un balance o ponderación entre dos principios que compiten en un caso concreto. Dicho análisis requiere centralmente una valoración, es decir, un juicio axiológico, que consiste en ponderar si la importancia constitucional de lograr el fin perseguido es congruente con la importancia de evitar el grado de afectación que se producirá al derecho fundamental. Este juicio valorativo tiene como trasfondo fáctico, naturalmente, el grado de seguridad fáctica respecto de que se logrará ese fin y se producirá esa afectación, respectivamente. En este sentido, mientras más importante sea evitar afectar un derecho fundamental, más importancia debe tener la realización del fin perseguido por el legislador, y más relevancia cobra la certeza de que ese fin se producirá afectando en esa medida el derecho fundamental.

Establecido lo previo, y en el caso concreto, dicho análisis se efectúa de la siguiente manera:

- **El fin válido y la existencia del PDE.** En el presente caso, el AIFA tiene a su cargo la concesión del Aeropuerto Internacional Felipe Ángeles, sin embargo, el realizar la captura y resguardo de datos biométricos, de forma conjunta con los datos personales existentes en el pasaporte electrónico, sin aplicar sobre estos últimos un criterio de minimización, resulta desproporcional, pues para realizar el tratamiento de datos personales en los términos planteados, no resulta necesaria el recabo de un número considerable de datos personales, lo anterior considerando que para lograr la identificación de las personas para efectos de la facilitación del uso de las instalaciones -preseguridad y abordaje-, así como la eventual cooperación con la justicia y la prevención del delito, no resulta necesario contar con la

totalidad de datos existentes en el pasaporte electrónico, solamente con aquellos que permita la individualización de aquellos necesarios para lograr asociarlos con el vector recabado.

Sin embargo, este Instituto observa que las medidas sin contacto dependen de que pueda identificarse a la persona que se ostenta como tal, por lo que el uso de datos biométricos tiene una relación estrecha con dichos medios, ya que permite conocer que la persona que se afirma ser lo es; sin embargo, ello no implica recabar otros datos adicionales que sean excesivos frente a la identificación de la persona.

- **La idoneidad del establecimiento de PDE en el marco del Sistema de Procesamiento:** En ese sentido, el recabo y resguardo posterior de datos biométricos de forma conjunta con aquellos existentes en el pasaporte electrónico, pues si bien en principio AIFA precisa que ello facilita el abordaje , lo cierto es que al existir otras finalidades previstas por OACI y que, como se abordó en el principio de licitud, no fueron contempladas por AIFA **resultan en una disparidad que afecta la esfera íntima, pues el AIFA tendría el acceso a la totalidad de esos datos personales sin tener claramente definidos los límites de esa actuación**, verificando aquellos datos personales que sean indispensables para lograr la identificación para los fines que persigue el PDE, congruente con la legislación aplicable.
- **La necesidad del PDE en el Sistema de Procesamiento:** En ese sentido, si el fin del AIFA es identificar a las personas para la prestación del servicio complementario de tráfico de pasajeros, **sin embargo, se advierte que debió valorarse, previo al diseño del sistema, cuales datos personales eran necesarios para ese fin, y a su vez que esos fines fueran acordes tanto a lo establecido por OACI y los principios y deberes de la materia**.
- **La proporcionalidad en sentido estricto del PDE.** Finalmente, AIFA aludió que su plataforma tecnológica serviría para la facilitación del uso de instalaciones aeroportuarias, específicamente las relacionadas con preseguridad y abordaje, el recabar y dar tratamiento a datos biométricos con otros datos que no resultan indispensables y sin contar con los fines claros de acuerdo con la legislación en materia de aviación, afecta ese derecho, pues la identidad una vez registrada en algún medio físico o electrónico puede afectar a las personas en su esfera más íntima, en tanto las somete a la incertidumbre sobre el destino y fines de esa información.

En ese sentido, si bien este Instituto advierte que los medios sin contacto requieren el establecimiento de medios de identificación diversos a los visuales o de acercamiento con otras personas, y la utilización de datos biométricos puede ayudar con ello, esa circunstancia no implica que deban recabarse datos más allá de aquellos necesarios que permitan la identificación de la persona.

Mismas consideraciones que deben contemplarse para aquellos casos en los que se utilice el pasaporte físico o la credencial para votar expedida por el INE, ya que el recabo y tratamiento de la totalidad de los datos contenidos en dichos documentos no son necesarios para dicha finalidad. Aunado a que, para dichos casos, debe establecer medios para corroborar la identidad, como es el caso del servicio de verificación que pone a disposición el INE, lo cual en caso de optarse deberá valorarse el cumplimiento de los principios y deberes establecidos en la Ley General.

Ahora bien, sobre los datos relacionados con el pase de abordar, si bien en principio el AIFA no los identificó como datos personales, lo cierto es que en su conjunto hacen identificable a las personas, por lo que al igual que en los datos relacionados con el pasaporte, se advierte que resulta desproporcional su recabo, considerando que estos sirven para comunicar, en la línea de abordaje, quienes ya han abordado su vuelo, de ahí que sea innecesario contar con la totalidad de esos datos.

Finalmente, y con independencia de las consideraciones que para tales efectos se encuentren en el principio de calidad, este Instituto advierte que el periodo de conservación de 24 horas posteriores al inicio del vuelo es desproporcional, en tanto que limita injustificadamente a los titulares de datos personales para el ejercicio de sus derechos ARCO, así como las actividades de investigación de las autoridades competentes sobre incidentes, accidentes y delitos. Esto último no es opcional, existen normas que regulan ese deber que no corresponde al AIFA limitar.

Tampoco precisan lo relacionado con los momentos de conservación antes del abordaje, pues dada la facilidad de hacerlo mediante la aplicación móvil, ello implica periodos de conservación que son indeterminados, por lo que ello debe ser definido por el AIFA, ya que no se advirtió alguna previsión al respecto.

En ese sentido, y en atención a la justificación aludida por el responsable, este Instituto advierte que es desproporcional el número de datos recabados para el Sistema de Procesamiento, pues si bien todos esos datos se toman de las identificaciones exhibidas por el usuario, ello no implica que deban tomarse la totalidad de datos en ellas y se deban utilizar en completitud para ello.

Recomendaciones en torno al principio de proporcionalidad

Clave	Recomendación
AIFA_PRO_001	Se sugiere valorar, conforme al criterio de minimización, la pertinencia de utilizar los datos personales existentes en el pasaporte físico, electrónico y credencial para votar o aquellos documentos que pueden utilizarse en razón de que la finalidad principal del Sistema de Procesamiento es permitir el flujo

	ininterrumpido para el acceso de los pasajeros para pasar a los filtros de pre-seguridad y realizar el embarque a la aeronave de manera rápida y segura.
AIFA_PRO_002	Se sugiere establecer, en el aviso de privacidad, aquellos datos personales que serán recabados en función al medio utilizado para tales efectos, tomando en consideración lo señalado en el principio de proporcionalidad.
AIFA_PRO_003	Se sugiere valorar la eliminación del nombre del vendedor en la información que se recaba en Quioscos de autoservicio (CUSS) y Mostradores de documentación CUPPS-Vdesk, y en su almacenamiento.
AIFA_PRO_004	Se sugiere valorar, en el caso del PDE, su construcción con el menor uso de datos personales posibles de los titulares.
AIFA_PRO_005	Se sugiere valorar los periodos de conservación del PDE considerando que el Aeropuerto Internacional Felipe Ángeles es considerado una instalación estratégica, así como los periodos con los que cuentan las autoridades para la investigación de incidentes, accidentes y delitos; los cuales superan las 24 horas.
AIFA_PRO_006	Se sugiere valorar el PDE únicamente en función a la función de identificación de las personas para facilitar su abordaje, pues tiene implicaciones en materia de seguridad nacional que deben ser considerados como parte de su construcción, uso y conservación.

1.7. Principio de información

Los artículos 3, fracción II, 26, 27 y 28 de la Ley General, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43 y 44 de los Lineamientos generales, de los cuales se advierte que el responsable está obligado a informar al titular sobre la existencia y características principales del tratamiento al que serán sometidos sus datos personales, a través del aviso de privacidad, a fin de que pueda tomar decisiones informadas al respecto. El aviso de privacidad se pondrá a disposición del titular en sus dos modalidades simplificado e integral.

El aviso de privacidad simplificado debe señalar la siguiente información:

- La denominación completa del responsable.
- Las finalidades o usos que motivan el tratamiento de los datos personales, distinguiendo aquéllas que requieran del consentimiento del titular.

- Las transferencias de datos personales que, en su caso, se tengan previstas realizar y que requieran del consentimiento del titular.
- El sitio o medio donde el titular podrá consultar el aviso de privacidad integral.

Por su parte, el aviso de privacidad integral, además de señalar la información prevista en el aviso de privacidad simplificado, debe informar lo siguiente:

- El domicilio del responsable.
- Los datos personales que serán sometidos a tratamiento, identificando aquéllos que sean sensibles.
- El fundamento legal que faculta al sujeto obligado para llevar a cabo el tratamiento de los datos personales.
- Los mecanismos, medios y procedimientos disponibles para que los titulares puedan ejercer sus derechos ARCO.
- El domicilio de la Unidad de Transparencia del responsable.
- Las transferencias, nacionales y/o internacionales, de datos personales que, en su caso, efectúe y que no requieran de su consentimiento.
- Los medios a través de los cuales el responsable comunicará a los titulares los cambios al aviso de privacidad.

De manera adicional a los elementos señalados, el aviso de privacidad, de manera opcional, puede contener los siguientes elementos:

- Abreviatura o acrónimo por el cual se identifica al responsable (aviso de privacidad simplificado e integral).
- Datos de contacto del responsable (aviso de privacidad integral).
- Medios y/o fuentes de obtención de los datos personales (aviso de privacidad integral).
- Las transferencias, nacionales y/o internacionales, de datos personales que, en su caso, efectúe y que no requieran de su consentimiento (aviso de privacidad integral).
- La posibilidad que tiene el titular de ejercer su derecho a la portabilidad en el caso que sea posible (aviso de privacidad integral).

El aviso de privacidad debe caracterizarse por ser sencillo, con la información necesaria, expresado en lenguaje claro y comprensible y con una estructura y diseño que facilite su entendimiento, atendiendo al perfil de los titulares a quien irá dirigido, con la finalidad de que sea un mecanismo de información práctico y eficiente.

El responsable está obligado a poner a disposición del titular el aviso de privacidad simplificado en un primer momento, lo cual no le impide que pueda dar a conocer el aviso de privacidad integral desde un inicio, conforme a las siguientes reglas:

- De manera previa a la obtención de los datos personales cuando los mismos se obtengan directamente del titular, independientemente de los formatos o medios físicos y/o electrónicos utilizados para tal fin, o
- Al primer contacto con el titular o previo al aprovechamiento de los datos personales cuando éstos se hubieren obtenido de manera indirecta del titular.

El responsable debe publicar de manera permanente el aviso de privacidad integral, en el sitio o medio que se informe en el aviso de privacidad simplificado, a efecto de que el titular tenga la posibilidad de consultarlo en cualquier momento.

Asimismo, el responsable está obligado a difundir, poner a disposición o reproducir el aviso de privacidad, independientemente de la modalidad, en formatos físicos y electrónicos, ópticos, sonoros, visuales o a través de cualquier otra tecnología que permita su eficaz comunicación.

Cabe destacar, que el responsable tiene la obligación de poner a disposición del titular, un nuevo aviso de privacidad, en sus dos modalidades, cuando:

- Cambie su identidad.
- Requiera recabar datos personales sensibles adicionales a aquéllos informados en el aviso de privacidad original, los cuales no se obtengan de manera directa del titular y se requiera de su consentimiento para el tratamiento de éstos.
- Cambie las finalidades señaladas en el aviso de privacidad original.
- Modifique las condiciones de las transferencias de datos personales o se pretendan realizar transferencias no previstas inicialmente y el consentimiento del titular sea necesario.

Al respecto, como parte de los anexos presentadas en conjunto con la evaluación de impacto presentada por el AIFA, se remitió el Anexo 11 que contiene tres avisos de privacidad integrales y simplificados, relativos al tratamiento de datos personales llevado a cabo mediante el CUPPS, la aplicación móvil y el CUSS.

Por su parte, en el desahogo de requerimiento de información adicional, se especificó lo siguiente, con relación al cumplimiento de este principio: *"En la página web será publicado el procedimiento de enrolamiento para conocimiento de los particulares, como un ejercicio del principio de información.*

Ahora bien, es importante señalar que para la materialización del principio de información se requiere del análisis en función de los siguientes elementos:

- La redacción del aviso de privacidad.
- El establecimiento y desarrollo de los elementos informativos conforme a lo dispuesto en la Ley General y los Lineamientos generales.
- La puesta a disposición del aviso de privacidad.
- Los medios de difusión del aviso de privacidad.

En este sentido a continuación se emitirán algunos hallazgos y consideraciones advertidas de manera particular en cada uno de los tres elementos del Sistema, esto es, mostrador convencional CUPPS-VDesk, aplicación móvil y quiosco de autoservicio - CUSS.

Mostrador convencional CUPPS-VDesk

Por lo que hace al establecimiento y desarrollo de los elementos informativos y la redacción, se advirtió lo siguiente respecto a los avisos de privacidad integral y simplificado del CUPPS-VDesk:

1. No se identifican que en el listado de los datos personales del aviso de privacidad sean acordes con los datos que se informan en la evaluación de impacto serán tratados, por ejemplo, no se incluye la fotografía que se tomará a los usuarios, con la que se hará al prueba de vida y el template biométrico, de igual forma se advierte que falta la inclusión del "país de nacimiento" "país de nacionalidad" que viene establecido en el documento Anexo 2 Experiencia sin contacto. De igual forma, se indica que uno de los datos será la biometría facial, término que no es claro si se refiere al template biométrico que se genera.
2. De igual forma, es preciso indicar que, en el documento, Experiencia sin contacto con tecnología biométrica, se advierte que, como parte de la validación de los documentos de identidad (pasaporte electrónico, no electrónico y credencial de elector), se observa que pudiera realizarse una captura de la "Foto del chip del pasaporte" y la "imagen del pasaporte" el cual no se visualiza en el listado de datos personales del aviso de privacidad.
3. Si bien se indica a la nacionalidad, género y biometría facial como datos personales sensibles a tratar, es importante señalar que, en el Anexo 2 Experiencia sin contacto se indica que la imagen del pasaporte (incluida la imagen del pasajero) y el número de pasaporte deben considerarse categorías sensibles de datos personales éste último por tratarse de un número personal único.
4. Si bien se indica como única finalidad el "Realizar el registro biométrico, en sitio y asistido por un agente, en los mostradores convencionales de documentación (Check-in), con la finalidad de permitir el proceso de flujo ininterrumpido para el acceso de los pasajeros a salas de última espera. Realizando la validación de existencia y coincidencia entre los registros biométricos", se considera conveniente revisar lo dispuesto en el análisis realizado en el principio de finalidad ya que el proceso en el mostrador responde a más de una finalidad.
5. Se advierte como transferencia la comunicación de datos que se realiza a Vision Box (Orchestra) en el Data Center, sin embargo, del análisis realizado en el apartado de

transferencias, se advierte que tal comunicación no corresponde propiamente a una transferencia puesto que dicho intercambio de datos se realiza entre diferentes sistemas que si bien, son gestionados por diferentes empresas, éstas fungen como encargados del AIFA y por lo tanto la comunicación que se realiza entre dichos desarrollos tecnológicos como lo es Visión Box constituyen una remisión de datos personales y no una transferencia.

6. En este sentido, es importante advertir que, en el caso de la evaluación de impacto, se documentó que las transferencias que se pretendían realizar referían a la comunicación que se realiza de los datos personales de los pases de abordar a las aerolíneas, situación que no se ve reflejado en el aviso de privacidad.
7. En el aviso de privacidad integral y simplificado, si bien se indicó que la transferencia de datos personales que se realiza a Vision Box (Orchestra) en el Data Center es una transferencia que requiere el consentimiento por lo que el titular puede externar su negativa no se observan los mecanismos y medios disponibles para que el titular, en su caso, pueda manifestar su negativa para el tratamiento de sus datos personales.
8. En el aviso de privacidad integral no se informa el sitio, lugar o mecanismo donde se podrá consultar el aviso de privacidad integral.
9. En el fundamento legal no se precisa su fecha de publicación o, en su caso, de la última reforma o modificación.
10. En el aviso de privacidad integral no se identifica el elemento que informe sobre los mecanismos y medios habilitados para atender las solicitudes para el ejercicio de los derechos ARCO y para el de portabilidad, ni el procedimiento o medios para atenderlas.
11. No se advierte la inclusión del domicilio completo de la unidad de transparencia, su número y extensión telefónica.
12. Por lo anterior, se observó que ambos avisos de privacidad no contienen información necesaria para informar a los titulares sobre todos los elementos necesarios para conocer sobre el tratamiento al que se someterán sus datos personales.

Aplicación móvil

1. No se identifican que en el listado de los datos personales del aviso de privacidad sean acordes con los datos que se informan en la evaluación de impacto serán tratados, en este caso, no se indica el template biométrico del rostro.
2. Al igual que en el caso anterior, si bien se indica a la foto obtenida del chip del pasaporte, nacionalidad, género y la foto capturada por el dispositivo móvil, en el Anexo 2 Experiencia sin contacto se indica que la imagen del pasaporte (incluida la imagen del pasajero) y el número de pasaporte deben considerarse categorías sensibles de datos personales éste último por tratarse de un número personal único.
3. Como se indicó en el aviso de privacidad anterior, se informa como única finalidad "realizar la validación del pasajero, permitiendo identificar al pasajero por los puntos de validación desde

el ingreso a salas de última espera, hasta el abordaje a la aeronave", se considera conveniente revisar lo dispuesto en el análisis realizado en el principio de finalidad ya que el proceso en el mostrador responde a más de una finalidad.

4. Se reitera la consideración anterior sobre la transferencia de datos personales y los medios para la manifestación de la negativa del consentimiento.
5. Se reiteran las consideraciones antes señaladas en los numerales 8-12.

Quiosco de autoservicio - CUSS.

1. Se reiteran las consideraciones anteriores.

Ahora bien, como regla general, se requerirá un aviso de privacidad por tratamiento, ssólo en los casos en que la información a incluir en el aviso de privacidad de distintos tratamientos sea la misma en su mayoría, se podrá redactar un aviso de privacidad común. El criterio para este supuesto es que la redacción del aviso de privacidad compartido no sea confusa.

Al respecto, es importante aclarar que los tratamientos refieren a un proceso en lo general, por ejemplo, un tratamiento es la obtención, uso y eliminación de datos personales en la atención de solicitudes de derechos ARCO, mientras que otro distinto es la obtención, uso y eliminación de datos personales para la integración del expediente laboral de los servidores públicos.

Por su parte, las finalidades son acciones específicas que ocurren dentro del tratamiento. Por ejemplo, una finalidad en el tratamiento de la atención de solicitudes de derechos ARCO sería identificar al titular, o realizar las notificaciones que exige la ley.

Con respecto a lo antes expuesto, se considera que, dado lo analizado en el principio de finalidad, el uso y operación mediante el CUPPS, la aplicación móvil y el CUSS atienden a las mismas finalidades, por lo que se considera conveniente valorar la realización de un solo aviso de privacidad.

Derivado de lo anterior, se realizan las recomendaciones siguientes:

Recomendaciones en torno al principio de información

Clave	Recomendaciones
AIFA_INF_001	Se recomienda valorar la posibilidad de homologar el contenido de todos los avisos de privacidad que nos fueron remitidos como parte de la evaluación de impacto, a efecto de elaborar uno solo respecto al proceso general de procesamiento del flujo de salida nacional e internacional.

AIFA_INF_002	Se recomienda, a manera de mejora práctica, incluir en los avisos de privacidad integrales, o en su caso, el aviso de privacidad integral homologado, los medios y/o fuentes a través de los cuales se obtienen los datos personales, y asociar el dato personal con cada una de las fuentes.
AIFA_INF_003	Se recomienda verificar que el fundamento establecido en los avisos de privacidad integrales, o en su caso, el aviso de privacidad integral homologado contemple lo establecido en las consideraciones manifiestas por este Instituto en el apartado del principio de licitud del presente documento.
AIFA_INF_004	Se recomienda que en el fundamento legal que se señala en los avisos de privacidad integrales o en su caso, el aviso de privacidad integral homologado se precise su fecha de publicación o, en su caso, de la última reforma o modificación.
AIFA_INF_005	Se recomienda verificar que, en la redacción de los avisos de privacidad integrales, o en su caso, el aviso de privacidad integral homologado se redacte claramente la relación de los documentos de los cuales se obtendrán los datos personales.
AIFA_INF_006	Se recomienda verificar e incluir la fotografía (sefie), país de nacimiento" "país de nacionalidad", "foto del chip del pasaporte" y la "imagen del pasaporte" en el listado de datos personales respecto del proceso en el Mostrador convencional CUPPS-VDesk;
AIFA_INF_007	Se recomienda redactar clara y correctamente los términos que se emplean en los avisos de privacidad, sin usar palabras ambiguas como pudiera ser "biometría facial".
AIFA_INF_008	Se recomienda revisar la inclusión en los avisos de privacidad integrales o en su caso, el aviso de privacidad integral homologado los datos referentes a la imagen del pasaporte (incluida la imagen del pasajero) y el número de pasaporte como datos personales sensibles en función de lo manifestado en el Anexo 2 Experiencia sin contacto.
AIFA_INF_009	Se considera conveniente revisar lo dispuesto en el análisis realizado en el principio de finalidad respecto a las finalidades que persigue la implementación del Sistema a efecto de poder reflejarlo en los avisos de privacidad integrales y simplificados o en su caso, el aviso de privacidad integral y simplificado homologados.
AIFA_INF_010	Se considera conveniente revisar lo dispuesto en el análisis realizado en el apartado de transferencias a efecto de reflejar las transferencias que son efectuadas en los correspondientes avisos de privacidad.

AIFA_INF_011	Se recomienda establecer los mecanismos y medios disponibles para que el titular, en su caso, pueda manifestar su negativa para el tratamiento de sus datos personales para finalidades y transferencias de datos personales que requieren el consentimiento del titular.
AIFA_INF_012	Se recomienda que en los avisos de privacidad simplificados o en su caso, el aviso de privacidad simplificado homologado se informe el sitio, lugar o mecanismo donde se podrá consultar el aviso de privacidad integral.
AIFA_INF_013	Se recomienda que en los avisos de privacidad integrales o en su caso, el aviso de privacidad integral homologado se informen los mecanismos y medios habilitados para atender las solicitudes para el ejercicio de los derechos ARCO y para el de portabilidad, ni el procedimiento o medios para atenderlas.
AIFA_INF_014	Se recomienda que en los avisos de privacidad integrales o en su caso, el aviso de privacidad integral homologado se informe el domicilio completo de la unidad de transparencia, su número y extensión telefónica.

1.8. Principio de responsabilidad

Los artículos 29 y 30 de la Ley General, 46, 47, 48, 49, 50, 51 y 52 de los Lineamientos generales, de los que se desprende que el responsable está obligado a implementar mecanismos que permitan acreditar el cumplimiento de los principios, deberes y demás obligaciones establecidas en la Ley General como son, de manera enunciativa más no limitativa, las siguientes:

- Elaborar políticas y programas de protección de datos personales obligatorios y exigibles al interior del sujeto obligado.
- Establecer un sistema de supervisión y vigilancia interna y/o externa para comprobar el cumplimiento de las políticas de protección de datos personales.
- Diseñar, desarrollar e implementar políticas públicas, programas, servicios o sistemas de conformidad con las disposiciones previstas en la Ley General.
- Garantizar que las políticas públicas, programas, servicios o sistemas cumplan por defecto con las obligaciones previstas en la Ley General.

Sobre el particular, el AIFA manifestó lo siguiente en la Evaluación de impacto:

"7. Política
Se han establecido Políticas Internas de la Subdirección de Sistemas y para el Sistema de Procesamiento de Pasajeros.
Actualmente no existe un presupuesto en específico asignado para este fin"

Bajo esta consonancia, en el Anexo 17 a la Evaluación de impacto presentada, se señalan los Términos y condiciones siguientes:

"Esta política de condiciones de uso es válida a partir del Nov 2022.
TÉRMINOS Y CONDICIONES — AEROPUERTO INTERNACIONAL "FELIPE ÁNGELES"
AEROPUERTO INTERNACIONAL "FELIPE ÁNGELES", persona jurídica de derecho privado describe, a través de este documento, las normas de uso del sitio https://aifa.aero y de cualquier otro sitio web, tienda o aplicación operada por el titular.
Al navegar por este sitio web, consideramos que está de acuerdo con las condiciones de uso que figuran a continuación.
Si no está de acuerdo con los términos de este acuerdo, le pedimos que no haga ningún otro uso de este sitio web, mucho menos que se registre o envíe sus datos personales.
Si cambiamos nuestras condiciones de uso, publicaremos el nuevo texto en este sitio web, con una fecha de revisión actualizada. Podemos modificar este documento en cualquier momento.
Si hay un cambio significativo en los términos de este acuerdo, podemos informarle utilizando la información de contacto que tenemos en nuestra base de datos o mediante una notificación.
El uso de este sitio web después de los cambios significa que usted acepta las condiciones de uso revisadas. Si, después de leer la versión revisada, no está de acuerdo con sus términos, por favor, termine su acceso.

- *Sección 1 - Usuario*

El uso de este sitio web le otorga automáticamente la condición de Usuario e implica su plena aceptación de todas las directrices y condiciones incluidas en estas Condiciones.

- *Sección 2 - Adhesión junto con la política de privacidad*

El uso de este sitio web implica la adhesión a estas Condiciones de Uso y a la versión más actualizada de la Política de Privacidad del AEROPUERTO INTERNACIONAL "FELIPE ÁNGELES".

- *Sección 3 - Condiciones de acceso*

En general, el acceso al sitio web del AEROPUERTO INTERNACIONAL "FELIPE ÁNGELES" es gratuito y no requiere registro previo.
Sin embargo, para hacer uso de algunas funcionalidades, el usuario ***puede necesitar registrarse****, creando una cuenta de usuario con un nombre de usuario y una contraseña de acceso.*
Es responsabilidad del usuario proporcionar únicamente información correcta, auténtica, válida, completa y actualizada, así como no revelar su nombre de usuario y contraseña a terceros.
Algunas partes de este sitio web ofrecen al usuario la opción de publicar comentarios en determinadas áreas. El AEROPUERTO INTERNACIONAL "FELIPE ÁNGELES" no consiente la publicación de contenidos de carácter discriminatorio, ofensivo o ilícito, o que infrinjan los derechos de autor o cualquier otro derecho de terceros.
La publicación de cualquier contenido por parte del usuario de este sitio web, incluidos los mensajes y comentarios, implica una licencia no exclusiva, irrevocable e irreversible para su

uso, reproducción y publicación por parte del AEROPUERTO INTERNACIONAL "FELIPE ÁNGELES" en su sitio web, plataformas de internet y aplicaciones, o incluso en otras plataformas, sin ninguna restricción o limitación.

- *Sección 4 - Cookies*

La información sobre el uso que usted hace de este sitio web puede recogerse a través de las cookies. Las cookies son piezas de información que se almacenan directamente en el equipo que está utilizando. Las cookies permiten recoger información como el tipo de navegador, el tiempo de permanencia en el sitio web, las páginas visitadas, las preferencias de idioma y otros datos de tráfico anónimos. Nosotros y nuestros proveedores de servicios utilizamos la información para la protección de la seguridad, para facilitar la navegación, mostrar la información de manera más eficiente y personalizar su experiencia al utilizar este sitio web, así como para el seguimiento en línea. También recopilamos información estadística sobre el uso del sitio web para mejorar continuamente nuestro diseño y funcionalidad, para entender cómo se utiliza el sitio web y para ayudarle a resolver problemas relevantes.

Si no desea que se recoja su información a través de las cookies, existe un procedimiento sencillo en la mayoría de los navegadores que permite rechazar automáticamente las cookies, o le da la opción de aceptar o rechazar la transferencia de una cookie específica (o varias) de un sitio web concreto a su ordenador. Sin embargo, esto puede crear inconvenientes en su uso del sitio web.

La configuración que elija puede afectar a su experiencia de navegación y al funcionamiento que requiere el uso de cookies. En este sentido, rechazamos cualquier responsabilidad por las consecuencias derivadas del funcionamiento limitado de este sitio web causado por la desactivación de las cookies en su dispositivo (incapacidad para establecer o leer una cookie).

- *Sección 5 - Propiedad intelectual*

Todos los elementos del AEROPUERTO INTERNACIONAL "FELIPE ÁNGELES" son propiedad intelectual de la misma o de sus licenciantes. Estos términos o el uso del sitio web no le otorgan ninguna licencia o derecho de uso de los derechos de propiedad intelectual del AEROPUERTO INTERNACIONAL "FELIPE ÁNGELES" o de cualquier tercero.

- *Sección 6 - Enlaces a sitios web de terceros*

Este sitio web puede contener enlaces de hipertexto que le redirigirán a sitios web de diferentes índoles. Si hace clic en uno de estos enlaces a cualquiera de estos sitios, recuerde que cada sitio tiene sus propias prácticas de privacidad y que nosotros no somos responsables de estas políticas. Por favor, consulte esas políticas antes de enviar cualquier dato personal a esos sitios.

No somos responsables de las políticas y prácticas de recopilación, uso y divulgación (incluidas las prácticas de protección de datos) de otras organizaciones, como Facebook, Apple, Google, Microsoft, o cualquier otro desarrollador de software o proveedor de aplicaciones, tienda de medios sociales, sistema operativo, proveedor de servicios de internet o fabricante de dispositivos, incluidos los Datos Personales que usted divulgue a otras organizaciones a través de las aplicaciones, en relación con dichas aplicaciones, o publicados

en nuestras redes sociales. Le recomendamos que se informe sobre la política de privacidad y las condiciones de uso de cada sitio web visitado o proveedor de servicios utilizado.

- *Sección 7 - Plazos y modificaciones*

El funcionamiento de este sitio web es por tiempo indefinido.

La totalidad del sitio web o cada una de sus secciones podrá ser cerrada, suspendida o interrumpida unilateralmente por el AEROPUERTO INTERNACIONAL "FELIPE ÁNGELES", en cualquier momento y sin previo aviso.

- *Sección 8 - Datos personales*

Durante el uso de este sitio web, ciertos datos personales serán recogidos y procesados por el AEROPUERTO INTERNACIONAL "FELIPE ÁNGELES" y/o los Socios. Las normas relativas al tratamiento de los datos personales del AEROPUERTO INTERNACIONAL "FELIPE ÁNGELES" están estipuladas en el Aviso de Privacidad.

Por su parte, en el desahogo del requerimiento de información adicional, se refirió lo siguiente con relación al cumplimiento de este principio:

"En los artículos 29 y 30 de la ley general de datos, referentes al principio de responsabilidad se solicita señalar las políticas internas y programas de gestión y tratamiento de protección de datos personales implementados y el presupuesto asignado para tal fin; la última revisión de los mismos y en su caso las modificaciones que se han realizado con motivo de la implementación del "sistema de procesamiento de pasajeros", incluyendo los procedimientos para recibir y responder dudas y quejas de los titulares, y los mecanismos o procedimientos relativos a la privacidad por diseño y defecto; todos los documentos deben ser remitidos en su versión íntegra, que si bien, se señala de manera expresa que se cuenta con estas políticas internas dentro de la subdirección de sistemas, no se remite al documento ni a la demás información aquí descrita y requerida.

Además de contar con las políticas internas y programas de gestión del AIFA, se encuentran disponibles en el apartado virtual https://mediaaifa.s3.us-east-2.amazonaws.com/1.2.2-Politica-de-Proteccion-de-Datosdel-AIFA-OCR.pdf

Se da cumplimiento a los mecanismos o procedimientos relativos a la privacidad por diseño y defecto con la documentación de la EIPDP en el anexo 3 "Documentación y certificación privacidad por diseño". (Anexo 9)

Las políticas internas del Sistema de Procesamiento de Pasajeros y la política de protección de datos de esta Subdirección se encuentran dentro del Documento de seguridad remitido el 9 de enero, al cual correspondió Anexo 16; no obstante, se reenvían nuevamente para su pronta referencia. (Anexo 6) para ello adicionalmente a lo anterior, se solicita remitir las documentales que permitan demostrar los mecanismos que ha adoptado el responsable para cumplir con el principio de responsabilidad y en ese sentido, demostrar el cumplimiento de las disposiciones aplicables en materia de protección de datos personales, tales como pueden ser: o La destinación de recursos autorizados para la instrumentación de programas y políticas de protección de datos personales; En el presente ejercicio fiscal no se tienen contemplados recursos específicos para capacitación ni para instrumentación de programas y Políticas De Protección De Datos Personales. o Las políticas y programas de protección de datos

personales, cuál obligatorios y exigibles al interior de la organización del responsable; Se da cumplimiento al principio de responsabilidad en el apartado virtual de protección de datos personales del AIFA https://vuelaaifa.mx/informacion-relevante-en-materia-deproteccion-de-datos-personales/ Asimismo, a continuación encontrará el vínculo electrónico que lo remite al el Acta de cuarta sesión Ordinaria del Comité de Transparencia, del año 2022. https://media-aifa.s3.us-east-2.amazonaws.com/Acta-4-SO.pdf o Los sistemas de supervisión y vigilancia interna y/o externa, incluyendo auditorías, para comprobar el cumplimiento de las políticas de protección de los datos personales; Los sistemas de supervisión y vigilancia interna y/o externa se dan a conocer en el apartado virtual https://vuelaaifa.mx/informacionrelevante-en-materia-de-proteccion-de-datos-personaies

Respecto a las fracciones I y II del artículo 30 de la Ley General en relación con el 47 de los Lineamientos Generales, se advierte que el responsable deberá elaborar e implementar políticas y programas de protección de datos personales que tengan por objeto establecer los elementos y actividades de dirección, operación y control de todos sus procesos que, en el ejercicio de sus funciones y atribuciones, impliquen un tratamiento de datos personales a efecto de proteger éstos de manera sistemática y continúa.

Al respecto, de forma específica, se señaló:

"7. Política Se han establecido Políticas Internas de la Subdirección de Sistemas y para el Sistema de Procesamiento de Pasajeros.
Actualmente no existe un presupuesto en específico asignado para este fin."
"En el presente ejercicio fiscal no se tienen contemplados recursos específicos para capacitación ni para instrumentación de programas y Políticas De Protección De Datos Personales"

Se advierte que actualmente no tiene para el ejercicio fiscal 2023 recursos específicos en materia de programas y políticas en materia de protección de datos personales, asimismo se advierte que en el "ACTA DE LA CUARTA SESIÓN ORDINARIA DEL COMITÉ DE TRANSPARENCIA" del AIFA de fecha 02 de junio de 2022, en su numeral CUARTO se aprobó:

"CUARTO. - Discusión, y en su caso, aprobación de la Política de Protección de Datos Personales, propuesta por la Unidad de Transparencia, en términos de lo dispuesto por el artículo 84, fracción I de La Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados."

De lo anterior, se advierte que el responsable aprobó el año pasado una política de Protección de Datos Personales, que, si bien no se tuvo alcance, se advierte que existe.

Por lo que hace a la fracción III del artículo 30 en relación con el 48 de los Lineamientos Generales, se establece que los responsables deben contar con un programa de capacitación y actualización

de los servidores públicos en materia de protección de datos personales de forma anual y que debe ser aprobado por el Comité de Transparencia.

Se advierte que se cuenta con el Programa de Capacitación a Servidores Públicos del Aeropuerto Internacional Felipe Ángeles aprobado mediante "ACTA DE LA PRIMER SESIÓN y ORDINARIA DEL COMITÉ DE TRANSPARENCIA" de fecha 18 de abril de 2022, en su numeral QUINTO que señala:

> *"QUINTO. - Discusión y en su caso aprobación de (i) programa de capacitación para el año 2022 del personal del AIFA propuesto por la Unidad de Transparencia, así como, (ii) el Programa de Capacitación para el personal de la Unidad de Transparencia."*

Asimismo, también se señaló:

> *"El plan de trabajo que propone la Subdirección a mi cargo tiene como eje medular la capacitación del personal de esta área, en este sentido, dentro del Programa de Capacitación aprobado por el Comité de Transparencia el pasado 12 de enero del año en curso, se propuso que el personal del AIFA, deberá tomar cursos específicos en materia de manejo de biométricos: (Anexo 9)"*

El artículo 30, fracciones IV y V de la Ley General, en relación el 49 de los Lineamientos generales en su artículo 49, se prevé que, por regla general, el responsable deberá revisar las políticas y programas de seguridad y el sistema de supervisión y vigilancia implementado, al menos, cada dos años, salvo que realice modificaciones sustanciales a los tratamientos de datos personales que lleve a cabo y, en consecuencia, amerite una actualización.

Referente a dicho punto se señaló en el desahogo del requerimiento de información adicional:

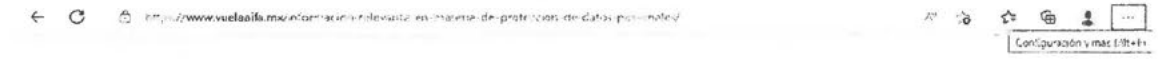
> *"[...]*
> *Se anexa documento de Análisis de Riesgos actualizado que cumple con el requerimiento solicitado en el Anexo 14*
> *Sobre las pruebas de calidad, vulnerabilidad y estrés, se detalla lo siguiente:*
> *A. Pruebas de calidad, se llevaron a cabo durante el mes de Julio 2022, donde se validó cada una de las funcionalidades de los diferentes equipos y sistemas, siendo completadas de manera satisfactoria. El detalle se incluye en el Anexo 13.*
> *B. Pruebas de vulnerabilidad, se llevaron a cabo durante el mes de diciembre 2022, donde se validó que el perímetro de seguridad lógica que protege la solución tecnológica cuenta con las medidas adecuadas de protección. El detalle se incluye en el Anexo 13.*
> *C. Pruebas de estrés, se cuenta con documentación y experiencia en otros aeropuertos, que muestran que el sistema cuenta con la solidez necesaria para atender un gran número de pasajeros y que serán procesados en menor tiempo respecto a la forma tradicional. Sin*

embargo, el AIFA validará el correcto dimensionamiento y capacidad para el procesamiento de pasajeros del sistema una vez que inicie su operación y sea utilizado de manera masiva.
[…]"
"[…]
Se anexa documento de Matriz Riesgos actualizado en versión digital que cumple con el requerimiento solicitado (Anexo 15)."

Asimismo, se señaló:

"Los sistemas de supervisión y vigilancia interna y/o externa, incluyendo auditorías, para comprobar el cumplimiento de las políticas de protección de los datos personales;
Los sistemas de supervisión y vigilancia interna y/o externa se dan a conocer en el apartado virtual:https://vuelaaifa.mx/información-relevante-en-materia-de-proteccion-de-datos-personales/"

Aclarando que al intentar ingresar a la liga aparece lo siguiente:



Error al establecer una conexión con la base de datos

Al respecto, a fin de poder distinguir el presente principio con elementos del deber se seguridad, se señala que en éste el responsable debe establecer un sistema de supervisión y vigilancia interna y/o externa para comprobar el cumplimiento del programa, incluyendo las medidas de seguridad, que prevea una revisión cada dos años o antes si es necesario por un cambio sustancial en el tratamiento.

Por lo que hace a la fracción VI del artículo 30 de la Ley General en relación con 50 de los Lineamientos General, se señala que el responsable debe determinar el procedimiento para recibir y responder dudas y quejas de los titulares en materia de protección de datos deberá ser de fácil acceso y con la mayor cobertura posible; considerando el perfil de los titulares y la forma en que se mantiene contacto o comunicación directa o cotidiana con ellos, así como estar, en todo momento, habilitado.

El AIFA señaló:

"El procedimiento para recibir y responder dudas y quejas de los titulares se encuentra en el apartado virtual https://vuelaaifa.mx/informacion-relevante-en-materia-de- Página 34 de 44

proteccion-de-datos-personales/ Variable 1.2: Mecanismos para acreditar el cumplimiento de principios, deberes y obligaciones de la Ley General y demás disposiciones aplicables, 1.2.5 Hipervínculo al documento en el cual el responsable establece el procedimiento para la recepción y respuesta de dudas, y quejas de los titulares en materia de protección de datos personales"

Tanto en el anexo número 9 del desahogo del requerimiento de información adicional, así como en la liga en cuestión, se advierte el documento denominado "PROCEDIMIENTO PARA LA RECEPCIÓN Y RESPUESTA DE DUDAS Y QUEJAS DE LOS TITULARES EN EL TRATAMIENTO Y EL MANEJO DE PROTECCIÓN DE DATOS PERSONALES." En el que se manifiesta de forma específica:

"A. Por correo electrónico, dirigido a la Unidad de Transparencia en transparencia@aifa.aero
B. Por escrito presentado físicamente en el módulo de atención de la Unidad de Transparencia instalados en la terminal, ubicada en Circuito Exterior Mexiquense Km. 33, Santa Lucía, Municipio de Zumpango, Estado de México. C.P. 55640.
C. El horario para la recepción de dudas y quejas referente al tratamiento de datos personales que se realicen por correo electrónico comprende de lunes a viernes de las 08:00hrs a 16:00 hrs."

Ahora bien, referente a la fracciones VII y VIII del artículo 30, de la Ley General, en relación con sus similares 51 y 52 de los Lineamientos Generales; se señala que el responsable debe cumplir e implementar acciones que prevean la privacidad por diseño y por defecto; en el que se consideren los avances tecnológicos, los costos de implementación, la naturaleza, el ámbito, el contexto y los fines del tratamiento de los datos personales, los riesgos de diversa probabilidad y gravedad que entraña éste para el derecho a la protección de datos personales de los titulares, así como otros factores que considere relevantes el responsable.

Asimismo, se precisa que respecto la cantidad de datos personales recabados y el alcance de tratamiento como del plazo de conservación se estará a lo señalada en el principio de calidad y proporcionalidad pues en este se advierte los datos personales recabados, los fines y se determinan si los datos son acordes y necesario a éstas, así como lo mencionado en el principio de finalidad.

Debido a lo anterior, se realizan las recomendaciones siguientes:

Recomendaciones en torno al principio de responsabilidad

Clave	Recomendación

AIFA_RE_001	Se recomienda en su caso actualizar los programas de datos y capacitación al año 2023 considerando en el primero los resultados obtenidos en el análisis de brecha y de riegos.
AIFA_RE_002	Se recomienda actualizar el Programa de capacitación en materia de protección de datos en el que se considere contar con la documentación que acredite la aplicación y actualización de capacitación en materia de protección de datos personales a los servidores públicos involucrados en el procedimiento;
AIFA_RE_003	Se sugiere incluir en el Programa General de Capacitación módulos de sensibilización sobre el uso e importancia de los datos biométricos.
AIFA_RE_004	Se recomienda establecer una periodicidad para la supervisión y vigilancia interna y/o externa del sistema, como pudiera ser cada dos años o antes si es necesario por un cambio sustancial en el tratamiento.
AIFA_RE_005	Sería deseable que en el procedimiento de dudas y quejas se consideren; las áreas administrativas responsables de las dudas, quejas y sugerencias; los plazos de respuesta y la información de contacto.
AIFA_RE_006	Se recomienda que el responsable implemente acciones que prevean la privacidad por diseño y por defecto; en el que se consideren los avances tecnológicos, los costos de implementación, la naturaleza, el ámbito, el contexto y los fines del tratamiento de los datos personales, los riesgos de diversa probabilidad y gravedad que entraña éste para los que puede considerar los resultados obtenidos en los análisis de riesgos y brecha, a fin de garantizar el derecho a la protección de datos personales de los titulares, así como otros factores que considere relevantes el responsable.

2. Deber de seguridad

2.2. Medidas de seguridad de carácter administrativo, físico y técnico que se pretenden adoptar

Con relación a las medidas de seguridad administrativas, físicas y técnicas, los artículos 31 y 34 de la Ley General, establecen que:

*"**Artículo 31.** Con independencia del tipo de sistema en el que se encuentren los datos personales o el tipo de tratamiento que se efectúe, el responsable deberá establecer y mantener las medidas de seguridad de carácter administrativo, físico y técnico para la protección de los datos personales, que permitan protegerlos contra daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado, así como garantizar su confidencialidad, integridad y disponibilidad.*

***Artículo 34.** Las acciones relacionadas con las medidas de seguridad para el tratamiento de los datos personales deberán ser documentadas y contenidas en un sistema de gestión.*
[...]"

Asimismo, el artículo 55 de los Lineamientos generales señalan que:

*"**Deber de seguridad***
***Artículo 55.** El responsable deberá establecer y mantener medidas de seguridad de carácter administrativo, físico y técnico para la protección de los datos personales en su posesión de conformidad con lo previsto en los artículos 31, 32 y 33 de la Ley General, con el objeto de impedir, que cualquier tratamiento de datos personales contravenga las disposiciones de dicho ordenamiento y los presentes Lineamientos generales.*

Las medidas de seguridad a las que se refiere el párrafo anterior constituyen mínimos exigibles, por lo que el responsable podrá adoptar las medidas adicionales que estime necesarias para brindar mayores garantías en la protección de los datos personales en su posesión."

Por otro lado, las Disposiciones Administrativas, en su artículo 15, fracción XIII establecen que, en la descripción de la política pública, programa, sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología que implique un tratamiento intensivo o relevante de datos personales y que pretenda poner en operación o modificar, el responsable deberá indicar, lo siguiente:

"XIII. Las medidas de seguridad de carácter administrativo, físico y técnico a implementar de conformidad con lo previsto en la Ley General o las legislaciones estatales en la materia y demás disposiciones aplicables."

Al respecto, en la Evaluación de impacto del Sistema de Procesamiento, se manifestó lo siguiente:

"[...]
XIII. Medidas de seguridad.
Medidas de seguridad de carácter administrativo, físico y técnico a implementar de conformidad con lo previsto en la Ley General o las legislaciones estatales en la materia y demás disposiciones aplicables;
En el documento de "Seguridad para la Protección de Datos Personales del Sistema de Procesamiento de Pasajeros del Aeropuerto Internacional Felipe Ángeles" se encuentran:

Funciones y obligaciones de las personas que tratan los datos personales.
Matriz de riesgo
Análisis de brecha
Mecanismos de monitoreo y revisión de las medidas de seguridad.
Política de privacidad y protección de datos personales para el sistema de procesamiento de pasajeros del AIFA.

XIV. Nombre y cargo del servidor.
Nombre y cargo del servidor o de los servidores públicos que cuentan con facultad expresa para decidir, aprobar o autorizar la puesta en operación o modificación del sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología que implique un tratamiento intensivo o relevante de datos personales.

Titular: Dr. Isidoro Pastor Román, Director General del Aeropuerto Internacional Felipe Ángeles (AIFA).
Responsable: Ing. Rogelio Gerardo Tejada Guerrero, Subdirector de Sistemas del Aeropuerto Internacional Felipe Ángeles (AIFA).

XV. Otra Información.
Cualquier otra información o documentos que considere conveniente hacer del conocimiento del Instituto o los organismos garantes.
Documento "Experiencia sin contacto en Aeropuertos con Tecnología Biométrica".
Documentación y Certificación "Privacy by Design (PbD)".
Manuales de Operación.
3. Justificación.

Justificación de la necesidad de implementar el sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología que implique un tratamiento intensivo o relevante de datos personales.

La creciente demanda del sector aeroportuario, conjugado con los avances tecnológicos en los sistemas de procesamiento de pasajeros, conducen a considerar en el AIFA sistemas que ofrezcan a los pasajeros y aerolíneas mayor seguridad, agilidad y eficiencia para el procesamiento de los pasajeros.

La tendencia tanto en México como en otros países del mundo es la transformación digital, y la industria aeroportuaria no está exenta, un ejemplo es el uso del pasaporte electrónico, que cuenta con un chip que almacena, de manera electrónica, la información de la persona, haciéndolo mucho más seguro, esta innovación tecnológica, conduce al uso de soluciones de vanguardia para el procesamiento de pasajeros en un aeropuerto.

Con el fin de mejorar la experiencia del pasajero y ofrecer mejores servicios a las aerolíneas, al utilizar las instalaciones del AIFA, se consideró contar con sistemas con funcionalidades que permiten realizar procedimientos ágiles, sin necesidad de contacto, minimizando el uso de papel y en modo auto-servicio, reduciendo así los riesgos asociados con el COVID-19 y otras enfermedades.

En este sentido, la solución de procesamiento de pasajeros permite que el pasajero pueda documentarse por sí solo, usando la aplicación móvil del AIFA, los quioscos de autoservicio (CUSS) o asistidos por agentes de las aerolíneas en los mostradores de facturación y documentación de uso común (CUPPS).

Por otra parte, la funcionalidad de biometría facial permite que, una vez que el pasajero haya realizado el registro biométrico, pueda acceder a los controles de preseguridad y abordar su vuelo simplemente escaneado su rostro en las puertas electrónicas (E-Gates).

La solución garantiza que el pasajero tenga una experiencia de viaje "Ininterrumpida", creando sinergias para la integración de tecnologías, además puede generar estadísticas/notificaciones sobre el flujo de pasajeros en el aeropuerto.

I. Las medidas propuestas son susceptibles o idóneas.

La o las medidas propuestas son susceptibles para garantizar el derecho a la protección de datos personales de los titulares.
Las medidas están detalladas en el documento de "Seguridad para la Protección de Datos Personales del Sistema de Procesamiento de Pasajeros del Aeropuerto Internacional Felipe Ángeles".
La solución vb orchestraTM cuenta con las certificaciones ISO 27001 y Privacy-byDesign. Donde, uno de los siete principios fundamentales de la Privacidad por Diseño conocido como la "Privacidad como la configuración predeterminada" establece: "La información personal se conservará solo el tiempo que sea necesario para cumplir con los propósitos establecidos y luego se destruirá de forma segura".
Técnicamente, vb orchestraTM, hace uso de las capacidades nativas de las funciones de eliminación de datos de Microsoft Windows del motor de base de datos SQL (DELETE Comando-SQL), que permiten borrar y eliminar de forma segura la información de las bases de datos y dispositivos de almacenamiento. Adicionalmente, Vision-Box, bajo los lineamientos de la certificación ISO 27001, garantiza que aplica los controles de seguridad al crear, manejar y eliminar información personal, asegurando que seguimos los procesos definidos por el Estándar Internacional.

II. Las Medidas propuestas son estrictamente necesarias.

Son las estrictamente necesarias y moderadas en el sentido de que los datos personales que se recaudan del pasajero son los mínimos necesarios para crear un buen balance entre seguridad y facilitación para tener una mejor identificación del pasajero durante su salida del AIFA.

III. Las medidas son equilibradas.

Se considera que las medidas son equilibradas debido a que se cumple con los objetivos descritos en este documento en el punto III. Objetivos generales y específicos, y se han implementado medidas para protección de los datos personales, contenidas en el "Documento de Seguridad para la Protección de Datos Personales del Sistema de Procesamiento de Pasajeros".

Existe un balance entre la facilidad y la seguridad debido a que se digitalizan, integran y automatizan los procesos de verificación de documentos e identificación de pasajeros.
[…]"

Por lo que hace al cumplimiento del deber de seguridad, en el requerimiento de información adicional se manifestó lo siguiente:

"[…]
La medida de carácter técnico que garantiza la encriptación es el empleo el Cifrado AES-256 Advanced Encryption Standard (AES) es uno de los algoritmos de cifrado más utilizados y seguros actualmente disponibles. Es de acceso público, y es el cifrado que la NSA utiliza para asegurar documentos con la clasificación "top secret". Su historia de éxito se inició en 1997, cuando el NIST (Instituto Nacional de Estándares y Tecnología) comenzó oficialmente a buscar un sucesor al envejecimiento cifrado estándar DES. Un algoritmo llamado "Rijndael", desarrollado por los criptografistas belgas Daemen y Rijmen, sobresalía tanto en seguridad como en rendimiento y flexibilidad.

Apareció en la cima de varios competidores y se anunció oficialmente el nuevo estándar de cifrado AES en 2001. El algoritmo se basa en varias sustituciones, permutaciones y transformaciones lineales, cada una ejecutada en bloques de datos de 16 bytes - por lo tanto, el término blockcipher. Esas operaciones se repiten varias veces, llamadas "rondas". Durante cada ronda, una clave circular única se calcula a partir de la clave de cifrado y se incorpora en los cálculos. Basado en la estructura de bloques de AES, el cambio de un solo bit, ya sea en la clave, o en el bloque de texto sin cifrado, da como resultado un bloque de texto cifrado completamente diferente - una ventaja clara sobre los cifrados de flujo tradicionales. La diferencia entre AES-128, AES-192 y AES-256 finalmente es la longitud de la clave: 128, 192 o 256 bits - todas las mejoras drásticas en comparación con la clave de 56 bits de DES. A modo de ilustración: El agrietamiento de una clave AES de 128 bits con un superordenador de última generación tomaría más tiempo que la presunta edad del universo. Y Boxcryptor incluso utiliza claves de 256 bits. Hasta el día de hoy, no existe un ataque factible contra AES.

Por lo tanto, AES sigue siendo el estándar de cifrado preferido para los gobiernos, bancos y sistemas de alta seguridad en todo el mundo.
En ese caso, se solicita, remitir el instrumento jurídico y/o dar a conocer la parte especifica de éste por medio del cual el proveedor se compromete a dicha confidencialidad y reserva de poder hacer accesibles estos datos personales a través de servicios que éste ofrezca.

De conformidad a la cláusula vigesimosegunda del instrumento jurídico en materia de tratamiento y protección de datos personales del sistema de procesamiento de pasajeros celebrado entre el responsable jurídico (agto. Ings. "Felipe ángeles"), el responsable de operación aeroportuaria (AIFA, S.A. DE C.V.) y el encargado (consorcio Apollo Communications S.A. de C.V.), (ver Anexo 4)."



De la revisión de la información entregada por el AIFA se logró identificar la construcción y funcionamiento de un sistema creado para el recabo de y almacenamiento de datos personales y datos biométricos en el Sistema de Procesamiento de Información, por lo que, respecto a este tema, se recomienda que adicional a la documentación presentada, se atiendan las recomendaciones de los apartados que siguen:

2.1.1. Tecnología utilizada

En lo que respecta la tecnología a utilizar, en la evaluación de impacto se señaló lo siguiente:

Tecnología que se pretende utilizar para efectuar el tratamiento intensivo o relevante de datos personales;

Este Sistema ofrece una solución ininterrumpida biométrica donde el primer punto de contacto es un punto de registro o enrolamiento, donde se recopilan los datos personales (biográficos y biométricos) del pasajero y la información de vuelo, con el objetivo de generar el token o identidad digital (PDE), que será utilizado y actualizado por la plataforma Vision Box vb

Se eliminan 12 lineas, con fundamento en el artículo 110, fracción I de la LFTAIP; Décimo séptimo de los lineamientos Generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas, en relación con el artículo 5, fracción VI de la Ley de Seguridad Nacional; 47, Bis 4 de la Ley de Aviación Civil, 46 y 47 de la Ley de Aeropuertos y 152 del Reglamento de Aeropuertos.

orchestra™ en los diferentes pasos del proceso (E-Gate de Pre-Seguridad y Abordaje). Información contenida en las especificaciones técnicas:
- E-21-MX-APOLLO-SEDENA.SystemSpecification.Pre-Security.ES v.1.
- E-21-MX-APPOLO-SEDENA.SystemSpecification.Self-BoardingES v.10.

Para verificar el correcto funcionamiento de la solución, se han realizado pruebas durante el proceso para la implementación del Sistema de procesamiento de pasajeros del AIFA, como sigue:

***Pruebas de calidad,** se llevaron a cabo durante el mes de Julio 2022; donde se validó cada una de las funcionalidades de los diferentes equipos y sistemas, siendo completadas de manera satisfactoria. El detalle se incluye en el Anexo 9.*

A. ***Pruebas de vulnerabilidad,** se llevaron a cabo durante el mes de diciembre 2022, donde se validó que el perímetro de seguridad lógica que protege la solución tecnológica cuenta con las medidas adecuadas de protección.*

B. ***Pruebas de estrés,** se cuenta con documentación (Anexo 8) y experiencia en otros aeropuertos, que muestran que el sistema cuenta con la solidez necesaria para atender un gran número de pasajeros y que serán procesados en menor tiempo respecto a la forma tradicional. Sin embargo, el AIFA validará el correcto dimensionamiento y capacidad para el procesamiento de pasajeros del sistema una vez que inicie su operación y sea utilizado de manera masiva.*

Los requerimientos técnicos de software, hardware e implementación in situ (instalación, configuración y aceptación) de los elementos que componen el aplicativo, se encuentran en el anexo "A" del contrato No. SDN/DN8/AIFA/12916F7/2021-ITP-043-02.
[...]"

De la revisión de la información entregada por el AIFA se logró identificar la construcción y funcionamiento de un sistema creado para el recabo de y almacenamiento de datos biométricos, específicamente de rasgos faciales, así como de datos relacionados con el pasaporte electrónico y de abordaje, por lo que, respecto a este tema, se recomienda que adicional a la documentación presentada, se atiendan las recomendaciones de los apartados que siguen:

2.1.2. Medidas de seguridad de carácter administrativo, físico y técnico que se pretenden adoptar

Con relación a las medidas de seguridad administrativas, físicas y técnicas, los artículos 31 y 34 de la Ley General, establecen que:

> *"**Artículo 31.** Con independencia del tipo de sistema en el que se encuentren los datos personales o el tipo de tratamiento que se efectúe, el responsable deberá establecer y mantener las medidas de seguridad de carácter administrativo, físico y técnico para la protección de los datos personales, que permitan protegerlos contra daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado, así como garantizar su confidencialidad, integridad y disponibilidad."*
> ***Artículo 34.** Las acciones relacionadas con las medidas de seguridad para el tratamiento de los datos personales deberán ser documentadas y contenidas en un sistema de gestión.*
> *[...]"*

Asimismo, el artículo 55 de los Lineamientos generales señala que:

> *"**Deber de seguridad***
> ***Artículo 55.** El responsable deberá establecer y mantener medidas de seguridad de carácter administrativo, físico y técnico para la protección de los datos personales en su posesión de conformidad con lo previsto en los artículos 31, 32 y 33 de la Ley General de Datos, con el objeto de impedir, que cualquier tratamiento de datos personales contravenga las disposiciones de dicho ordenamiento y los presentes Lineamientos generales.*
> *Las medidas de seguridad a las que se refiere el párrafo anterior constituyen mínimos exigibles, por lo que el responsable podrá adoptar las medidas adicionales que estime necesarias para brindar mayores garantías en la protección de los datos personales en su posesión."*

Por otro lado, las Disposiciones administrativas, en su artículo 15, fracción XIII establecen que, en la descripción de la política pública, programa, sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología que implique un tratamiento intensivo o relevante de datos personales y que pretenda poner en operación o modificar, el responsable deberá indicar, lo siguiente:

> *"**XIII.** Las medidas de seguridad de carácter administrativo, físico y técnico a implementar de conformidad con lo previsto en la Ley General de Datos o las legislaciones estatales en la materia y demás disposiciones aplicables. [...]"*

Al respecto, el responsable en la evaluación de impacto manifestó lo siguiente:

> *"[...]*
> *XIII. Medidas de seguridad.*
> ***Medidas de seguridad de carácter administrativo, físico y técnico a implementar de conformidad con lo previsto en la Ley General o las legislaciones estatales en la materia y demás disposiciones aplicables;***
> *En el documento de "Seguridad para la Protección de Datos Personales del Sistema de Procesamiento de Pasajeros del Aeropuerto Internacional Felipe Ángeles" se encuentran:*
> *Funciones y obligaciones de las personas que tratan los datos personales.*
> *Matriz de riesgo*

Análisis de brecha
Mecanismos de monitoreo y revisión de las medidas de seguridad.
Política de privacidad y protección de datos personales para el sistema de procesamiento de pasajeros del AIFA.
[….]"

Adicionalmente, el sujeto obligado remitió en su escrito de desahogo al requerimiento de información adicional un vínculo electrónico en el que señaló se encontraba su Documento de Seguridad, y respecto a ello mencionó:

"[…]
• De igual forma se solicita remitir las medidas de seguridad implementadas, así como el análisis de brecha a realizar sobre la aplicación móvil del AIFA e indicar que al momento de descargarla se solicitan permisos a los usuarios, y en su caso, qué tipo de permisos, a qué información se accede y las razones por las cuales se solicitan; todos los documentos deben ser remitidos en su versión íntegra.
Los permisos requeridos para la descarga de la aplicación son determinados por las tiendas digitales de descarga de aplicaciones, y son estas plataformas las que definen los lineamientos para la descarga que garanticen la correcta funcionalidad en los dispositivos.
[…]
18. Con fundamento en los artículos 15, fracción XIII, y 19, fracción III y 20 de las disposiciones administrativas, se solicita la siguiente información:
Respecto a las medidas de seguridad, se identifica que refieren que las medidas de seguridad están integradas en la columna tipo de control identificado del anexo Matriz de riesgo de datos personales, por lo que, no es posible identificar si las medidas enlistadas en los 34 riesgos describen todas las medidas de seguridad administrativas, físicas y técnicas implementadas de manera general y/o particular para todos los elementos que comprende el sistema, por lo que a partir de las observaciones realizadas al contenido del análisis de riesgos, es necesario fortalecer la descripción de las medidas de seguridad considerando todos los componentes del sistema incluyendo estas medidas en el análisis en el análisis de brecha con resultados de la eventual re evaluación de riesgos.
Se anexa documento de Matriz Riesgos actualizado en versión digital que cumple con el requerimiento solicitado (Anexo 15).
[…]"

Inicialmente, se desprende que respecto de las medidas que cuenta para la seguridad en torno al Sistema de Procesamiento, el AIFA omitió estableció concretamente las medidas de seguridad administrativas, físicas y técnicas correspondientes a dicho sistema, debidamente identificadas por cada clase de medida adoptada.

Lo anterior, ya que, si bien describió que estas se encontraban en los documentos denominados documento de "Seguridad para la Protección de Datos Personales del Sistema de Procesamiento

de Pasajeros del Aeropuerto Internacional Felipe Ángeles" y documento de Matriz Riesgos, lo cierto es que no tienen identificada una sección específica para esas medidas de seguridad.

Incluso, al requerir al AIFA que especificara las medidas adoptadas en los términos establecidos en la normatividad, se limitó a señalar que en el último de los documentos destacados se encontraba dicha información.

Al respecto, en el documento en estudio, una sección denominada "Tipo de Control Identificado", en la que se establecen una serie de acciones para realizar intervenciones en la prevención o erradicación de las vulnerabilidades identificadas, lo cierto es que no puede desprenderse con exactitud si se trata de medidas de seguridad o bien de contención en caso de que el riesgo se hubiera actualizado.

En ese sentido, este Instituto no identificó evidencia de que se realizó el análisis de riesgos a todos los elementos del sistema, es difícil determinar si el listado de medidas de seguridad entregado es suficiente y se desprende de la realización de un análisis de brecha que incluye la interpretación de los resultados del análisis de riesgos, es así que, al no tener identificados puntualmente los riesgos.

Igualmente, no es posible asociar si los controles están orientados a minimizar los riesgos que pudieran haberse encontrado en el análisis de riesgos o bien, solo se integró al documento un listado de controles de seguridad genéricos contemplados en el desarrollo que no atienden una minimización del riesgo.

También se advirtió que el AIFA cuenta con la denominada "CARTA DE CONFIDENCIALIDAD Y NO DIVULGACIÓN", la cual se observa vincula únicamente a la persona designada y/o comisionada por la Subdirección de Sistemas; sin que sea posible identificar si se dirige únicamente a servidores públicos o también se hace extensiva al personal que funge como encargado.

Finalmente, no pasa desapercibido a este Instituto que el AIFA insistió en las certificaciones con las que cuenta, incluso su apego al RGPD, sin embargo, la sola mención de adhesión a un instrumento como el instrumento normativo no puede contar como cumplimiento a los deberes establecidos en la Ley General respecto al deber de seguridad, en tanto que dicha descripción debe encontrarse adminiculada con una descripción de las medidas de seguridad adoptadas debidamente identificadas, lo cual no aconteció.

Finalmente, este Instituto observa que, sobre la certificación, esta únicamente abarca lo relacionado con Orchestra, sin que se pueda advertir pueda ser relacionada o vinculada con la

totalidad de procesos que componen el Sistema de Procesamiento. Aunado a lo anterior, no se desprende que el AIFA tenga constancia en qué consisten esas certificaciones, las evaluaciones que se realizan al mismo y sus resultados.

No obstante, se precisa lo siguiente:

Recomendaciones en torno al deber de seguridad

Clave	Recomendación
AIFA_SE_001	Se sugiere establecer puntualmente las medidas de seguridad físicas que serán aplicables al Sistema de Procesamiento, esto considerando los equipos utilizados, los medios de recabo de datos biométricos y los riesgos y vulnerabilidades que deriven del análisis de riesgo.
AIFA_SE_002	Se sugiere establecer puntualmente las medidas de seguridad administrativas que serán aplicables al Sistema de Procesamiento, esto considerando los equipos utilizados, los medios de recabo de datos biométricos y los riesgos y vulnerabilidades que deriven del análisis de riesgo.
AIFA_SE_003	Se sugiere establecer puntualmente las medidas de seguridad técnica que serán aplicables al Sistema de Procesamiento, esto considerando los equipos utilizados, los medios de recabo de datos biométricos y los riesgos y vulnerabilidades que deriven del análisis de riesgo.
AIFA_SE_004	Se sugiere identificar plenamente cada uno de los elementos del Sistema de Procesamiento, identificando por cada uno de ellos las medidas de seguridad administrativas, físicas y técnicas que son aplicables de conformidad con los riesgos identificados en cada uno.
AIFA_SE_005	Se sugiere precisar en el documento de seguridad el cargo de las personas, tanto del responsable como de los encargados, que se encuentren vinculados con el funcionamiento y mantenimiento del Sistema de Procesamiento.
AIFA_SE_006	Se sugiere vincular las medidas de seguridad que se implemente a la normatividad aplicable en la materia, como la Ley General y los Lineamientos generales.
AIFA_SE_007	Se sugiere, además de la certificación, identificar cómo se cumplen, las auditorias que se realizan y sus resultados.

Clave	Recomendación
AIFA_SE_008	Se sugiere que, además de la plataforma vb orchestra, se verifique que los restantes elementos del Sistema de Procesamiento cuenten con medidas de seguridad administrativas, físicas y técnicas.

2.1.3 Políticas Internas

De conformidad con el artículo 33, fracción I de la Ley General que a letra señala:

> *"**Artículo 33**. Para establecer y mantener las medidas de seguridad para la protección de los datos personales, el responsable deberá realizar, al menos, las siguientes actividades interrelacionadas:*
> ***I.** Crear políticas internas para la gestión y tratamiento de los datos personales, que tomen en cuenta el contexto en el que ocurren los tratamientos y el ciclo de vida de los datos personales, es decir, su obtención, uso y posterior supresión;"*

Y el artículo 56 de los Lineamientos generales que prevé:

> *"**Artículo 56.** Con relación a lo previsto en el artículo 33, fracción I de la Ley General, el responsable deberá incluir en el diseño e implementación de las políticas internas para la gestión y el tratamiento de los datos personales, al menos, lo siguiente:*
>
> ***I.** El cumplimiento de todos los principios, deberes, derechos y demás obligaciones en la materia, de conformidad con lo previsto en la Ley General y los presentes Lineamientos generales;*
> ***II.** Los roles y responsabilidades específicas de los involucrados internos y externos dentro de su organización, relacionados con los tratamientos de datos personales que se efectúen;*
> ***III.** Las sanciones en caso de incumplimiento;*
> ***IV.** La identificación del ciclo de vida de los datos personales respecto de cada tratamiento que se efectúe; considerando la obtención, almacenamiento, uso, procesamiento, divulgación, retención, destrucción o cualquier otra operación realizada durante dicho ciclo en función de las finalidades para las que fueron recabados;*
> ***V.** El proceso general para el establecimiento, actualización, monitoreo y revisión de los mecanismos y medidas de seguridad; considerando el análisis de riesgo realizado previamente al tratamiento de los datos personales, y*
> ***VI.** El proceso general de atención de los derechos ARCO."*

Los responsables deben establecer disposiciones que regulen el tratamiento que brindan a los datos personales en su posesión, a fin de que éstas sean cumplan en materia de seguridad deben considerar las acciones necesarias a fin de que se advierta el cumplimiento a todas las obligaciones en la materia de protección de datos, entre ellas de forma enunciativa, más no limitativa, la identificación las funciones del personal que intervenga en todo el ciclo de vida del dato personal

ya sea parte del sujeto obligado o externo; en su caso, las correspondientes sanciones por incumplimiento, así como el proceso de atención en el ejercicio de los derechos ARCO.

En ese sentido, en la evaluación de impacto presentada por el AIFA, precisó lo siguiente:

> *"[…]*
> *7. Política*
> *Se han establecido Políticas Internas de la Subdirección de Sistemas y para el Sistema de Procesamiento de Pasajeros.*
> *Actualmente no existe un presupuesto en específico asignado para este fin.*
> *[…]"*

Por su parte, en el desahogo al requerimiento de información adicional, este Instituto advierte que el AIFA puntualizó lo siguiente:

> *"[…]*
> *Además de contar con las políticas internas y programas de gestión del AIFA, se encuentran disponibles en el apartado virtual https://mediaaifa.s3.us-east-2.amazonaws.com/1.2.2-Politica-de-Proteccion-de-Datosdel-AIFA-OCR.pdf Se da cumplimiento a los mecanismos o procedimientos relativos a la privacidad por diseño y defecto con la documentación de la EIPDP en el anexo 3 "Documentación y certificación privacidad por diseño". (Anexo 9) Las políticas internas del Sistema de Procesamiento de Pasajeros y la política de protección de datos de esta Subdirección se encuentran dentro del Documento de seguridad remitido el 9 de enero, al cual correspondió Anexo 16; no obstante, se reenvían nuevamente para su pronta referencia. (Anexo 6)*
> *[…]*
> *Se da cumplimiento al principio de responsabilidad en el apartado virtual de protección de datos personales del AIFA https://vuelaaifa.mx/informacion-relevante-en-materia-deproteccion-de-datos-personales/*
>
> *Asimismo, a continuación encontrará el vínculo electrónico que lo remite al el Acta de cuarta sesión Ordinaria del Comité de Transparencia, del año 2022. https://media-aifa.s3.us-east-2.amazonaws.com/Acta-4-SO.pdf*
>
> *o Los sistemas de supervisión y vigilancia interna y/o externa, incluyendo auditorías, para comprobar el cumplimiento de las políticas de protección de los datos personales; Los sistemas de supervisión y vigilancia interna y/o externa se dan a conocer en el apartado virtual https://vuelaaifa.mx/informacionrelevante-en-materia-de-proteccion-de-datos-personales/*
> *[…]"*

Este Instituto advierte que, para el caso concreto del Sistema de Procesamiento, el AIFA primero señala de forma genérica que estableció de Políticas Internas de la Subdirección de Sistemas y

para el Sistema de Procesamiento de Pasajeros, lo anterior sin remitir algún documento que de cuenta de esa circunstancia.

Lo previo es importante, ya que, si bien el responsable aprobó el año pasado una política de Protección de Datos Personales, a la que no se tuvo alcance, lo cierto es que se advierte existe.

Ahora bien, al desahogar el requerimiento de información adicional, este Instituto pudo advertir que el AIFA remitió una serie de vínculos para señalar la localización de la documentación que manifestó daría cuenta del cumplimiento de lo relacionado con el tema en estudio, sin embargo, ninguno de los vínculos electrónicos dirigió al recurso electrónico aludido, excepto con el relacionado con el acta del Comité de Transparencia. Lo anterior ya que al entrar se despliega el siguiente aviso:



404

Oops! No Se Encontró La Página

Parece que no podemos encontrar lo que estás buscando. Tal vez la búsqueda de ayuda.

Respecto al último de los documentos aludidos, es importante señalar que se trata del acta de la cuarta sesión ordinaria del Comité de Transparencia del AIFA, del cual se desprende el siguiente orden del día:

ORDEN DEL DÍA

PRIMERO. - Verificación de Quórum.

SEGUNDO. - Lectura y aprobación del Orden del Día.

TERCERO. - Discusión, y en su caso, aprobación de la clasificación de la información solicitada por la Dirección de Administración a la respuesta de la solicitud de acceso con número de folio 332724322000207.

CUARTO. - Discusión, y en su caso, aprobación de la Política de Protección de Datos Personales, propuesta por la Unidad de Transparencia, en términos de lo dispuesto por el artículo 84, fracción I de La Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados.

QUINTO. - Asuntos Generales.

Si bien uno de los puntos a tratar se relaciona con la discusión, y en su caso, la aprobación de la Política de Protección de Datos Personales, propuesta por la Unidad de Transparencia, en términos de lo dispuesto por el artículo 84, fracción I, de la Ley General, lo cierto es que no se adjuntó ese documento.

Cabe destacar que el AIFA hace mención al Documento de Seguridad relacionado con el Sistema de Procesamiento; sin embargo, no se tiene certeza de que se trate del mismo documento o bien se trate de dos documentos diversos.

2.1.4 Inventario de datos personales y de los sistemas de tratamiento

De conformidad con el artículo 33, fracción III y 35, fracción I de la Ley General que a letra señala:

> *"**Artículo 33.** Para establecer y mantener las medidas de seguridad para la protección de los datos personales, el responsable deberá realizar, al menos, las siguientes actividades interrelacionadas:*
> *[...]*
> ***III.** Elaborar un inventario de datos personales y de los sistemas de tratamiento;*
> *[...]"*
> ***Artículo 35.** De manera particular, el responsable deberá elaborar un documento de seguridad que contenga, al menos, lo siguiente:*
> *[...]*
> ***I.** El inventario de datos personales y de los sistemas de tratamiento"*

Y los artículos 58 y 59 de los Lineamientos generales que prevé:

*"**Inventario de datos personales***
***Artículo 58.** Con relación a lo previsto en el artículo 33, fracción 111 de la Ley General, el responsable deberá elaborar un inventario con la información básica de cada tratamiento de datos personales, considerando, al menos, los siguientes elementos:*
***I.** El catálogo de medios físicos y electrónicos a través de los cuales se obtienen los datos personales;*
***II**. Las finalidades de cada tratamiento de datos personales;*
***III**. El catálogo de los tipos de datos personales que se traten, indicando si son sensibles o no;*
***IV.** El catálogo de formatos de almacenamiento, así como la descripción general de la ubicación física y/o electrónica de los datos personales;*
***V**. La lista de servidores públicos que tienen acceso a los sistemas de tratamiento;*
***VI.** En su caso, el nombre completo o denominación o razón social del encargado y el instrumento jurídico que formaliza la prestación de los servicios que brinda al responsable, y*
***VII.** En su caso, los destinatarios o terceros receptores de las transferencias que se efectúen, así como las finalidades que justifican éstas.*

Ciclo de vida de los datos personales en el inventario de éstos
***Artículo 59**. Aunado a lo dispuesto en el artículo anterior de los presentes Lineamientos generales, en la elaboración del inventario de datos personales el responsable deberá considerar el ciclo de vida de los datos personales conforme lo siguiente:*
I. La obtención de los datos personales;
II. El almacenamiento de los datos personales;
III. El uso de los datos personales conforme a su acceso, manejo, aprovechamiento, monitoreo y procesamiento, incluyendo los sistemas físicos y/o electrónicos utilizados para tal fin;
IV. La divulgación de los datos personales considerando las remisiones y transferencias que, en su caso, se efectúen;
V. El bloqueo de los datos personales, en su caso, y
VI. La cancelación, supresión o destrucción de los datos personales.
El responsable deberá identificar el riesgo inherente de los datos personales, contemplando su ciclo de vida y los activos involucrados en su tratamiento, como podrían ser hardware, software, personal, o cualquier otro recurso humano o material que resulte pertinente considerar."

Respecto al inventario de datos personales respecto al Sistema de Procesamiento, el AIFA adjuntó a su evaluación de impacto, un inventario de datos personales que se observa se encuentra ajustado a lo previsto en los Lineamientos.

En ese sentido, este Instituto advierte que el AIFA identificó una sección denominada "Tercero que transfiere los datos personales, en su caso", en la que señaló una serie de comunicaciones entre

las tecnologías que comprenden la solución contratada. Por lo que, en principio, este Instituto advierte que se trata de remisiones al constituir comunicaciones entre encargado y responsable y no así de responsable a responsable.

Destaca también la mención de "El SDK se encuentra inserto dentro de la aplicación móvil provista por Point Consulting., la que también es mencionada en el documento denominado "Experiencia sin contacto con tecnología biométrica", así como el diverso "Memoria Técnica Aplicación Movil", sin que se desprenda si se trata de un desarrollador adscrito a alguna de las empresas con las que SEDENA contrató la solución tecnológica o una Plataforma.

También se precisó que el consentimiento requerido se trataba de consentimiento tácito, sin embargo, para este punto es recomendable que ese apartado se homologue con las recomendaciones relacionadas con el principio de consentimiento.

Con base en ello, se emiten las siguientes consideraciones:

Clave	Recomendación
AIFA_SE_009	Se sugiere precisar de forma puntual si lo descrito en transferencias se trata de tales o se relaciona con remisiones, atendiendo lo relativo al apartado de transferencias del presente dictamen, y una vez puntualizada esa circunstancia, impactarla en el inventario de datos personales.
AIFA_SE_010	Se sugiere precisar de forma puntual si "Point Consulting", se trata de un desarrollo tecnológico de alguno de los encargados, si se trata de una entidad aparte o una subcontratación y atendiendo lo relativo al apartado de transferencias del presente dictamen, impactar la transferencia o remisión, según sea el caso, en el inventario de datos personales.

2.1.5 Funciones de los servidores públicos que tratan datos personales

De conformidad con el artículo 33, fracción II y 35, fracción II de la Ley General que a letra señala:

> *"**Artículo 33.** Para establecer y mantener las medidas de seguridad para la protección de los datos personales, el responsable deberá realizar, al menos, las siguientes actividades interrelacionadas:*
> *[...]*

> ***II.*** *Definir las funciones y obligaciones del personal involucrado en el tratamiento de datos personales;*
> *[...]*
> ***Artículo 35.*** *De manera particular, el responsable deberá elaborar un documento de seguridad que contenga, al menos, lo siguiente:*
> *[...]*
> ***II.*** *Las funciones y obligaciones de las personas que traten datos personales; [...]"*

Y el artículo 57 de los Lineamientos Generales que prevé:

> ***"Funciones y obligaciones***
> ***Artículo 57.*** *Con relación a lo dispuesto en el artículo 33, fracción II de la Ley General, el responsable deberá establecer y documentar los roles y responsabilidades, así como la cadena de rendición de cuentas de todas las personas que traten datos personales en su organización, conforme al sistema de gestión implementado. El responsable deberá establecer mecanismos para asegurar que todas las personas involucradas en el tratamiento de datos personales en su organización conozcan sus funciones para el cumplimiento de los objetivos del sistema de gestión, así como las consecuencias de su incumplimiento."*

Al respecto, dentro de la evaluación de impacto en la protección de datos personales se estableció lo siguiente:

> *"[...]*
> *XIV. Nombre y cargo del servidor.*
> *Nombre y cargo del servidor o de los servidores públicos que cuentan con facultad expresa para decidir, aprobar o autorizar la puesta en operación o modificación del sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología que implique un tratamiento intensivo o relevante de datos personales.*
> *- Titular: Dr. Isidoro Pastor Román, Director General del Aeropuerto Internacional Felipe Ángeles (AIFA).*
> *- Responsable: Ing. Rogelio Gerardo Tejada Guerrero, Subdirector de Sistemas del Aeropuerto Internacional Felipe Ángeles (AIFA).*
> *[...]"*

Por su parte, en el requerimiento de información adicional, el responsable aludió, respecto de las funciones del personal, lo siguiente:

> *"[...]*
> *Siendo misión de la Subdirección de sistemas garantizar la infraestructura y los servicios de tecnologías de la información y comunicaciones al Aeropuerto Internacional Felipe Ángeles.*
> *Y atendiendo las funciones del área como:*
> *Supervisar que las comunicaciones, sistemas de operación aeroportuaria, administrativos, financieros y comercias, equipos de cómputo, sistemas de CCTV y control de Acceso,*

megafonía y Servicios de correo, internet y antivirus operan eficientemente a fin de apoyar la productividad del AIFA.
Se anexa Manual de Organización General - octubre 2021
[...]"

Sobre el último de los documentos mencionados, se desprenden las atribuciones conferidas a la persona que ostente el cargo de Subdirector de Sistemas.

Aunado a lo previo, en el documento denominado "Definición de responsable, Encargado y Subencargados del Sistema de Procesamiento de Pasajeros"", este Instituto advierte la existencia, de al menos, otros tres servidores públicos involucrados, mismos que ostentan el cargo de Coordinador de Desarrollo, Coordinador de Controles de TI y Mesa de Servicios y Analista Técnico, sin que al efecto pudieran advertirse sus funciones específicas en el Manual remitido.

Para el caso de Empresa Vision-Box Soluções de Visão Por Computador S.A., Vision Box, Apollo Communications, Amadeus IT Group, S.A, se señala la existencia de empleados encargados de soporte, sin embargo, no se puede apreciar con claridad sus funciones en torno al Sistema de Procesamiento.

Al respecto y, en atención a lo informado por el AIFA se advirtieron las siguientes consideraciones y recomendaciones:

Clave	Recomendación
AIFA_SE_011	Se sugiere establecer, en el Manual de Organización General o especifico, según corresponda, las funciones de dichos servidores públicos.
AIFA_SE_012	Se sugiere, como parte de las obligaciones contractuales establecidas en el principio de licitud, establecer las funciones específicas a realizar por las personas que designen los encargados para intervenir en el soporte, mantenimiento y demás tareas en relación al Sistema de Procesamiento, mismas que deberán ser verificables por parte de los servidores públicos del AIFA.

2.1.6 Análisis de riesgo, de brecha y plan de trabajo.

Análisis de riesgo

El artículo 33, fracción IV de la Ley General establece:

> *"**Artículo 33**. Para establecer y mantener las medidas de seguridad para la protección de los datos personales, el responsable deberá realizar, al menos, las siguientes actividades interrelacionadas:*
> *[...]*
> ***IV.** Realizar un análisis de riesgo de los datos personales, considerando las amenazas y vulnerabilidades existentes para los datos personales y los recursos involucrados en su tratamiento, como pueden ser, de manera enunciativa más no limitativa, hardware, software, personal del responsable, entre otros;"*

Por su parte, los Lineamientos generales en su artículo 60 prevén:

> *"**Artículo 60.** Para dar cumplimiento al artículo 33, fracción IV de la Ley General, el responsable deberá realizar un análisis de riesgos de los datos personales tratados considerando lo siguiente:*
> ***I.** Los requerimientos regulatorios, códigos de conducta o mejores prácticas de un sector específico;*
> ***II.** El valor de los datos personales de acuerdo a su clasificación previamente definida y su ciclo de vida;*
> ***III.** El valor y exposición de los activos involucrados en el tratamiento de los datos personales;*
> ***IV.** Las consecuencias negativas para los titulares que pudieran derivar de una vulneración de seguridad ocurrida, y*
> ***V.** Los factores previstos en el artículo 32 de la Ley General."*

El artículo 32 de la Ley General señala:

> *"**Artículo 32**. Las medidas de seguridad adoptadas por el responsable deberán considerar:*
> ***I.** El riesgo inherente a los datos personales tratados;*
> ***II.** La sensibilidad de los datos personales tratados;*
> ***III.** El desarrollo tecnológico*
> ***IV.** Las posibles consecuencias de una vulneración para los titulares;*
> ***V.** Las transferencias de datos personales que se realicen;*
> ***VI.** El número de titulares;*
> ***VII.** Las vulneraciones previas ocurridas en los sistemas de tratamiento, y*
> ***VIII.** El riesgo por el valor potencial cuantitativo o cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada para su posesión."*

Respecto a lo remitido por el AIFA respecto al análisis de riesgos, se hace mención que en la evaluación de impacto en la protección de datos personales existe un capítulo denominado "IV. Identificación, análisis y descripción de la gestión de los riesgos inherentes para la protección de los datos personales" al desahogar el requerimiento de información adicional estableció el tipo de amenaza, amenazas específicas, vulnerabilidad, riesgo, tipo de control, tipo de riesgo y activo.

Análisis de brecha

El artículo 33, fracción V de la Ley General establece:

> *"**Artículo 33**. Para establecer y mantener las medidas de seguridad para la protección de los datos personales, el responsable deberá realizar, al menos, las siguientes actividades interrelacionadas:*
> *[...]*
> ***V**. Realizar un análisis de brecha, comparando las medidas de seguridad existentes contra las faltantes en la organización del responsable;"*

En ese mismo tema, los Lineamientos generales contemplan en su artículo 61:

> *"**Artículo 61**. Con relación al artículo 33, fracción V de la Ley General, para la realización del análisis de brecha el responsable deberá considerar lo siguiente:*
> *I. Las medidas de seguridad existentes y efectivas;*
> *II. Las medidas de seguridad faltantes, y*
> *III. La existencia de nuevas medidas de seguridad que pudieran remplazar a uno o más controles implementados actualmente."*

Respecto a lo remitido por el AIFA respecto al análisis de riesgos, se hace mención que en la evaluación de impacto en la protección de datos personales existe un capítulo denominado "VII. Identificación, análisis y gestión de los riesgos para la protección de los datos personales", así como al desahogar el requerimiento de información adicional se desprende lo subsecuente.

[redacted]

el

Se eliminan 15 lineas, con fundamento en el artículo 110, fracción I de la LFTAIP; Décimo séptimo de los lineamientos Generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas, en relación con el artículo 5, fracción VI de la Ley de Seguridad Nacional; 47, Bis 4 de la Ley de Aviación Civil, 46 y 47 de la Ley de Aeropuertos y 152 del Reglamento de Aeropuertos.

[redacted]

Al respecto y, en atención a lo informado por el AIFA se advirtieron las siguientes consideraciones y recomendaciones:

Clave	Recomendación
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]

Plan de trabajo

El artículo 33, fracción VI de la Ley General establece:

> *"**Artículo 33.** Para establecer y mantener las medidas de seguridad para la protección de los datos personales, el responsable deberá realizar, al menos, las siguientes actividades interrelacionadas:*
> *[...]*
> *VI. Elaborar un plan de trabajo para la implementación de las medidas de seguridad faltantes, así como las medidas para el cumplimiento cotidiano de las políticas de gestión y tratamiento de los datos personales;"*

Por su parte, los Lineamientos generales, en su artículo 62 prevén:

> *"**Artículo 62.** De conformidad con lo dispuesto en el artículo 33, fracción VI de la Ley General, el responsable deberá elaborar un plan de trabajo que defina las acciones a implementar de acuerdo con el resultado del análisis de riesgos y del análisis de brecha, priorizando las medidas de seguridad más relevantes e inmediatas a establecer.*

Se eliminan 13 lineas, con fundamento en el artículo 110, fracción I de la LFTAIP; Décimo séptimo de los lineamientos Generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas, en relación con el artículo 5, fracción VI de la Ley de Seguridad Nacional; 47, Bis 4 de la Ley de Aviación Civil, 46 y 47 de la Ley de Aeropuertos y 152 del Reglamento de Aeropuertos.

Lo anterior, considerando los recursos designados; el personal interno y externo en su organización y las fechas compromiso para la implementación de las medidas de seguridad nuevas o faltantes."

[redacted]

Al respecto y, reiterando en este apartado las recomendaciones realizadas en los numerales AIFA_SE_013, AIFA_SE_014 y AIFA_SE_015, se advirtieron las siguientes consideraciones y recomendaciones:

Clave	Recomendación
[redacted]	[redacted] y

Revisión y vigilancia.

De conformidad con el artículo 33, fracción VII y 35, fracción VI de la Ley General que a letra señala:

*"**Artículo 33.** Para establecer y mantener las medidas de seguridad para la protección de los datos personales, el responsable deberá realizar, al menos, las siguientes actividades interrelacionadas:*
[…]
***VII.** Monitorear y revisar de manera periódica las medidas de seguridad implementadas, así como las amenazas y vulneraciones a las que están sujetos los datos personales,*
[…]"

*"**Artículo 35.** De manera particular, el responsable deberá elaborar un documento de seguridad que contenga, al menos, lo siguiente:*
[…]
***VI.** Los mecanismos de monitoreo y revisión de las medidas de seguridad, y*
[…]"

Y el artículo 63 de los Lineamientos generales prevé:

*"**Monitoreo y supervisión periódica de las medidas de seguridad implementadas***
***Artículo 63.** Con relación al artículo 33, fracción VII de la Ley General, el responsable deberá evaluar y medir los resultados de las políticas, planes, procesos y procedimientos implementados en materia de seguridad y tratamiento de los datos personales, a fin de*

Se eliminan 6 lineas, con fundamento en el artículo 110, fracción I de la LFTAIP; Décimo séptimo de los lineamientos Generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas, en relación con el artículo 5, fracción VI de la Ley de Seguridad Nacional; 47, Bis 4 de la Ley de Aviación Civil, 46 y 47 de la Ley de Aeropuertos y 152 del Reglamento de Aeropuertos.

verificar el cumplimiento de los objetivos propuestos y, en su caso, implementar mejoras de manera continua. Para cumplir con lo dispuesto en el párrafo anterior del presente artículo, el responsable deberá monitorear continuamente lo siguiente:

I. Los nuevos activos que se incluyan en la gestión de riesgos;
II. Las modificaciones necesarias a los activos, como podría ser el cambio o migración tecnológica, entre otras;
III. Las nuevas amenazas que podrían estar activas dentro y fuera de su organización y que no han sido valoradas;
IV. La posibilidad de que vulnerabilidades nuevas o incrementadas sean explotadas por las amenazas correspondientes;
V. Las vulnerabilidades identificadas para determinar aquéllas expuestas a amenazas nuevas o pasadas que vuelvan a surgir;
VI. El cambio en el impacto o consecuencias de amenazas valoradas, vulnerabilidades y riesgos en conjunto, que resulten en un nivel inaceptable de riesgo, y
VII. Los incidentes y vulneraciones de seguridad ocurridas. Aunado a lo previsto en las fracciones anteriores del presente artículo, el responsable deberá contar con un programa de auditoría, interno y/o externo, para monitorear y revisar la eficacia y eficiencia del sistema de gestión."

Dentro del desahogo al requerimiento de información adicional, se desprende en relación con la vigilancia, lo siguiente:

"[...]
c o Los sistemas de supervisión y vigilancia interna y/o externa, incluyendo auditorías, para comprobar el cumplimiento de las políticas de protección de los datos personales;
Los sistemas de supervisión y vigilancia interna y/o externa se dan a conocer en el apartado virtual https://vuelaaifa.mx/informacionrelevante-en-materia-de-proteccion-de-datos-personales/ [...]"

Dentro de lo que puede encontrarse entre los documentos remitidos en el desahogo al requerimiento de información adicional, se encuentra el documento denominado "MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD", este Instituto advierte un mecanismo dividido en dos etapas, una de monitoreo en la que se desprenden ocho medidas que deben verificarse, y ante la alguna en la que se respondiera "NO" se continua con la etapa denominada supervisión.

En ese sentido, si bien en principio se cuenta de manera general con un mecanismo de supervisión y vigilancia, lo cierto es que es de carácter genérico y no se desprenden esas medidas específicas para el Sistema de Procesamiento, mismas que pueden ser incluidas dentro del Plan de Trabajo.

Al respecto y, en atención a lo informado por el AIFA se reitera en el presente la recomendación efectuada en el numeral AIFA_SE_016.

Capacitación.

De conformidad con el artículo 33, fracción VIII y 35, fracción VII de la Ley General que a letra señala:

> *"**Artículo 33.** Para establecer y mantener las medidas de seguridad para la protección de los datos personales, el responsable deberá realizar, al menos, las siguientes actividades interrelacionadas:*
> *[…]*
> *VIII. Diseñar y aplicar diferentes niveles de capacitación del personal bajo su mando, dependiendo de sus roles y responsabilidades respecto del tratamiento de los datos personales.*
> *[…]"*
> ***"Artículo 35.** De manera particular, el responsable deberá elaborar un documento de seguridad que contenga, al menos, lo siguiente:*
> *[…]*
> I. *El programa general de capacitación."*

Y el artículo 64 de los Lineamientos generales que prevé:

> ***"Capacitación***
> ***Artículo 64.** Para el cumplimiento de lo previsto en el artículo 33, fracción VIII de la Ley General, el responsable deberá diseñar e implementar programas a corto, mediano y largo plazo que tengan por objeto capacitar a los involucrados internos y externos en su organización, considerando sus roles y responsabilidades asignadas para el tratamiento y seguridad de los datos personales y el perfil de sus puestos.*
> *En el diseño e implementación de los programas de capacitación a que se refiere el párrafo anterior del presente artículo, el responsable deberá tomar en cuenta lo siguiente:*
> *I. Los requerimientos y actualizaciones del sistema de gestión;*
> *II. La legislación vigente en materia de protección de datos personales y las mejores prácticas relacionadas con el tratamiento de éstos;*
> *III. Las consecuencias del incumplimiento de los requerimientos legales o requisitos organizacionales, y*
> *IV. Las herramientas tecnológicas relacionadas o utilizadas para el tratamiento de los datos personales y para la implementación de las medidas de seguridad."*

Al respecto, se tare a colación lo señalado en el requerimiento de información adicional, en el cual el AIFA señala lo siguiente:

> *"[…]*

Capacitación.
i. El programa de Instrucción de Seguridad de la Aviación Civil del Aeropuerto Internacional "Felipe Ángeles", es el documento que establece el contenido de la capacitación a la que se sujeta el personal de la Guardia Nacional que desempeña las funciones de Inspector y Guardia de Seguridad, este incluye el curso "Tronco común", en el que se contempla la información correspondiente a Derechos Humanos, para prevenir la discriminación de los usuarios del AIFA (se anexa contenido del curso).
5.1.1.6 Contenido del curso

Tema	Inicial (min)	Recurrente (min)
Modulo 1 "Concientización en materia de Seguridad de la Aviación Civil"	01:40	00:55
Modulo 2 "Trabajo en el aeropuerto"	01:30	00:45
Modulo 3 "Derechos Humanos y facilitación de los pasajeros"	02:00	01:10
Modulo 4 "Identificación de artefactos explosivos y otros artículos de uso restringido"	03:30	01:50
Modulo 5 "Inspección del edificio2	02:00	01:00
Modulo 6 "Marco legal y normativo"	06:00	08:30
Total, de horas	16:25	08:30

ii. Los instructores que imparten la capacitación al personal de la Guardia Nacional que se desempeña como Inspectores y Guardias de Seguridad, cuentan con la certificación correspondiente para impartir capacitación en materia de seguridad de la aviación ante la Agencia Federal de Aviación Civil.
[...]
o La destinación de recursos autorizados para la instrumentación de programas y políticas de protección de datos personales;
En el presente ejercicio fiscal no se tienen contemplados recursos específicos para capacitación ni para instrumentación de programas y Políticas De Protección De Datos Personales.
[...]
El plan de trabajo que propone la Subdirección a mi cargo tiene como eje modular la capacitación del personal de esta área, en este sentido, dentro del Programa de Capacitación aprobado por el Comité de Transparencia el pasado 12 de enero del año en curso, se propuso que el personal del AIFA, deberá tomar cursos específicos en materia de manejo de biométricos: (Anexo 9)
[...]"

Sobre la capacitación, y como se señaló en este dictamen, el responsable manifestó por una parte que realiza capacitación al personal de Guardia Nacional para evitar la discriminación a los usuarios

del Aeropuerto Internacional Felipe Ángeles, por otra parte aluden que no cuentan con presupuesto para realizar capacitaciones y, finalmente, que se propuso que el personal del AIFA, deberá tomar cursos específicos en materia de manejo de biométricos, sin especificar cual.

Si bien se advierte que se realiza capacitación constante a sus empleados, lo cierto es que no se advierte una especialización en el marco de la PBI, pues dado el tratamiento que se realiza en dicha Plataforma, se requiere acreditar capacitación especializada a los servidores públicos encargados de la operación, uso y mantenimiento de dicha Plataforma.

Por lo expuesto, este Instituto reitera en sus términos las observaciones sobre el tema que se efectuaron en el apartado de responsabilidad, así como las recomendaciones identificadas con los numerales: AIFA_SE_016, AIFA_RE_002 y AIFA_RE_003.

3. Deber de confidencialidad

El artículo 42 de la Ley General dispone lo siguiente:

> *"**Artículo 42**. El responsable deberá establecer controles o mecanismos que tengan por objeto que todas aquellas personas que intervengan en cualquier fase del tratamiento de los datos personales, guarden confidencialidad respecto de éstos, obligación que subsistirá aún después de finalizar sus relaciones con el mismo.*
> *Lo anterior, sin menoscabo de lo establecido en las disposiciones de acceso a la información pública."*

A su vez, el artículo 71 de los Lineamientos Generales señala lo siguiente:

> ***"Deber de confidencialidad***
> ***Artículo 71.** El responsable deberá establecer controles o mecanismos que tengan por objeto que todas aquellas personas que intervengan en cualquier fase del tratamiento de los datos personales, guarden confidencialidad respecto de éstos, obligación que subsistirá aún después de finalizar sus relaciones con el mismo."*

De las disposiciones anteriores, se desprende que el responsable está obligado a guardar reserva u sigilo durante todo el tratamiento de los datos personales.

Respecto al cumplimiento del deber de confidencialidad, en la evaluación de impacto se señaló lo siguiente:

> ***IV. "Divulgación de los datos personales.***
> *En los sistemas de Procesamiento de Pasajeros del AIFA no existe divulgación de datos personales.*

Los datos personales recolectados de los pasajeros son transmitidos entre los componentes de la plataforma de Vision Box para la identificación del pasajero y transferidos (datos asociados al pase de abordar) a los Sistemas de Control de las Aerolíneas para la elegibilidad del pasajero."

"Como medidas adicionales de seguridad y confidencialidad y según lo establece el Artículo 55 de la mencionada Ley, en este caso el ejercicio de los derechos ARCO no sería procedente porque los datos personales no se encontrarán en posesión del responsable."

"En cumplimiento al deber de confidencialidad, cada uno de los servidores públicos enlistados, suscribirán la "Carta de Confidencialidad y No Divulgación", a través de la cual se comprometen a guardar completa confidencialidad de la información a la que tienen acceso".

Por otro lado, en el requerimiento de información adicional se manifestó lo siguiente:

"La medida de carácter técnico que garantiza la encriptación es el empleo el Cifrado AES-256 Advanced Encryption Standard (AES) es uno de los algoritmos de cifrado más utilizados y seguros actualmente disponibles. Es de acceso público, y es el cifrado que la NSA utiliza para asegurar documentos con la clasificación "top secret". Su historia de éxito se inició en 1997, cuando el NIST (Instituto Nacional de Estándares y Tecnología) comenzó oficialmente a buscar un sucesor al envejecimiento cifrado estándar DES. Un algoritmo llamado "Rijndael", desarrollado por los criptografistas belgas Daemen y Rijmen, sobresalía tanto en seguridad como en rendimiento y flexibilidad.

Apareció en la cima de varios competidores y se anunció oficialmente el nuevo estándar de cifrado AES en 2001. El algoritmo se basa en varias sustituciones, permutaciones y transformaciones lineales, cada una ejecutada en bloques de datos de 16 bytes - por lo tanto, el término blockcipher. Esas operaciones se repiten varias veces, llamadas "rondas". Durante cada ronda, una clave circular única se calcula a partir de la clave de cifrado y se incorpora en los cálculos. Basado en la estructura de bloques de AES, el cambio de un solo bit, ya sea en la clave, o en el bloque de texto sin cifrado, da como resultado un bloque de texto cifrado completamente diferente - una ventaja clara sobre los cifrados de flujo tradicionales. La diferencia entre AES-128, AES-192 y AES-256 finalmente es la longitud de la clave: 128, 192 o 256 bits - todas las mejoras drásticas en comparación con la clave de 56 bits de DES. A modo de ilustración: El agrietamiento de una clave AES de 128 bits con un superordenador de última generación tomaría más tiempo que la presunta edad del universo. Y Boxcryptor incluso utiliza claves de 256 bits. Hasta el día de hoy, no existe un ataque factible contra AES. Por lo tanto, AES sigue siendo el estándar de cifrado preferido para los gobiernos, bancos y sistemas de alta seguridad en todo el mundo.

En ese caso, se solicita, remitir el instrumento jurídico y/o dar a conocer la parte específica de éste por medio del cual el proveedor se compromete a dicha confidencialidad y reserva de poder hacer accesibles estos datos personales a través de servicios que éste ofrezca.

De conformidad a la cláusula vigesimosegunda del instrumento jurídico en materia de tratamiento y protección de datos personales del sistema de procesamiento de pasajeros celebrado entre el responsable jurídico (agto. Ings. "Felipe ángeles"), el responsable de operación aeroportuaria (AIFA, S.A. DE C.V.) y el encargado (consorcio Apollo Communications S.A. de C.V.), (ver Anexo 4)."

Asimismo, adjuntó como anexo una Carta de confidencialidad que señala lo siguiente:

CARTA DE CONFIDENCIALIDAD Y NO DIVULGACIÓN

Zumpango, Estado de México, a ____ de _____ de _____

Con motivo de las funciones que tengo encomendadas como personal designado y/o comisionado en la Subdirección de Sistemas del Aeropuerto Internacional "Felipe Ángeles" S.A de C.V., y toda vez que dentro de mi ámbito de atribuciones puedo tener acceso a documentos de carácter confidencial, reservado, y/o a datos personales concernientes a personas fisicas identificadas o identificables; por este medio expresamente manifiesto que me obligo a evitar: divulgar, revelar, comunicar, transmitir, grabar, duplicar, copiar o reproducir información clasificada por cualquier otro medio electrónico, físico o tecnológico sin autorización previa, expresa o por escrito de mi superior jerárquico.

De igual forma, me comprometo a no entregar ni difundir a cualquier persona ajena a esta institución y/o Unidad, de forma verbal o por escrito, directa o indirectamente, información confidencial y/o reservada contenida en cualquier tipo de documento, ya sea expediente, escrito, oficio, acuerdo, directiva, directriz, circular, contrato, convenio, instructivo, nota, tarjeta, memorando, estadística o cualesquier otro que se encuentre en cualquier medio sea fisico, electrónico, impreso, escrito, sonoro, visual, informático u holográfico, de la que tenga conocimiento con motivo de las actividades que desarrollo con motivo de mi empleo, cargo o comisión.

Reconozco y acepto que el incumplimiento a lo anterior, podrá traer consigo las responsabilidades penales y administrativas en las que pudiera incurrir en términos de lo establecido en los artículos 7, fracción V, 49 de la Ley General de Responsabilidades Administrativas de los Servidores Públicos; 214, fracción IV del Código Penal Federal, 186 de la Ley Federal de Transparencia y Acceso a la Información Pública; artículo 42 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados; Décimo de los Lineamientos Generales de Clasificación y Desclasificación; así como elaboración de las versiones públicas.

A T E N T A M E N T E

*Nombre completo del servidor público:*_____

*Firma:*_____

*Cargo:*_____

En atención a las cuestiones anteriormente vertidas por parte del AIFA con relación al deber de confidencialidad, es importante precisar que, del análisis efectuado a la información proporcionada, se advierten algunas consideraciones al respecto conforme a lo siguiente:

Como ha quedado referenciado con anterioridad en atención al artículo 42 de la Ley General, se debe de garantizar que se cuente con los controles o mecanismos que tengan por objeto que todas aquellas personas que intervengan en cualquier fase del tratamiento de los datos personales, guarden confidencialidad respecto de éstos, obligación que subsistirá aún después de finalizar sus relaciones con el mismo.

Bajo este contexto, como se puede observar de la información proporcionada se advierte que el responsable suscribirá cartas de confidencialidad y no divulgación con relación al personal del AIFA con la finalidad de que se garantice el deber de confidencialidad que nos ocupa.

Asimismo, se señala que en cuanto al encargado siendo el consorcio Apollo Communications S.A. de C.V. conforme al instrumento jurídico suscrito el proveedor se compromete a dicha confidencialidad y reserva de poder hacer accesibles estos datos personales a través de servicios que éste ofrezca, por su parte se agrega el siguiente documento: "INSTRUMENTO JURÍDICO EN MATERIA DE TRATAMIENTO Y PROTECCIÓN DE DATOS PERSONALES DEL SISTEMA DE PROCESAMIENTO DE PASAJEROS CELEBRADO ENTRE EL RESPONSABLE JURÍDICO (AGRUPAMIENTO DE INGENIEROS "FELIPE ÁNGELES"), EL RESPONSABLE DE OPERACIÓN AEROPORTUARIA (AIFA, S.A. DE C.V.) Y EL ENCARGADO (CONSORCIO APOLLO COMMUNICATIONS, S.A. DE C.V.), A QUIENES EN SU CONJUNTO SE DENOMINARAN COMO LAS PARTES", en el cual se señala que **el responsable de operación aeroportuaria deberá formalizar un documento con el encargado sobre el deber de confidencialidad que debe cumplir con respecto de los datos personales que se tratan**; En el caso de que los servicios del encargado estén contratados o adheridos a los servicios aplicaciones e infraestructura en el cómputo en la nube, **el responsable de operación aeroportuaria debe garantizar que, en el tratamiento de datos personales, el encargado garantice políticas de protección de datos personales en términos de la legislación mexicana. Y aunado a lo anterior el encargado deberá acreditar fehacientemente a través de documentos legales la confidencialidad que debe guardar con respecto de los datos personales sobre los que preste el servicio**, de los cuales no se observa con claridad que se esté dando cumplimiento conforme a lo señalado en dicho instrumento.

Aunado lo anterior, derivado de análisis efectuado se advierte que existen otras personas que intervienen en el tratamiento de los datos personales ya sea por parte del Responsable o en su

carácter de encargados e inclusive sub encargados, sin que se observe se señalen los controles y mecanismos mediante los cuales se garantizara el deber de confidencialidad de estos.

Es importante destacar que se observa que por parte del personal de las aerolíneas se pudiera estar efectuando el tratamiento de datos personales durante el proceso de enrolamiento de las y los titulares de los datos personales.

Cabe mencionar que si bien dentro de los anexos presentados se contempla en contrato SDN/DN8/AIFA/12916-F7/2021-ITP-043.02 mismo que se reitera es suscrito por parte de SEDENA con Apollo, Visión Box y Amadeus, el cual si bien señala en su cláusula décimo novena lo referente a la confidencialidad, también lo es que este es con relación a la Adquisición, Suministro, Instalación, Comisionamiento, y Puesta en operación del Sistema de Seguridad de la Aviación, Operación Aeroportuaria, Procesamiento del Pasajero, Infraestructuras de Telecomunicaciones, Ciberseguridad y Soporte al Pasajero para la Ciudad Aeroportuaria (AIFA).

- Por lo que, con relación a lo previamente señalado y también, considerando que el deber de confidencialidad se encuentra intrínsecamente relacionado con el deber de seguridad, el cual ya fue analizado, debido a que éste último busca garantizar los tres pilares de seguridad de la información, a saber:
  1. Disponibilidad, la cual implica que la información estará disponible para acceder a ella en el momento que se necesite y en la forma requerida;
  2. Integridad, la cual busca garantizarse estableciendo y delimitando a las entidades autorizadas para su creación, modificación o eliminación, y
  3. Confidencialidad, misma que busca garantizar que la información no sea expuesta o accedida por entidades no autorizadas.

En ese sentido, el establecer las medidas de seguridad administrativas, físicas y técnicas adecuadas y suficientes y bajo un enfoque basado en riesgos, coadyuvara en el cumplimiento del deber de confidencialidad, de las cuales ya se emitieron las consideraciones pertinentes conforme a la información proporcionada por el AIFA.

En ese sentido, se realizan las recomendaciones siguientes:

Recomendaciones en torno al deber de confidencialidad

Clave	Recomendación
AIFA_CONF_001	Es importante que, en todo momento se tengan identificadas claramente las diferentes fases del tratamiento de datos personales considerando todas las finalidades a las que serán

	sometidos los datos personales y las personas que intervienen en cada etapa, esto pudiera aplicar al personal de las aerolíneas, a efecto de que se establezcan los procedimientos específicos para garantizar el resguardo de la confidencialidad de estos y evitar fuga de información o acceso indebido de los datos personales.
AIFA_CONF_002	Se recomienda la contemplación de cláusulas de confidencialidad pertinentes para tal efecto en los convenios de colaboración que se suscriban, considerando la sensibilidad de los datos, así como en su caso, las nuevas relaciones con encargados o terceros receptores.
AIFA_CONF_003	Se recomienda realizar un análisis de las personas que intervienen en el tratamiento de los datos personales ya sea por parte del responsable o en su carácter de encargados e inclusive sub encargados, a fin de determinar los controles y mecanismos mediante los cuales se garantizara el deber de confidencialidad de estos, esto con la finalidad de que se pueda efectuar el tratamiento de los datos personales a manera de que se garantice su protección más amplia.

4. Derechos ARCO y portabilidad de datos personales

Los artículos 43, 44, 45, 46, 47, 49, 50, 51, 52, 53, 54, 55 y 86 de la Ley General, los artículos 73, 76, 77, 78, 79, 80, 81, 91, 92, 93, 94 y 95 de los Lineamientos generales, de los cuales se advierte que los derechos ARCO son prerrogativas que tiene toda persona física para:

- Acceder a los datos personales y conocer la información relacionada con las condiciones y generalidades de su tratamiento.
- Rectificar sus datos personales cuando resulten ser inexactos, incompletos o no se encuentren actualizados.
- Cancelar sus datos personales de los archivos, registros, expedientes y sistemas del responsable, a fin de que los mismos ya no estén en su posesión y dejen de ser tratados por este último.
- Oponerse al tratamiento de sus datos personales cuando aun siendo lícito el tratamiento, el mismo deba cesar para evitar que su persistencia cause un daño o perjuicio al titular y los datos personales sean objeto de un tratamiento automatizado, el cual le produzca efectos jurídicos no deseados o afecte de manera significativa sus intereses, derechos o libertades, y estén destinados a evaluar, sin intervención humana, determinados aspectos personales del

mismo o analizar o predecir, en particular, su rendimiento profesional, situación económica, estado de salud, preferencias sexuales, fiabilidad o comportamiento.

En este sentido, la solicitud para el ejercicio de los derechos ARCO debe señalar lo siguiente:

- El nombre del titular y su domicilio o cualquier otro medio para recibir notificaciones.
- Los documentos que acrediten la identidad del titular y, en su caso, la personalidad e identidad de su representante.
- De ser posible, el área responsable que trata los datos personales y ante el cual se presenta la solicitud.
- La descripción clara y precisa de los datos personales respecto de los que el titular busca ejercer alguno de los derechos ARCO.
- La descripción del derecho ARCO que se pretende ejercer, o bien, lo que solicita el titular.
- Cualquier otro elemento o documento que facilite la localización de los datos personales, en su caso.
- Tratándose del ejercicio del derecho de acceso, deberá contener el señalamiento de la modalidad en la que el titular prefiere que sus datos personales se reproduzcan.

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, conforme las siguientes reglas:

- El titular deberá acreditar su identidad a través de los medios previstos en el artículo 76 de los Lineamientos generales. Por su parte, su representante deberá acreditar su identidad y la personalidad con la que actúa conforme a los medios enlistados en el artículo 77 de los Lineamientos generales.
- En el caso del 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.
- Para la acreditación de la identidad de un menor y la representación de los padres que ejercen la patria potestad, de una persona distinta a los padres que ejercen la patria potestad o del tutor se deberán observar las reglas y medios previstos en los artículos 78, 79 y 80 de los Lineamientos generales.
- Cuando el titular sea una persona en estado de interdicción o incapacidad declarada por ley o por autoridad judicial, además de acreditar la identidad de la persona, su representante deberá acreditar su identidad y representación conforme a los medios previstos por el artículo 81 de los Lineamientos generales.

Es por ello, que el responsable se encuentra obligado a establecer procedimientos sencillos que permitan el ejercicio de los derechos ARCO de los datos personales utilizados, bajo las siguientes condiciones:

- Los derechos ARCO se pueden ejercer en cualquier momento, donde el ejercicio de cualquiera de ellos no es requisito previo, ni impide el ejercicio de otro.
- Procurar que las personas con algún tipo de discapacidad o grupos vulnerables puedan ejercer, en igualdad de circunstancias, su derecho a la protección de datos personales.
- La prohibición de imponer al titular mayores requisitos en las solicitudes para el ejercicio de los derechos ARCO que las señaladas en el artículo 52 de la Ley General y 83 de los Lineamientos generales.
- La prohibición de aumentar los plazos previstos en el artículo 51 de la Ley General para la atención y respuesta de solicitudes para el ejercicio de los derechos ARCO, los cuales se traducen en 20 días hábiles, contados a partir del día siguiente a la recepción de la solicitud, para que el responsable determine la procedencia o improcedencia del derecho de que se trate, el cual podrá ampliarse por una sola vez hasta por 10 días hábiles. En caso de que resulte procedente el ejercicio de los derechos ARCO, el responsable deberá hacerlo efectivo en un plazo que no podrá exceder de quince días hábiles, contados a partir del día siguiente en que se haya notificado la respuesta al titular.
- El ejercicio del derecho de acceso es gratuito. Los cobros solo podrán realizarse cuando se quiera recuperar los costos de reproducción, certificación o envío.

De esta manera, la obligación de acceso a los datos personales se dará por cumplida cuando el responsable ponga a disposición del titular, previa acreditación de su identidad y, en su caso, la identidad y personalidad de su representante, los datos personales a través de los medios previstos en el artículo 92 de los Lineamientos Generales.

Asimismo, la obligación de rectificar los datos personales se dará por cumplida cuando el responsable notifique al titular, previa acreditación de su identidad y, en su caso, la identidad y personalidad de su representante, una constancia que acredite la corrección solicitada. Para ello deberá considerar, al menos, los requisitos previstos por el artículo 93 de los Lineamientos generales.

Por su parte, la obligación de cancelar los datos personales se dará por cumplida cuando el responsable notifique al titular, previa acreditación de su identidad y, en su caso la identidad y personalidad de su representante, una constancia que cumpla con los requisitos y formalidades previstas en el artículo 94 de los Lineamientos generales.

Mientras que la obligación de cesar el tratamiento de los datos personales se dará por cumplida cuando el responsable notifique al titular, previa acreditación de su identidad y, en su caso, la identidad y personalidad de su representante, una constancia que señale dicha situación.

Finalmente, el responsable podrá determinar la improcedencia del ejercicio de los derechos ARCO cuando se actualice alguna de las siguientes razones:

- El titular o su representante no estén debidamente acreditados.
- Los datos personales no se encuentren en posesión del responsable.
- Exista un impedimento legal.
- Se lesionen los derechos de un tercero.
- Se obstaculicen actuaciones judiciales o administrativas.
- Exista una resolución de autoridad competente que restrinja el acceso a los datos personales o no permita la rectificación, cancelación u oposición de los mismos.
- La cancelación u oposición haya sido previamente realizada.
- El responsable no sea competente.
- Los datos personales sean necesarios para proteger intereses jurídicamente tutelados del titular.
- Los datos personales sean necesarios para dar cumplimiento a obligaciones legalmente adquiridas por el titular.
- En función de sus atribuciones legales el uso cotidiano, resguardo y manejo sean necesarios y proporcionales para mantener la integridad, estabilidad y permanencia del Estado mexicano.
- Los datos personales sean parte de la información que las entidades sujetas a la regulación y supervisión financiera del responsable hayan proporcionado a éste, en cumplimiento a requerimientos de dicha información sobre sus operaciones, organización y actividades.

Los artículos 49, último párrafo y 97 de la Ley General, así como 75, 82, 96 y 129 de los Lineamientos Generales, aplicables a los responsables del sector público, refieren respecto a personas fallecidas, así como al interés jurídico o legítimo, lo siguiente:

- Tratándose de datos personales concernientes a personas fallecidas, la persona que acredite tener un interés jurídico, de conformidad con las leyes aplicables, podrá ejercer los derechos ARCO, siempre que el titular de los derechos hubiere expresado fehacientemente su voluntad en tal sentido o que exista un mandato judicial para dicho efecto. En caso de que la persona fallecida no hubiere expresado fehacientemente su voluntad, bastará que la persona que pretende ejercer los derechos ARCO acredite su interés jurídico.
- La interposición de un recurso de revisión o de inconformidad de datos personales concernientes a personas fallecidas, podrá realizarla la persona que acredite tener un interés jurídico o legítimo.
- Se entenderá por interés jurídico aquel que tiene una persona física que, con motivo del fallecimiento del titular, pretende ejercer los derechos ARCO de éste, para el reconocimiento de derechos sucesorios, atendiendo a la relación de parentesco por consanguinidad o

afinidad que haya tenido con el titular, el cual se acreditará en términos de las disposiciones legales aplicables.

- Puede alegar interés jurídico, de manera enunciativa más no limitativa, el albacea, herederos, legatarios, familiares en línea recta sin limitación de grado y en línea colateral hasta el cuarto grado, lo que se acreditará con copia simple del documento delegatorio, pasado ante la fe de notario público o suscrito ante dos testigos.
- Cuando el titular sea un menor de edad, el interés jurídico se acreditará con la copia del acta de defunción del menor, el acta de nacimiento o identificación del menor, así como la identificación de quien ejercía la patria potestad y/o tutela.
- Cuando el titular sea una persona en estado de interdicción o incapacidad declarada por ley o por autoridad judicial, el interés jurídico se acreditará con la copia de su acta de defunción, el documento de su identificación oficial y de quien ejercía la tutela, así como el instrumento legal de designación del tutor.
- La persona que acredite tener un interés jurídico deberá presentar ante el responsable los siguientes documentos:
  - Acta de defunción del titular.
  - Documentos que acrediten el interés jurídico de quien pretende ejercer el derecho, y
  - Documento de identificación oficial de quien solicita el ejercicio de los derechos ARCO.
- Se entenderá por interés legítimo aquel interés personal, individual o colectivo, cualificado, actual, real y jurídicamente relevante, que puede traducirse en un beneficio jurídico en favor del peticionario derivado de una afectación a su esfera jurídica en sentido amplio, que puede ser de índole económica, profesional, de salud, o de cualquier otra.

Por su parte, en lo que respecta al ejercicio de los derechos ARCO de personas en estado de interdicción o incapacidad legal, se deberá observar lo dispuesto en las leyes civiles y la representación será conforme a las reglas que establezca dicha normatividad.

Por su parte, el artículo 74 de los Lineamiento Generales dispone lo siguiente:

> ***"Ejercicio de derechos ARCO de menores de edad y personas en estado de interdicción o incapacidad***
> *Artículo 74. En términos del artículo 49, párrafo tercero de la Ley General, en el ejercicio de los derechos ARCO de menores de edad o de personas físicas que se encuentren en estado de interdicción o incapacidad declarada por ley o por autoridad judicial, se estará a las reglas de representación dispuestas en el Código Civil Federal y demás disposiciones que resulten aplicables en la materia, así como a los artículos 76, 77, 78, 79, 80, 81 Y 82 de los presentes Lineamientos generales. Además de lo dispuesto en el párrafo anterior del presente artículo, tratándose de menores de edad se deberá privilegiar el interés superior del menor conforme a la legislación que resulte aplicable en la materia."*

En ese mismo sentido, el artículo 76 de los mismos Lineamientos señala que la identidad de las personas en estado de interdicción o incapacidad declarada por la ley, se podrá acreditar mediante su acta de nacimiento, CURP, pasaporte o cualquier otro documento o identificación oficial expedida para tal fin.

En ese orden de ideas, el artículo 77 de los lineamientos, se refiere a los medios para acreditar la identidad y personalidad del representante presentando ante el responsable lo siguiente:

"I. Copia simple de la identificación oficial del titular;
II. Identificación oficial del representante, e
III. Instrumento público; carta poder simple firmada ante dos testigos anexando copia simple de las identificaciones oficiales de quienes intervengan en la suscripción del mismo, o declaración en comparecencia personal del titular."

Sumado a ello, cuando el titular sea una persona en estado de interdicción o incapacidad declarada por ley o por autoridad judicial, además de acreditar la identidad de la persona, su representante deberá acreditar su identidad y representación mediante los siguientes documentos:

"I. Instrumento legal de designación del tutor, y
II. Documento de identificación oficial del tutor."

Adicionalmente, el artículo 57 de la Ley General, previene el derecho a la portabilidad de datos personales, en los términos siguientes:

Ley General
"Capítulo III
De la Portabilidad de los Datos
Artículo 57. *Cuando se traten datos personales por vía electrónica en un formato estructurado y comúnmente utilizado, el titular tendrá derecho a obtener del responsable una copia de los datos objeto de tratamiento en un formato electrónico estructurado y comúnmente utilizado que le permita seguir utilizándolos.*
Cuando el titular haya facilitado los datos personales y el tratamiento se base en el consentimiento o en un contrato, tendrá derecho a transmitir dichos datos personales y cualquier otra información que haya facilitado y que se conserve en un sistema de tratamiento automatizado a otro sistema en un formato electrónico comúnmente utilizado, sin impedimentos por parte del responsable del tratamiento de quien se retiren los datos personales.
El Sistema Nacional establecerá mediante lineamientos los parámetros a considerar para determinar los supuestos en los que se está en presencia de un formato estructurado y comúnmente utilizado, así como las normas técnicas, modalidades y procedimientos para la transferencia de datos personales."

Precepto normativo del cual es posible advertir lo siguiente, en relación con la portabilidad de los datos personales:

- Los datos personales deben de ser tratados por vía electrónica en un formato estructurado y comúnmente utilizado.
- El titular tendrá la prerrogativa de obtener del responsable una copia de los datos objeto de tratamiento en un formato electrónico estructurado y comúnmente utilizado que le permita seguir utilizándolos.
- Cuando el titular haya facilitado los datos personales y el tratamiento se base en el consentimiento o en un contrato, tendrá derecho a transmitir dichos datos personales y cualquier otra información que haya facilitado y que se conserve en un sistema de tratamiento automatizado a otro sistema en un formato electrónico comúnmente utilizado, sin impedimentos por parte del responsable del tratamiento de quien se retiren los datos personales.

Al respecto de todo lo anterior, el AIFA señala en su evaluación de impacto lo siguiente:

> *"VI. Cancelación o supresión de datos personales*
> *[...]*
> *Como medidas adicionales de seguridad y confidencialidad y según lo establece el Artículo 55 de la mencionada Ley,* ***en este caso el ejercicio de los derechos ARCO no sería procedente porque los datos personales no se encontrarán en posesión del responsable.***
> *[...]*
> *Una vez que se tengan figuras reales sobre los flujos de datos, el comportamiento del sistema, y* ***para garantizar los derechos ARCO de los titulares se podría analizar, validar y ampliar el período de ciclo de vida del tratamiento de los datos personales en el Sistema de Procesamiento de Pasajeros del AIFA.***
>
> ***[Énfasis añadido]***

Asimismo, en el desahogo del requerimiento de información adicional se manifestó lo siguiente:

> *"[...]*
> *Toda vez que los datos personales tratados por el encargado son encriptados, irreversibles y cifrados lo cual impide la legibilidad de los mismos aunado al hecho de que el AIFA no cuenta con la posibilidad de hacer un proceso de reversibilidad de los mismos, en virtud de que no cuenta con dichos datos de manera identificable en su repositorio* ***no puede hacer efectivas las solicitudes de los derechos ARCOP de las personas titulares dado que el responsable Operador Aeroportuario no puede identificar al titular de los mismos debido a que los datos se encuentran codificados.*** *Por lo que se vería así la información (imagen código en símbolo del sistema).*



[Énfasis añadido]

Ahora bien, en el documento denominado "Experiencia sin contacto con tecnología biométrica Gestión de Datos Personales. Solución Biométrica" se establece:

> *"1.7.3 Derechos de los interesados*
> *Dado que los datos se derivan de los sistemas y bases de datos existentes, los pasajeros pueden ejercer sus derechos en los sistemas y fuentes pertinentes."*

Como se advierte de acuerdo con lo manifestado por el AIFA se advierte que existen dos razones por las que menciona que no será procedente los derechos ARCO, sin embargo, en el documento remitido se afirma que los pasajeros pueden ejercer sus derechos en los sistemas y fuentes, existiendo contradicción entre la información.

Ahora bien, respecto al supuesto referente de la temporalidad del tratamiento -24 horas - se precisa en la evaluación de impacto que dicho tiempo inicia a partir de la "fecha de la salida del vuelo", es importante señalar que de la información y documentación remitida no se advierte que para la obtención de los datos (enrolamiento biométrico) se cuente con un límite de tiempo de antelación a de realizarse, situación que muchas veces depende de la aerolínea, y del que es evidente que se realiza con antelación al despeje del avión, por lo que la obtención se puede dar en cualquier momento que el titular lo decida y cuente con pase de abordar, situación de la que se advierte que el tratamiento de datos personales se realiza con mayor tiempo al señalado de 24 horas.

Por lo que corresponde a que los datos personales se encuentran encriptados, son irreversibles y cifrados, lo que impide la legibilidad de estos y que no puede hacer efectiva las solicitudes de derechos arco, es importante señalar que como responsable es quien decide sobre el tratamiento de datos personales ya sea directamente él o por medio de un encargado o subencargado, sin embargo, no se deslinda de sus obligaciones por lo que se debe dar cumplimiento a los principios, deberes y obligaciones establecidos en la normatividad.

Al respecto, es importante señalar En esta tesitura, es dable hacer referencia al alcance del ejercicio de **derechos ARCO**, prerrogativas reconocidas dentro del artículo 16, segundo párrafo, de la Constitución, en los términos siguientes:

> *"**Artículo 16.** ...*
> ***Toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición**, en los términos que fije la ley, **la cual establecerá los supuestos de excepción** a los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros".*
>
> ***[Énfasis añadido].***

Disposición constitucional que reconoce implícitamente el derecho a la protección de datos personales con el carácter de derecho fundamental lo que implica también, la posibilidad de que los titulares puedan hacer ejercicio de los derechos ARCO, a través de los cuales se constituyen prerrogativas para que tengan la posibilidad de acceder, rectificar, cancelar u oponerse al tratamiento de sus datos personales cuando así lo requiera, conforme a los supuestos establecidos por la Ley General y los Lineamientos Generales; por lo que es imprescindible se considere en el tratamiento que se pretende realizar.

Conforme lo anterior, se procede a realizar las siguientes recomendaciones:

Recomendaciones en torno a Derechos ARCO

Clave	Recomendaciones
AIFA_ARCO_001	Se recomienda buscar y establecer los mecanismos necesarios con la finalidad de garantizar el debido ejercicio de los derechos ARCO, a través de los procedimientos pertinentes a fin de que la persona titular no se enfrente a barreras para su ejercicio.
AIFA_ARCO_002	Se recomienda considerar en el procedimiento de ejercicio de los derechos ARCO la posibilidad de personas en estado de interdicción.
AIFA_ARCO_003	Se sugiere establecer procedimientos internos para cumplir con sus funciones y para gestionar de manera eficiente las solicitudes de derechos ARCO.
AIFA_ARCO_004	Se recomienda analizar la procedencia del derecho a la portabilidad, verifique que se ajuste a los supuestos, parámetros y procedimientos establecidos en los Lineamientos que establecen los parámetros, modalidades y procedimientos para la portabilidad de datos personales.

5. Encargado

Los artículos 3, fracciones VI y XV, 58, 59, 60, 61, 62, 63, 64 y 71 de la Ley General, 108, 109, 110, 111 y 112 de los Lineamientos generales, de los que se advierte que el encargado es una persona

física o moral, de carácter público o privado, ajena a la organización del responsable, que sola o conjuntamente con otras, trata datos personales a nombre y por cuenta de éste.

Es decir, el encargado es un prestador de servicios que realiza actividades de tratamiento de datos personales a nombre y por cuenta del responsable, como consecuencia de la existencia de una relación jurídica que lo vincula con el mismo y delimita el ámbito de su actuación en la prestación de un servicio.

En ese sentido, la figura del encargado debe cumplir con cada una de las siguientes características:

- Puede ser una persona física o moral del ámbito público o privado.
- Ser ajeno a la organización del responsable, es decir, los trabajadores que forman parte de la estructura del responsable no tienen la calidad de encargados.
- Puede tratar los datos personales solo o en conjunto con otras personas.
- Se vincula con el responsable a través de una relación jurídica que delimita el ámbito de su actuación.
- No ostenta poder de decisión sobre el tratamiento de los datos personales que efectúe, sino que en virtud de la relación jurídica que lo vincula con el responsable se limita a tratarlos a nombre y por cuenta de este último, siguiendo expresamente sus instrucciones.

En otras palabras, el encargado actualiza una especie de delegación de funciones en el tratamiento de los datos personales que lleve a cabo, acotando su actuación a las instrucciones dadas por el responsable y sin ostentar poder alguno de decisión sobre el alcance y contenido del tratamiento.

En este sentido, el responsable está obligado a formalizar con el encargado la prestación de sus servicios a través de la suscripción de un contrato o cualquier otro instrumento jurídico de conformidad con la normatividad que le resulte aplicable, considerando, al menos, las siguientes cláusulas relacionadas con los servicios contratados:

- Realizar el tratamiento de los datos personales conforme a las instrucciones del responsable.
- Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por el responsable.
- Implementar las medidas de seguridad conforme a la Ley General, los Lineamientos generales y demás instrumentos jurídicos aplicables.
- Informar al responsable cuando ocurra una vulneración a los datos personales que trata por sus instrucciones.
- Guardar confidencialidad respecto de los datos personales tratados.
- Suprimir o devolver los datos personales, objeto de tratamiento, una vez cumplida la prestación de servicios con el responsable, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales.

- Abstenerse de transferir los datos personales salvo en el caso de que el responsable así lo determine o la comunicación derive de una subcontratación o por mandato expreso de la autoridad competente.
- Permitir al Instituto o al responsable realizar verificaciones en el lugar o establecimiento donde lleva a cabo el tratamiento de los datos personales.
- Colaborar con el Instituto en las investigaciones previas y verificaciones que lleve a cabo, en términos de lo dispuesto en la Ley General, los Lineamientos generales y demás normatividad aplicable.
- Generar, actualizar y conservar la documentación necesaria que le permita acreditar el cumplimiento de sus obligaciones.

Asimismo, el responsable está obligado a autorizar expresamente la subcontratación de servicios que involucren el tratamiento de datos personales, ya sea en el propio contrato o instrumento jurídico que suscriba con el prestador de servicios o encargado, o bien, de manera previa a la contratación.

Cuando la subcontratación de servicios sea autorizada por el responsable, el encargado está obligado a formalizar ésta a través de la suscripción de un contrato o cualquier otro instrumento jurídico que determine el encargado, el cual debe contener, al menos, las cláusulas previstas para la formalización de la prestación de servicios entre el responsable y el encargado.

En caso de que el encargado incumpla las instrucciones del responsable y decida por sí mismo sobre los fines, medios y demás cuestiones relacionadas con el tratamiento de datos personales instruido por el responsable, asumirá el carácter de responsable conforme a la legislación que le resulte aplicable en función de que su naturaleza sea pública o privada.

El responsable está obligado, en su caso, a contratar o adherirse a aquellos servicios de cómputo en la nube y otras materias, entendidos como modelos de provisión externa de servicios de cómputo bajo demanda que implica el suministro de infraestructura, plataforma o programa informático, distribuido de modo flexible mediante procedimientos virtuales en recursos compartidos dinámicamente, que garanticen políticas de protección de datos personales equivalentes a los principios y deberes establecidos en la Ley General, los Lineamientos generales y demás normatividad derivada.

Los proveedores de servicios de cómputo en la nube y otras materias tienen la calidad de encargados, por lo cual, si el responsable tiene la posibilidad de convenir con el proveedor las condiciones y términos de este tipo de servicios a través de la suscripción de un contrato o instrumento jurídico específico, éste debe prever, al menos, las cláusulas generales señaladas en

los artículos 59 de la Ley General y 109 de los Lineamientos generales, obligación que no exime al responsable de observar lo siguiente:

- Que el servicio de cómputo en la nube o de otras materias cumpla, al menos, con:
  - Tener y aplicar políticas de protección de datos personales afines a los principios y deberes aplicables que establece la Ley General, los Lineamientos generales y demás normativa aplicable.
  - Transparentar las subcontrataciones que involucren los datos personales sobre los que se preste el servicio.
  - Abstenerse de incluir condiciones en la prestación del servicio que le autoricen o permitan asumir la titularidad o propiedad de los datos personales sobre los que se preste el servicio.
  - Guardar confidencialidad respecto de los datos personales sobre los que se preste el servicio.
- Que los servicios de cómputo en la nube o de otras materias cuenten con mecanismos, al menos, para:
  - Dar a conocer cambios en sus políticas de privacidad o condiciones del servicio que se preste.
  - Permitir al responsable limitar el tipo de tratamiento de los datos personales sobre los que se preste el servicio.
  - Establecer y mantener medidas de seguridad para la protección de los datos personales sobre los que se preste el servicio.
  - Garantizar la supresión de los datos personales una vez que hubiere concluido el servicio prestado al responsable y que este último haya podido recuperarlos.
  - Impedir el acceso a los datos personales a personas que no cuenten con privilegios de acceso, o bien, en caso de que sea a solicitud fundada y motivada de autoridad competente informar sobre tal situación al responsable.

En caso contrario, el responsable sólo está obligado a observar las reglas previstas en los artículos 59 de la Ley General y 109 de los Lineamientos generales.

Respecto a esta figura, conforme a la información proporcionada por el AIFA en la respuesta al requerimiento de información adicional, señaló lo siguiente:

> *"...A este respecto el día 12 de enero del año en curso la empresa estatal de participación estatal mayoritaria Aeropuerto Internacional Felipe Ángeles S.A de C.V., (AIFA, S.A. de C.V.) entregó a la H. Dirección General a su cargo el documento denominado instrumento jurídico en materia de tratamiento y protección de datos personales del sistema de procesamiento de pasajeros celebrado entre el responsable jurídico (agto. Ings. "Felipe ángeles"), el responsable de operación aeroportuaria (AIFA, S.A. DE C.V.) y el encargado (consorcio Apollo Communications S.A. de C.V.), cuya justificación de conformidad a lo establecido en los art. 58, 59, 60, 61, 62, 63 y 64 de la LGPDPPSO y 108 de los lineamientos generales, los*

cuales expresan que la relación entre el responsable y el encargado deberá estar formalizada mediante contrato o cualquier otro instrumento jurídico que le vincula con el mismo y delimita el ámbito de su actuación para la prestación de un servicio.

[...]

6. Con fundamento en el artículo 3, fracción XV, XXVII, XXXII, articulo 65 al 71 de Ley General de Datos y articulo 15, fracción X y fracción XV de las Disposiciones administrativas, se solicita definir claramente las figuras de los actores involucrados como son: responsable, encargado y en su caso subencargado que participan en el tratamiento de datos personales objeto de esta Evaluación de impacto, así como definir, los procesos, motivos y procedimientos establecidos por los cuales desempeñarán la figura correspondiente, en su caso, y la forma de obtener los datos personales, es decir, si el AIFA tratará los datos directamente del titular o serán recabados de algún medio diferente, así como las fuentes de su obtención, es decir, de manera directamente de este (cuando el responsable obtiene directamente del titular los datos personales cuando este los proporciona por algún medio que permita su entrega directa: medios electrónicos, ópticos, sonoros, visuales, vía telefónica, internet o cualquier otra tecnología y/o medio) o indirectamente de este (cuando no se obtienen de la forma descrita previamente), de conformidad con el artículo 18 y 19 de los lineamientos generales.

Las figuras de los actores involucrados son las siguientes:

Responsable de Operación Aeroportuaria (Subdir. Sist. AIFA, S.A. de C.V.) proceso Supervisión de Cumplimiento.

Responsable jurídico. Agrupamiento de Ingenieros

Encargado: Consorcio Apollocom, AMADEUS, Vision-Box S.A. de C.V.

En relación al artículo 3 Fracción XV el responsable es el AIFA identificando como encargado del tratamiento de los datos personales al consorcio Apollocom, AMADEUS, Vision-Box S.A. de C.V., fracción XXVII, de quienes se define el nivel de responsabilidad comunicación y remisión es realizada exclusivamente entre el responsable y el encargado dentro del AIFA.

El encargado será el responsable del tratamiento de los datos personales, por lo que es este quien recibe directamente del titular dicha información.

Definiéndolos como responsables de realizar los procesos y procedimientos de almacenamiento y procesamiento de los datos, soporte en sitio, encargados de atender las fallas en relación con el Hardware y Software del "Sistema de Procesamiento de Pasajeros", con motivo de mantener la funcionalidad del sistema operativo 24/7/365.

Con fundamento en el Art. 65 se obtendrá el consentimiento expreso del titular a través de los avisos de privacidad que se darán a conocer por medio de los 3 puntos de enrolamiento del sistema.

[...]

Toda vez que los datos personales ***tratados por el encargado son encriptados****, irreversibles y cifrados lo cual impide la legibilidad de los mismos aunado al hecho de que el AIFA no cuenta con la posibilidad de hacer un proceso de reversibilidad de los mismos, en virtud de que no cuenta con dichos datos de manera identificable en su repositorio no puede hacer efectivas las solicitudes de los derechos ARCOP de las Página 35 de 44 personas*

titulares dado que el responsable Operador Aeroportuario no puede identificar al titular de los mismos debido a que los datos se encuentran codificados. Por lo que se vería así la información (imagen código en símbolo del sistema)
[…]
Se adjunta en el Anexo 4 el instrumento jurídico en materia de Tratamiento y Protección de Datos Personales del Sistema de Procesamiento de Pasajeros celebrado entre el responsable jurídico (Agto. Ings. "Felipe Ángeles"), el responsable de operación aeroportuaria (AIFA, S.A. de C.V.) y el encargado (consorcio Apollo Communications S.A. de C.V.),
[…]
De conformidad a la cláusula vigesimosegunda del instrumento jurídico en materia de tratamiento y protección de datos personales del sistema de procesamiento de pasajeros celebrado entre el responsable jurídico (agto. Ings. "Felipe ángeles"), el responsable de operación aeroportuaria (AIFA, S.A. DE C.V.) y el encargado (consorcio Apollo Communications S.A. de C.V.), (ver Anexo 4)…"
[…]

Asimismo, como parte de los Anexos, se contempla el documento "Definición de figuras de los actores involucrados: Responsable, Encargado y Subencargado" del cual se desprende:
"[…] Responsable: Aeropuerto Internacional Felipe Ángeles (AIFA).
Perfil 1: Supervisión de Cumplimiento.
Evaluar y dirigir las actividades de planeación, desarrollo y soporte de los recursos tecnológicos, informáticos y de redes.
Supervisar y mantener integrado y articulado el equipo humano del área, a fin de alcanzar el cumplimiento de sus objetivos operativos y estratégicos.
- *Coordinador de Desarrollo*
- *Coordinador de Controles de TI y Mesa de Servicios*
- *1 Analista Técnico*

[…]
Encargado: almacenamiento y procesamiento de los datos
Empresa Vision-Box Soluções de Visão Por Computador S.A., Vision Box:
[…]
Subencargardo:
Empresa Apollo Communications: ingenieros de soporte en sitio, encargados de atender las fallas en relación con el hardware del "Sistema de Procesamiento de Pasajeros"
[…]
Amadeus IT Group, S.A.: ingenieros de soporte remoto encargados de atender las fallas en relación con el sistema ACUS y APV de AMADEUS del "Sistema de Procesamiento de Pasajeros"
[…]"

Por lo que, derivado de lo anterior, se advierte que conforme a la información proporcionada por parte del AIFA, con relación a las partes que intervienen en proceso que nos ocupa, efectivamente se puede a apreciar que nos encontramos ante las figuras de responsable y encargado e inclusive subencargados del tratamiento de los datos personales de las y los titulares, a lo cual se señala que:

Responsable: AIFA.-
Encargado: Vision Box
Subencargados: Apollo Communications y *Amadeus*.

Bajo este contexto, no se debe de perder de vista que, con base en la normatividad en materia de protección de datos personales, el encargado es un prestador de servicios que realiza actividades de tratamiento de datos personales a nombre y por cuenta del responsable, como consecuencia de la existencia de una relación jurídica que lo vincula con el mismo y delimita el ámbito de su actuación en la prestación de un servicio.

Por su parte, el encargado podrá, a su vez, subcontratar servicios que impliquen el tratamiento de datos personales por cuenta del responsable, siempre y cuando medie la autorización expresa de este último.

El subcontratado asumirá el carácter de encargado en los términos de la Ley y demás disposiciones que resulten aplicables en la materia.

Cuando el contrato o el instrumento jurídico mediante el cual se haya formalizado la relación entre el responsable y el encargado prevea que este último pueda llevar a cabo a su vez las subcontrataciones de servicios, la autorización se entenderá como otorgada a través de lo estipulado en éstos.

Por lo que, vez obtenida la autorización expresa del responsable, el encargado deberá formalizar la relación adquirida con el subcontratado a través de un contrato o cualquier otro instrumento jurídico que decida, de conformidad con la normatividad que le resulte aplicable, y permita acreditar la existencia, alcance y contenido de la prestación del servicio en términos de Ley

Bajo este supuesto, con independencia de lo señalado en el principio de licitud, en cuanto al carácter de responsable se trata, se puede advertir que conforme a las documentales presentadas por parte del AIFA, no se tienen perfectamente definidas las figuras mediante las cuales se efectuara el tratamiento de los datos personales de las y los titulares.

Para lo cual podemos observar que si bien se cuenta con un instrumento jurídico en materia de Tratamiento y Protección de Datos Personales del Sistema de Procesamiento de Pasajeros celebrado entre el responsable jurídico (Agto. Ings. "Felipe Ángeles"), el responsable de operación aeroportuaria (AIFA, S.A. de C.V.) y el encargado (consorcio Apollo Communications S.A. de C.V.), también lo es que esto no corresponde con lo señalado por parte del AIFA en cuanto a las figuras que se señalan ya que en una primera instancia se le señala como encargado y con posterioridad como sub encargado.

No obstante lo anterior, se tiene que precisar que conforme a la información respectiva en el caso de que Apollo Comunications tenga el carácter de Encargado, conforme a la normatividad aplicable en materia de protección de datos personales, seria este el que a su vez debería de suscribir el instrumento jurídico respectivo con los subencargados los cuales serían AMADEUS, Vision-Box S.A. de C.V. o en su caso si el encargado lo es Vision Box, este sería quien debería de subcontratar a AMADEUS y Apollo o viceversa.

Mas, sin embargo, derivado del análisis que se pretende y de acuerdo al tratamiento de los datos personales el AIFA como responsable, eventualmente tendría que contar con los instrumentos jurídicos necesarios tanto con Consorcio Apollocom, AMADEUS y Vision-Box S.A. de C.V. en términos de la normatividad de protección de datos personales, ya que estos ostentarían el carácter de encargados ya que estos se encuentran prestando servicios que realizan actividades de tratamiento de datos personales a nombre y por cuenta del responsable.

Ahora bien, de igual manera se advierte que durante el proceso también se contempla la participación por parte de las aerolíneas en el enrolamiento directo y a su vez recibirán información a través de los diversos sistemas a efecto de conocer los estatus de los resultados obtenidos, por lo que de igual manera, no se advierte que se tenga perfectamente definido el carácter con el cual se ostentarían las mismas, ni mucho menos que se cuente con los instrumentos jurídicos necesarios en los cuales se garantice su posible calidad de encargadas del tratamiento de los datos personales.

Tomando en consideración lo anterior, se emiten las siguientes recomendaciones:

Recomendaciones en torno a relación responsable y encargado

Clave	Recomendación
AIFA_EN_001	Se recomienda definir conforme a la normatividad aplicable en materia de protección de datos personales las figuras que ostentan aquellos que intervienen en el tratamiento de los datos personales, conforme a su carácter de responsable, encargado o inclusive sub encargado, esto a efecto de que se

	garantice la seguridad mediante las cual se efectuara dicho tratamiento, para lo cual de igual manera una vez definidas estas figuras se puedan contar con los instrumentos jurídicos entre los diversos actores ya sea en términos de la Ley General cuando estas figuran se encuentren intrínsecamente ligadas por parte del AIFA, o cuando se vinculen entre empresas del sector privado conforme a lo estipulado en la normatividad para este sector, siendo la LFPDPPP.
AIFA_EN_002	Se recomienda observar el cumplimiento de las obligaciones en materia de datos personales relacionadas con la relación responsable-encargado e inclusive sub-encargado, en los convenios u otros instrumentos jurídicos, estableciendo cláusulas con las siguientes obligaciones del encargado: o Realizar el tratamiento de los datos personales conforme a las instrucciones del responsable; o Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por el responsable; o Implementar las medidas de seguridad conforme a los instrumentos jurídicos aplicables; o Informar al responsable cuando ocurra una vulneración a los datos personales que trata por sus instrucciones; o Guardar confidencialidad respecto de los datos personales tratados; o Suprimir o devolver los datos personales objeto de tratamiento una vez cumplida la relación jurídica con el responsable, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales; o Abstenerse de transferir los datos personales salvo en el caso de que el responsable así lo determine, o la comunicación derive de una subcontratación, o por mandato expreso de la autoridad competente; o Permitir al INAI o al responsable realizar verificaciones en el lugar o establecimiento donde lleva a cabo el tratamiento de los datos personales; o Colaborar con el INAI en las investigaciones previas y verificaciones que lleve a cabo en términos de lo dispuesto en la LGPDPPSO y los Lineamientos Generales, proporcionando la información y documentación que se estime necesaria para tal efecto, y o Generar, actualizar y conservar la documentación necesaria que le permita acreditar el cumplimiento de sus obligaciones.
AIFA_EN_003	Se recomienda establecer mecanismos para verificar que las empresas que prestan servicios de cómputo en la nube cumplen con sus obligaciones en torno

	al tratamiento de datos personales establecidas en el Contrato de servicios que fue compartido y documentar cualquier incumplimiento.

6. Cómputo en la nube

Es importante precisar que, la Ley General, destaca en su artículo 63, lo relacionado a la contratación de servicios de cómputo en la nube, para lo cual al efecto refiere lo siguiente:

> ***Artículo 63.*** *El responsable podrá contratar o adherirse a servicios, aplicaciones e infraestructura en el cómputo en la nube, y otras materias que impliquen el tratamiento de datos personales, siempre y cuando el proveedor externo garantice políticas de protección de datos personales equivalentes a los principios y deberes establecidos en la presente Ley y demás disposiciones que resulten aplicables en la materia. En su caso, el responsable deberá delimitar el tratamiento de los datos personales por parte del proveedor externo a través de cláusulas contractuales u otros instrumentos jurídicos.*

Disposición normativa de la que es posible advertir que, el responsable podrá contratar o adherirse a servicios, aplicaciones e infraestructura en el cómputo en la nube, y otras materias que impliquen el tratamiento de datos personales, siempre y cuando el proveedor externo garantice al responsable políticas de protección de datos personales equivalentes a los principios y deberes establecidos en la Ley General y demás disposiciones que resulten aplicables en la materia. Estableciendo además que, de ser aplicable, el responsable deberá delimitar el tratamiento de los datos personales por parte del proveedor externo a través de cláusulas contractuales u otros instrumentos jurídicos.

Por su parte el artículo 64 de la citada Ley General, refiere que para que se realice el tratamiento de datos personales en cómputo en la nube, en los que el responsable se adhiera a los mismos mediante condiciones o cláusulas generales de contratación, sólo podrá utilizar aquellos servicios en los que el proveedor:

I. Cumpla, al menos, con lo siguiente:

a) Tener y aplicar políticas de protección de datos personales afines a los principios y deberes aplicables que establece la Ley General y demás normativa aplicable;
b) Transparentar las subcontrataciones que involucren la información sobre la que se presta el servicio;
c) Abstenerse de incluir condiciones en la prestación del servicio que le autoricen o permitan asumir la titularidad o propiedad de la información sobre la que preste el servicio, y
d) Guardar confidencialidad respecto de los datos personales sobre los que se preste el servicio;

II. Cuente con mecanismos, al menos, para:

a) Dar a conocer cambios en sus políticas de privacidad o condiciones del servicio que presta;
b) Permitir al responsable limitar el tipo de tratamiento de los datos personales sobre los que se presta el servicio;
c) Establecer y mantener medidas de seguridad para la protección de los datos personales sobre los que se preste el servicio;
d) Garantizar la supresión de los datos personales una vez que haya concluido el servicio prestado al responsable y que este último haya podido recuperarlos, y
e) Impedir el acceso a los datos personales a personas que no cuenten con privilegios de acceso, o bien, en caso de que sea a solicitud fundada y motivada de autoridad competente, informar de ese hecho al responsable.

Aunado a lo anterior, dicho artículo refiere que, en cualquier caso, el responsable no podrá adherirse a servicios que no garanticen la debida protección de los datos personales, conforme a la Ley General y demás normatividad que resulte aplicables en la materia.

Así mismo, el artículo 111 de los Lineamientos Generales, refiere que en caso de que en la contratación de servicios de cómputo en la nube y otras materias el responsable tenga la posibilidad de convenir con el proveedor las condiciones y términos de este tipo de servicios que impliquen un tratamiento de los datos personales, en el contrato o instrumento jurídico que suscriban se deberán prever, al menos, las cláusulas generales a que se refieren los artículos 59 de la Ley General y 109 de los Lineamientos Generales, sin menoscabo de lo establecido en los artículos 63 y 64 de la Ley General.

Para mayor referencia se colocan de manera textual los artículos 59 de la Ley General y 109 de los Lineamientos generales, de acuerdo con lo siguiente:

Ley General

Artículo 59. *La relación entre el responsable y el encargado deberá estar formalizada mediante contrato o cualquier otro instrumento jurídico que decida el responsable, de conformidad con la normativa que le resulte aplicable, y que permita acreditar su existencia, alcance y contenido.*

En el contrato o instrumento jurídico que decida el responsable se deberán prever, al menos, las siguientes cláusulas generales relacionadas con los servicios que preste el encargado:

I. Realizar el tratamiento de los datos personales conforme a las instrucciones del responsable;

II. Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por el responsable; III. Implementar las medidas de seguridad conforme a los instrumentos jurídicos aplicables;

IV. Informar al responsable cuando ocurra una vulneración a los datos personales que trata por sus instrucciones;
V. Guardar confidencialidad respecto de los datos personales tratados;
VI. Suprimir o devolver los datos personales objeto de tratamiento una vez cumplida la relación jurídica con el responsable, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales, y
VII. Abstenerse de transferir los datos personales salvo en el caso de que el responsable así lo determine, o la comunicación derive de una subcontratación, o por mandato expreso de la autoridad competente. Los acuerdos entre el responsable y el encargado relacionados con el tratamiento de datos personales no deberán contravenir la presente Ley y demás disposiciones aplicables, así como lo establecido en el aviso de privacidad correspondiente.
[…]

Lineamientos generales
Formalización de la prestación de servicios del encargado
Artículo 109. *Además de las cláusulas generales señaladas en el artículo 59 de la Ley General para la prestación de los servicios del encargado, el responsable deberá prever en el contrato o instrumento jurídico a que se refiere el párrafo anterior del presente artículo las siguientes obligaciones:*
I. Permitir al Instituto o al responsable realizar verificaciones en el lugar o establecimiento donde lleva a cabo el tratamiento de los datos personales;
II. Colaborar con el Instituto en las investigaciones previas y verificaciones que lleve a cabo en términos de lo dispuesto en la Ley General y los presentes Lineamientos generales, proporcionando la información y documentación que se estime necesaria para tal efecto, y
III. Generar, actualizar y conservar la documentación necesaria que le permita acreditar el cumplimiento de sus obligaciones.
[…]"

[Énfasis añadido]

En cualquier caso, el responsable no podrá adherirse a servicios que no garanticen la debida protección de los datos personales, conforme a la Ley General y demás disposiciones que resulten aplicables en la materia.

Por lo anterior, es posible señalar que el responsable está obligado a establecer la relación con el encargado a través de un instrumento jurídico que permita acreditar la existencia de la relación jurídica, su alcance y contenido, como por ejemplo un contrato, cláusulas contractuales, acuerdos, convenios u otros instrumentos jurídicos. En todo caso, los acuerdos que se alcancen entre el responsable y el encargado deberán ser acordes con lo previsto en el aviso de privacidad.

En este contexto, tal y como ya se refirió, los artículos 17 de la Ley General y 8 de los Lineamientos Generales, señalan que, el responsable deberá tratar los datos personales que posea sujetándose

a las atribuciones o facultades que la normatividad aplicable le confiera, respetando los derechos y libertades de los titulares.

Por tal motivo, el responsable y el encargado determinarán libremente cuales son las obligaciones y compromisos que tomen en cuanto a la contratación para el tratamiento de datos personales, en congruencia con las disposiciones previamente establecidas.

Es preciso mencionar que, los sujetos obligados son los responsables de la seguridad del contenido que almacenan o procesan utilizando los servicios de cómputo en la nube que elijan. Lo anterior, teniendo en cuenta que los sujetos obligados son quienes determinan qué contenido almacenan o procesan utilizando estos servicios y el nivel de seguridad que dicho contenido requiere, conforme al análisis de riesgos que lleven a cabo. Corresponde a los sujetos obligados administrar de manera segura el servicio, de acuerdo con los controles que implementen y las herramientas que les suministre el proveedor de servicios de cómputo en la nube.

Al respecto en el instrumento jurídico en materia de tratamiento y protección de datos personales del sistema de procesamiento de pasajeros celebrado el 15 de diciembre de 2021, la SEDENA, el AIFA, y las empresas Apollo Communications, S.A. de C.V., Química Apollo S.A de C.V., Vision-Box Soluções de Visão Por Computador S.A., y Amadeus IT Croup, S.A., y que fue remitido como anexo de la evaluación de impacto, se señala en la cláusula Novena lo siguiente:

> *"[…]*
> *Novena. En el caso de que los servicios del encargado estén contratados o adheridos a los servicios aplicaciones e infraestructura en el cómputo en la nube, el responsable de operación aeroportuaria debe garantizar que, en el tratamiento de datos personales, el encargado garantice políticas de protección de datos personales en términos de la legislación mexicana. Y aunado a lo anterior el encargado deberá acreditar fehacientemente a través de documentos legales que:*
> *a) Aplica políticas de protección de datos personales afines a los principios y deberes de la LGPDPPSO y/o la Ley Federal de Protección de Datos Personales en Posesión de Particulares;*
> *b) Transparenta las subcontrataciones que involucren la información relativa al servicio que brinda al responsable de operación aeroportuaria;*
> *c) Abstenerse de incluir condiciones que le autoricen la titularidad o propiedad de cualquier información de los datos personales sobre la que encuentre el servicio al subcontratado;*
> *d) La confidencialidad que debe guardar con respecto de los datos personales sobre los que prese el servicio;*
> *e) Dar a conocer sus políticas de privacidad;*
> *f) Tener la posibilidad de limitar el tratamiento de los datos personales de la prestación del servicio en caso de que el responsable lo requiera;*
> *g) Establecer las medidas de seguridad para la protección de los datos personales*

h) Garantizar la supresión de los datos personales una vez que hay concluido el servicio prestado al responsable.

Al respecto, se advierte que, en el caso de que los servicios del encargado estén contratados o adheridos a los servicios aplicaciones e infraestructura en el cómputo en la nube, el responsable de operación aeroportuaria debe garantizar que, en el tratamiento de datos personales, el encargado garantice políticas de protección de datos personales en términos de la legislación mexicana.

Por su parte, es importante señalar que en los Anexos denominados Apollo anexo A des. tec. pag. 1-30 e ITP-043-02 Apollo Anexo A pag. 75-114, se advirtió lo siguiente:

*"**3.4 Sistema de Procesamiento de Pasajeros de Uso Común (CUPPS)***
Descripción. El Sistema de Procesamiento de Pasajeros de Uso Común (CUPPS) proporciona un medio centralizado para brindar servicios asistidos a pasajeros en un entorno común para las aerolíneas en el Aeropuerto
*Amadeus ha desarrollado el servicio de procesamiento de pasajeros de uso común de próxima generación. **Este nuevo enfoque para la infraestructura de uso compartido se llama Amadeus Airport Cloud Use Services (ACUS).***
ACUS ofrece una solución resistente, escalable y rentable que se aloja de forma centralizada y a la que se accede de forma segura a través de cualquier conexión de red."

"¿Por qué Amadeus?
Repositorio de datos rico en contenido que contiene información operacional, de demanda y de programación con hasta 365 días de anticipación
***Opción para trasladar las operaciones a la nube,** lo que resulta en una reducción de los costos de mantenimiento de TI y la huella ambiental, así como una fácil integración e implementaci6n en varios aeropuertos".*

[Énfasis añadido]

Al respecto en el documento denominado ITP-043-02 Apollo Anexo A pag. 31-74, se documenta lo siguiente:

"AMADEUS tiene la capacidad de proporcionar un servicio completo de integración para las aplicaciones de las aerolíneas, que incluye lo siguiente:
...
Opcional: Alojamiento de la Aplicación de la Linea Aérea en la "Nube" - sin gasto de capital para el hardware del servidor, fácilmente re-desplegable en otros puertos, carga escalable a través de Elastic Cross Load Balancers, Red de Alta Disponibilidad."

De lo antes expuesto, se observa que el servicio de Amadeus tiene la capacidad de ofrecer alojamiento de la aplicación de la línea aérea en la "nube" y trasladar las operaciones a la misma.

Asimismo, establece que el servicio de procesamiento de pasajeros de uso común de próxima generación, desarrollado por Amadeus, cuenta con un nuevo enfoque para la infraestructura de uso compartido se llama Amadeus Airport Cloud Use Services (ACUS).

Por lo anterior y retomando lo establecido en el apartado "IV. Descripción del Sistema de Procesamiento de Pasajeros del AIFA, contexto y justificación de la evaluación de impacto", se advierten indicios de que los servicios de Amadeus se tratan de una solución basada en cómputo en la nube, esto considerando que el tratamiento de datos personales realizado no se efectúa en equipos del AIFA sino de las empresas Amadeus y Apollo, salvo el resguardo del PDE, que, conforme a lo expuesto en la evaluación de impacto, se almacena en los servidores del AIFA.

Al respecto, es oportuno considerar, a manera de estricta referencia, que este Instituto emitió la Guía breve para sujetos obligados para la contratación de servicios de cómputo en la nube que impliquen el tratamiento de datos personales[58], en la que se estableció que constituyen modalidades de cómputo en la nube las siguientes:

- Infraestructura como Servicio (Infrastructure as a Service o IaaS): La infraestructura como servicio, contiene los bloques de creación fundamentales para la Tecnología de la Información (TI) en la nube. Por lo general, permite acceder a las características de conexión en red, a los equipos (virtuales o en software dedicado) y al espacio de almacenamiento de datos. La infraestructura como servicio le ofrece el mayor nivel de flexibilidad y control de la administración en torno a sus recursos de TI y guarda el mayor parecido con los recursos de TI existentes con los que muchos departamentos de TI y desarrolladores están familiarizados.
- Plataforma como Servicio (Platform as a Service o PaaS): Las plataformas como servicio eliminan la necesidad de las organizaciones de administrar la infraestructura subyacente (normalmente hardware y sistemas operativos) y le permiten centrarse en la implementación y la administración de sus aplicaciones. Esto contribuye a mejorar su eficacia, pues no tienen que preocuparse del aprovisionamiento de recursos, la planificación de la capacidad, el mantenimiento de software, los parches ni ninguna de las demás arduas tareas que conlleva la ejecución de su aplicación.
- Software como Servicio (Software as a Service o SaaS): El software como servicio les proporciona a los clientes un producto completo que el proveedor externo de servicios de nube ejecuta y administra. En la mayoría de los casos, quienes hablan de software como servicio en realidad se refieren a aplicaciones de usuario final. Con una oferta de SaaS, el cliente no tiene que pensar en cómo se mantiene el servicio ni en cómo se administra la infraestructura subyacente. Solo debe preocuparse por cómo utilizar ese sistema de software concreto. Un ejemplo común de una aplicación SaaS es un programa de correo electrónico basado en la

[58] Disponible para su consulta en el siguiente vínculo: https://home.inai.org.mx/wp-content/uploads/Guia_SO_CC.pdf, consultado por última vez el 28/02/2023.

web que le permite enviar y recibir mensajes sin tener que administrar la incorporación de características ni mantener los servidores y los sistemas operativos en los que se ejecuta, por ejemplo, el programa de correo electrónico. Con el tiempo se han agregado distintas denominaciones que usualmente vemos identificadas como XaaS (X como Servicio), que se refieren a casos de servicios especializados que en realidad utilizan uno de los tres modelos fundamentales, en su mayor parte SaaS. Independiente del modelo de que se trate, el PSN puede implementar protocolos de encriptación para proteger la diseminación de información en la red.

- Por otro lado, para el despliegue de la plataforma de nube se pueden adoptar varios modelos, a saber: Nube Pública, Nube Privada, Nube Comunitaria y Nube Híbrida, aunado a que se recomienda utilizar el concepto completo al que se refiere: Modelos de implementación. Y detallar un poco sobre los cuatro tipos de modelos de implementación o de despliegue y mejorar la calidad de la imagen y utilizar una que ejemplifique todos los modelos de computación en la nube contemplados en el documento Special Publication 800-146 de NIST.

Considerando que en muchos casos los proveedores externos de servicios de nube cuentan con términos y condiciones que se tratan de contratos de adhesión, es que en los artículos 63 y 64 de la Ley General, y 111 de los Lineamientos, se prevé lo siguiente:

- Que el responsable podrá contratar o adherirse a servicios, aplicaciones e infraestructura en el cómputo en la nube, y otras materias que impliquen el tratamiento de datos personales, siempre y cuando el proveedor externo garantice políticas de protección de datos personales equivalentes a los principios y deberes establecidos en la Ley General y demás disposiciones.
- Que, en su caso, el responsable deberá delimitar el tratamiento de los datos personales por parte del proveedor externo a través de cláusulas contractuales u otros instrumentos jurídicos.
- Que para el tratamiento de datos personales en servicios, aplicaciones e infraestructura de cómputo en la nube y otras materias, en los que el responsable se adhiera a los mismos mediante condiciones o cláusulas generales de contratación, sólo podrá utilizar aquellos servicios en los que el proveedor cumpla, al menos, con lo siguiente: Tener y aplicar políticas de protección de datos personales afines a los principios y deberes aplicables que establece la presente Ley y demás normativa aplicable; Transparentar las subcontrataciones que involucren la información sobre la que se presta el servicio; Abstenerse de incluir condiciones en la prestación del servicio que le autoricen o permitan asumir la titularidad o propiedad de la información sobre la que preste el servicio, y Guardar confidencialidad respecto de los datos personales sobre los que se preste el servicio.
- También debe asegurarse de que el proveedor externo de servicios de cómputo en la nube contar con mecanismos, al menos, para: Dar a conocer cambios en sus políticas de privacidad o condiciones del servicio que presta; permitir al responsable limitar el tipo de tratamiento de los datos personales sobre los que se presta el servicio; establecer y mantener medidas de

seguridad para la protección de los datos personales sobre los que se preste el servicio; garantizar la supresión de los datos personales una vez que haya concluido el servicio prestado al responsable y que este último haya podido recuperarlos, e impedir el acceso a los datos personales a personas que no cuenten con privilegios de acceso, o bien, en caso de que sea a solicitud fundada y motivada de autoridad competente, informar de ese hecho al responsable.

- Que, en cualquier caso, el responsable no podrá adherirse a servicios que no garanticen la debida protección de los datos personales.
- Que en caso de que, en la contratación de servicios de cómputo en la nube y otras materias, el responsable tenga la posibilidad de convenir con el proveedor las condiciones y términos de este tipo de servicios que impliquen un tratamiento de los datos personales, en el contrato o instrumento jurídico que suscriban se deberán prever al menos, las cláusulas generales a que se refieren los artículos 59 de la Ley General y 109 de los presentes Lineamientos, relacionadas con la figura del encargado.
-

En ese sentido, este Instituto no advirtió de los documentos remitidos por el AIFA, que se diera cumplimiento a lo establecido en los artículos precedentes, pues únicamente se acompañó el contrato celebrado y el instrumento jurídico con el cual pretendieron dar cumplimiento a lo establecido en los preceptos legales antes señalados, en los que la SEDENA fue quien adquirió el Sistema de Procesamiento. Sin que ello demuestre el cabal cumplimiento a lo expuesto previamente.

Lo anterior es relevante, ya que en el artículo 64, último párrafo, de la Ley General, se establece la prohibición de que el responsable no podrá adherirse a servicios que no garanticen la debida protección de los datos personales; y el no acatar esa disposición podría ser motivo de incumplimiento a los principios y deberes en la materia.

En este contexto, se emiten las siguientes recomendaciones:

Recomendaciones en torno cómputo en la nube:

Clave	Recomendaciones
AIFA_CN_001	Se recomienda solicitar al proveedor de servicios sus Términos y condiciones que rigen el tratamiento del contenido, para asegurarse que el responsable tiene el control completo del contenido; que le permita cumplir con los principios y deberes aplicables que establece la Ley General y demás normatividad que resulte aplicable. En este sentido, resulta recomendable verificar que, dentro de dichos términos y

Clave	Recomendaciones
	condiciones, se permita al responsable limitar el tipo de tratamiento de los datos personales.
AIFA_CN_002	Se recomienda verificar que los proveedores de servicios sean transparentes sobre los subcontratados que utilizan para procesar la información sobre la que prestan los servicios.
AIFA_CN_003	Se recomienda que los Términos y condiciones del proveedor de servicios, no incluyan condiciones en la prestación del servicio que le autoricen o permitan asumir la titularidad o propiedad de la información sobre la que preste el servicio.
AIFA_CN_004	Se recomienda verificar que el proveedor de servicios implemente estándares de seguridad apropiadas en los servicios que los responsables utilizan para los datos personales.
AIFA_CN_005	Se recomienda verificar en los términos y condiciones u otros mecanismos del proveedor de servicios, la forma en la que el responsable podrá conocer de cambios o modificaciones de los términos o condiciones del proveedor
AIFA_CN_006	Se recomienda verificar que el proveedor de servicios permita al responsable eliminar su contenido bajo demanda. Esto tomando en consideración que, los responsables deberán de proceder a la supresión y eliminación de los datos personales sujetos a tratamiento, una vez concluida su finalidad.
AIFA_CN_007	Se recomienda verificar que el proveedor de servicios proporcione al responsable herramientas para controlar el acceso a su contenido en la nube, incluyendo datos personales.

7. Transferencias

Los artículos 3, fracción XXXII, 65, 66, 67, 68, 69 y 70 de la Ley General, 113, 114, 115 y 116 de los Lineamientos generales, que disponen que toda comunicación de datos personales sea nacional o internacional, realizada a persona distinta del responsable, encargado y titular se denomina transferencia.

En este sentido, toda transferencia de datos personales que se efectúe debe estar autorizada previamente por el titular, salvo que se actualice alguna de las siguientes excepciones:

- Cuando la transferencia de los datos personales esté prevista en una ley, convenio o tratado internacional suscrito y ratificado por México.

- Cuando la transferencia se realice entre responsables, siempre y cuando los datos personales se utilicen para el ejercicio de facultades propias, compatibles o análogas con la finalidad que motivó el tratamiento de los datos personales.
- Cuando la transferencia de los datos personales sea legalmente exigida para la investigación y persecución de los delitos, así como la procuración o administración de justicia.
- Cuando la transferencia de los datos personales sea precisa para el reconocimiento, ejercicio o defensa de un derecho ante autoridad competente, siempre y cuando medie el requerimiento de esta última.
- Cuando la transferencia de los datos personales sea necesaria para la prevención, diagnóstico médico, prestación de asistencia sanitaria, tratamiento médico o gestión de servicios sanitarios, siempre y cuando dichos fines sean acreditados.
- Cuando la transferencia de los datos personales sea precisa para el mantenimiento o cumplimiento de una relación jurídica entre el responsable y el titular.
- Cuando la transferencia de los datos personales sea necesaria por virtud de un contrato celebrado o por celebrar en interés del titular, por el responsable y un tercero.
- Cuando el responsable no esté obligado a recabar el consentimiento del titular para el tratamiento de sus datos personales.
- Cuando la transferencia de datos personales sea necesaria por razones de seguridad nacional.

Cabe señalar, que el hecho de que el responsable no esté obligado a requerir el consentimiento del titular para la transferencia de sus datos personales, de ninguna manera, deberá entenderse que esta excepción se extienda o resulte aplicable a la observancia de las demás obligaciones previstas en la Ley General, los Lineamientos generales y demás disposiciones aplicables.

Por regla general, la autorización del titular para la transferencia de sus datos personales debe ser en la modalidad tácita, salvo que una disposición legal exija al responsable recabar el consentimiento expreso del titular. En aquellos casos donde se requiera el consentimiento expreso del titular, el responsable está obligado a establecer cualquier medio que le permita obtener dicho consentimiento de manera previa a la transferencia de los datos personales, siempre y cuando el medio habilitado sea de fácil acceso y con la mayor cobertura posible, considerando el perfil de los titulares y la forma en que mantienen contacto cotidiano o común con éstos.

Asimismo, el responsable transferente de los datos personales está obligado a:

- Informar en su aviso de privacidad los destinatarios de los datos personales y las finalidades que motivaron la comunicación de estos.

- Limitar el tratamiento de los datos personales transferidos a las finalidades que originaron la misma.
- Comunicar su aviso de privacidad al receptor o destinatario de los datos personales.
- Formalizar la transferencia de datos personales mediante la suscripción de cláusulas contractuales, convenios de colaboración o cualquier otro instrumento jurídico, que le permita demostrar el alcance del tratamiento de los datos personales, las obligaciones y responsabilidades asumidas por las partes, salvo que se actualice alguna de las siguientes excepciones:
  - Cuando la transferencia de datos personales sea nacional y se realice entre responsables en cumplimiento de una disposición legal o en el ejercicio de atribuciones expresamente conferidas a éstos.
  - Cuando la transferencia de datos personales sea internacional y se encuentre prevista en una ley o tratado suscrito y ratificado por México, o bien, se realice a petición de una autoridad extranjera u organismo internacional competente en su carácter de receptor, siempre y cuando las facultades entre el transferente y el receptor sean homólogas, o bien, las finalidades que motivan la transferencia de datos personales sean análogas o compatibles respecto de aquéllas que dieron origen al tratamiento del responsable transferente.
  - Cuando se trate de una transferencia nacional de datos personales, además de las reglas generales señaladas anteriormente, el receptor o destinatario de los datos personales:
    - Asume el carácter de responsable conforme a la legislación que en esta materia le resulte aplicable, atendiendo a su naturaleza jurídica, pública o privada.
    - Está obligado a tratar los datos personales conforme a dicha legislación y a lo convenido en el aviso de privacidad que le será comunicado por el responsable.
    - Debe garantizar la confidencialidad de los datos personales.
    - Está obligado a tratar los datos personales para las finalidades que motivaron su transferencia atendiendo a lo convenido en el aviso de privacidad del responsable transferente.

Si se trata de una transferencia internacional de datos personales, además de las reglas generales señaladas anteriormente, el responsable sólo podrá transferir datos personales fuera del territorio nacional cuando el receptor o destinatario se obligue a proteger los datos personales conforme a obligaciones similares o equiparables a las previstas en la Ley General, los Lineamientos generales y demás normatividad mexicana aplicable en la materia, así como a los términos establecidos en el aviso de privacidad que le será comunicado por el responsable transferente.

En la evaluación de impacto se señaló:

"X. Transferencias de datos.

Transferencias de datos personales que, en su caso, pretendan efectuarse con la puesta en operación del Sistema de Procesamiento de Pasajeros

Es posible que una persona enrolada biométricamente y que una persona que no se haya enrolado biométricamente crucen por las puertas de pre-seguridad y las puertas de abordaje empleando un modo no biométrico. En este caso la plataforma orchestra comparte los datos del pase de abordar con los componentes APV y ACUS respectivamente, y estos a su vez comparten esos datos con las aerolíneas.

Dentro del procesamiento de pasajeros de manera biométrica existe transferencia de datos entre los componentes tecnológicos de la solución instalados en el AIFA, hacia las aerolíneas, transfiriendo solamente la información del pase de abordar, esto con el objetivo de avisar a la aerolínea que el pasajero ha abordado la aeronave.

[...]

• Transferencia de datos entre la aplicación móvil y la plataforma vb orchestra™, para la creación del PDE.

...

• Transferencia de datos entre el quiosco de auto-servicio (CUSS) y la plataforma vb orchestra™, para la creación del PDE.

...

Transmisión de datos entre el mostrador convencional (CUPPS), V-desk y la plataforma vb orchestra™, para la creación del PDE.

...

• Transmisión de datos entre la E-Gate de Pre-Seguridad y el módulo APV de Amadeus:

...

• Transferencia de datos entre la E-Gate de Abordaje y el módulo ACUS de Amadeus

...

• Transmisión de datos entre el componente APV de Amadeus y los sistemas de las aerolíneas.

...

• Transferencia de datos entre el componente ACUS de Amadeus y los sistemas de las aerolíneas.

...

El detalle de las transferencias de datos personales que se efectúan en el Sistema de Procesamiento de Pasajeros se encuentra en el Inventario de Datos Personales.

El resumen de las transferencias se encuentra en el documento Experiencia sin contacto con tecnología biométrica, Gestión de Datos Personales, Solución Biométrica, 2.3 "Resumen ilustrativo de la gestión de datos personales en la solución de procesamiento biométrico y no biométrico de pasajeros".

Por su parte en la respuesta al requerimiento de información adicional se estipula que:

"..Asimismo, toda vez que se advierte puede haber comunicación de datos personales durante la implementación del "Sistema de Procesamiento de Pasajeros", se requiere mayor información sobre las transferencias y/o remisiones que en su caso se efectúen; identificando los momentos en los que se llevarán a cabo, así como los actores involucrados en este proceso como pueden ser; aerolíneas, sujetos obligados, entre otros en este sentido, remitir los convenios, contratos o instrumentos jurídicos que definen y regulan dicha relación y por los cuales se establecen dichas comunicaciones de datos personales, en su caso, así como las cláusulas por las cuales se rigen conforme la normatividad en materia."

Las transferencias y transmisiones de datos se encuentran definidas en los inventarios de datos que integran la EIPDP presentada a ese instituto el pasado 9 de enero del presente. Asimismo, se comparte nuevamente en formato digital el mencionado inventario. (Anexo 6 "Documento de Seguridad y Diagramas de Flujo")

...

Además de lo ya mencionado, en los avisos de privacidad (simple e integral) se ve reflejada la obtención del consentimiento expreso del particular, así como las finalidades por las cuales se recaban los datos, así como las transferencias que para el procesamiento de pasajeros se requieran, lo anterior en cumplimiento a lo que dispone el último párrafo del artículo 21 de la LGTAIP, que expresa que tratándose de datos personales sensibles el responsable deberá obtener el consentimiento expreso y por escrito del titular para su tratamiento, a través de mecanismos como el de autenticación que se establezca..."

Ahora bien, en los diferentes avisos de privacidad integrales que fueron compartidos como parte de la evaluación de impacto, se advierte que las transferencias que se pretenden efectuar corresponden a la comunicación que se realizará a la plataforma vOrchestra de los datos que son en los diferentes momentos de obtención que previamente ya se han señalado.

No obstante, se indica en la evaluación de impacto, por lo que hace al medio de obtención de los mostradores de documentación CUPPS-Vdesk serán en los mostradores de las diferentes aerolíneas en las cuales los titulares podrán realizar el enrolamiento biométrico con asistencia de personal de la aerolínea.

Al respecto, se advierten dos posibles supuestos que el AIFA señala como transferencias:

- Las comunicaciones que se realizan entre la plataforma vb orchestra y las demás herramientas que conforman el Sistema de Procesamiento, esto es, entre la aplicación móvil, el quiosco de autoservició-CUSS, el mostrador CUPPS-vDesk, las puertas E-Gate de Pre Seguridad y el módulo APV y la E-Gate de Abordaje y el módulo ACUS.
- Transmisión de datos a los sistemas de las aerolíneas.

En este sentido, por lo que hace al primer supuesto se advierte que se realiza un intercambio y comunicación de datos personales entre los diferentes elementos que componen el Sistema de Procesamiento, por lo que se realizan como parte del funcionamiento del mismo Sistema y entre los mismos elementos que lo componen.

Esto es así ya que si bien, las diferentes tecnologías son proporcionadas por diversas empresas, es decir, Consorcio Apollocom, AMADEUS y Vision-Box S.A. de C.V, de conformidad con lo establecido en el apartado de responsable y encargado, éstos pudieran constituir como encargados, en su caso, subencargado del AIFA en términos de lo establecido en el artículo 3, fracción XV ya que son empresas privadas ajenas a la organización del responsable, en este caso el AIFA, que conjuntamente con otras tratan datos personales a nombre y por cuenta del responsable.

Por lo anterior, la comunicación aludida por el AIFA, en este caso no correspondería como una transferencia, sino como una remisión en términos de lo establecido en el artículo 3, fracción XXVII entendida como la comunicación de datos personales realizada exclusivamente entre el responsable y encargado, dentro o fuera del territorio mexicano.

Al respecto y tal como se mencionó en el apartado anterior, la relación entre ambos deberá estar formalizada mediante contrato o cualquier otro instrumento jurídico que decida el responsable, de conformidad con la normatividad que les resulte aplicable, incluida la Ley General.

El anterior supuesto pudiera ser aplicable en el caso de que la aerolínea fungiera como encargado en la transmisión que hace al momento del enrolamiento biométrico en los mostradores convencionales puesto que se realiza una transmisión de datos personales a la plataforma vb orchestra mediante la tecnología Vdesk proporcionada por el AIFA. Por lo que, ante este supuesto se podría estar ante una relación de un responsable como AIFA y el encargado, la aerolínea, toda vez que realiza el proceso de registro biométrico a nombre y por cuenta del AIFA toda vez es éste quien decide los medios de tratamiento y la forma en la que se recabarán y remitirán a la vb orchestra. No obstante, dicha determinación deberá ser confirmada o en su caso identificada por el responsable.

Por lo que corresponde al segundo supuesto de las aerolíneas, es importante observar que de la plataforma vb orchestra se pretende remitir a las aerolíneas a través de los diversos sistemas, a efecto de conocer los estatus de los resultados obtenidos al momento de verificar la identidad de las personas en las E-gates de abordaje, no obstante, como ya se señaló en el apartado de responsable y encargado, no se advierte que se tenga perfectamente definido el carácter con el cual se ostentarían las mismas, ya que si las aerolíneas en este proceso constituyen como

encargados, la misma suerte correrá del primer supuesto antes referido y se estaría ante una remisión.

Sin embargo, en el caso de que la aerolínea se constituya como un tercer responsable a quien se le transfieren los datos personales del pase de abordar una vez que los titulares han pasado por las E-gates de abordaje, entonces se estaría ante una transferencia y en tal caso, se tendría que cumplir con las obligaciones señaladas en la normatividad aplicable.

Ahora bien, como se puede observar las transferencias de datos personales se pretende se lleve a cabo a través de diversas empresas, es decir, Consorcio Apollocom, AMADEUS y Vision-Box S.A. de C.V, las cuales conforme la información proporcionada pudiera contar con domicilio fuera del territorio nacional, motivo de la importancia que tiene que se suscriban las cláusulas contractuales en las cuales se señale lo relacionado con las transferencias que se pudieran efectuar.

Lo anterior, es importante tener en cuenta que Amadeus, constituye un servicio de cómputo en la nube, es por ello que a mayor referencia se debe de garantizar que las transferencias de datos personales se realicen de conformidad con la normatividad aplicable, tomando en consideración las obligaciones y deberes de cumplimiento y el ámbito territorial de dicha empresa e inclusive la normatividad para el sector privado en nuestro país.

En este mismo contexto, conforme a la información proporcionada se advierte que se pretende estar efectuando diversas transferencias de datos personales, más, sin embargo, tomando en cuenta los principios de finalidad y de proporcionalidad se debe de tomar en consideración las finalidades para las cuales se pretende realizar las transferencias de estos datos personales y por su parte verificar la proporcionalidad de efectuar las mismas, como lo puede ser el nombre del vendedor de las aerolíneas.

Por lo que, tomando en consideración lo anterior, se emiten las siguientes recomendaciones:

Recomendaciones en torno a transferencias

Clave	Recomendación
AIFA_TR_001	Una vez que se definan las figuras con las cuales se ostentarían todos aquellos que intervienen en el tratamiento de los datos personales, en apego a la normatividad en materia de protección de datos personales, la Ley General en su carácter de Responsable, Encargado y Subencargado, se recomienda definir si se efectuarían transferencias o remisiones de datos, esto a efecto de que se observe la normatividad antes señalada e inclusive la normatividad del

	sector privado en el supuesto de que se efectúe transferencias o remisiones entre empresas de este sector.
AIFA_TR_002	Se recomienda establecer el procedimiento y mecanismos para solicitar el consentimiento, expreso y por escrito para la realización de las transferencias que se llevarán a cabo a través de las modalidades establecidas por parte del AIFA.
AIFA_TR_003	Se recomienda establecer en los convenios de colaboración cláusulas relativas al cumplimiento en materia de protección de datos personales, en el que se incluya lo siguiente: o Realizar tratamiento de datos personales, por las partes, en términos de las normatividades que les facultan para ello y de conformidad con el artículo 34 de la Ley General mediante el respectivo sistema de gestión y documento de seguridad en la que se adoptan estándares nacionales e internaciones, así como buenas prácticas en la materia y 19 de la Ley Federal de Datos y 57 y 59 del Reglamento, en el caso de responsables del sector privado. o Con relación al documento de seguridad reconocer que se tuvo conocimiento de los elementos que lo integran en lo que corresponda al tratamiento de datos que derive del cumplimiento del objeto del Convenio. o Establecer la responsabilidad de las partes sobre las bases de datos que se generen con motivo de la celebración del Convenio de colaboración, cuyo tratamiento deberá apegarse a la normatividad en la materia; así como llevar a cabo el cumplimiento de principios, deberes y obligaciones establecidas en la Ley General, Ley Federal de Datos y la normatividad que de estos derive. o Reconocer el carácter de cada una de las partes como responsables del tratamiento de datos personales de manera independiente en lo que respecta a su régimen de protección de datos personales. o Reconocer el tratamiento de datos personales de datos personales sensibles y la obligación de las partes de realizar las adecuaciones necesarias a fin de que las medidas de seguridad sean acordes atendiendo a las características particulares de la información. o Establecer el compromiso de notificar vulneraciones de datos personales, así como realizar las acciones encaminadas a realizar un

	proceso de revisión exhaustiva sobre las vulneraciones y determinar la afectación que puedan sufrir los titulares. o Establecer las obligaciones de las autoridades y sector privado, como terceros receptores de los datos personales: ▪ Llevar a cabo el tratamiento de datos personales en términos de lo establecido por la Secretaría en su aviso de privacidad y asumir el carácter de responsable a partir de que se materialice la transferencia de los datos personales, obligándose a proteger los datos personales conforme a los principios, deberes y demás obligaciones previstas en la Ley General, Ley Federal de Datos. ▪ Elaborar y poner a disposición de los titulares el/los aviso(s) de privacidad los cuales deberán ser validados por las partes para efectos de dar cumplimiento a lo establecido en el artículo 115 de los Lineamientos Generales y 36 de la Ley Federal y 68 del Reglamento, y cumplir con los elementos informativos obligatorios y en las modalidades que sea necesario. ▪ No compartir los datos personales con terceros, con excepción de las autoridades competentes. ▪ Conservar los datos personales de manera bloqueada hasta que se agoten los plazos legales que resulten aplicables, una vez que se dé cumplimiento a las obligaciones del Convenio y se agoten las finalidades que dieron origen al tratamiento de los datos personales. ▪ Contar con las medidas de seguridad necesarias para el cumplimiento de las obligaciones que derivan del deber de seguridad, especialmente aquellas que se refieren a los medios y mecanismos para realizar las comunicaciones de datos personales. o Reconocer el compromiso de las partes de no realizar ningún uso posterior de los datos personales que le son entregados o transferidos, una vez que se cumpla con las obligaciones del Convenio, y sólo conservar los datos personales de manera bloqueada hasta que se agote el plazo legal, procediendo a su borrado seguro. o Adoptar esquemas de mejores prácticas en protección de datos personales como pueden ser la implementación de acciones preventivas.
AIFA_TR_004	Se sugiere considerar en los convenios de colaboración el establecer una cláusula específica en la que se precise la responsabilidad sobre la atención del ejercicio de cualquiera de los derechos ARCO, considerando que el responsable es quien tenga en su posesión los datos del titular.

8. Datos biométricos

Al respecto, cabe señalar que, si bien los datos biométricos no están mencionados de manera expresa en el listado de datos personales sensibles que se incluyen en la Ley General, ello no implica que no se puedan considerarse como tal bajo ciertas circunstancias, al actualizar los supuestos señalados por dicha normatividad en su artículo 3, fracción X.

En ese sentido, cabe señalar en el ámbito internacional, el contenido del Tratado 223 de la Serie del Consejo de Europa, relativo al Protocolo de Enmienda del Convenio para la Protección de las Personas respecto al Tratamiento Automatizado de Datos de Carácter Personal[59] que, en su artículo 6, refiere dentro de sus categorías especiales de datos, el tratamiento de datos biométricos que identifican únicamente a una persona, preceptuando que, estará permitido únicamente cuando se consagren garantías apropiadas conforme a la ley, complementando aquellas del Convenio de referencia.

Asimismo, cabe señalar que el Reglamento General de Protección de Datos, define a los datos biométricos en su artículo 4, numeral 14 como aquellos *"datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos"*. Asimismo, en su artículo 9, numeral 1, contempla a los datos biométricos dentro de las **categorías especiales de datos personales** que merecen mayor protección debido a su sensibilidad.

Por otro lado, es importante mencionar que de acuerdo al documento *Guía para el tratamiento de datos biométricos*[60], elaborada por el INAI en la cual se identifican las principales tecnologías biométricas de reconocimiento de características físicas y fisiológicas que consideran parámetros derivados de la medición directa de algún rasgo estrictamente físico o funcional del cuerpo humano a la hora de identificar personas, entre las que destacan la huella digital, el rostro (reconocimiento facial), la retina, el iris, la geometría de la mano o de los dedos, la estructura de las venas de la mano, la forma de las orejas, la piel o textura de la superficie dérmica, el ADN, la composición química del olor corporal y el patrón vascular, pulsación cardíaca, entre otros.

---

[59] Disponible en el vínculo siguiente: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/223/signatures?module=treatydetail&treatynum=223, consultado por última vez el 28/02/2023.

[60] Disponible en el siguiente vínculo electrónico: https://home.inai.org.mx/wp-content/documentos/DocumentosSectorPublico/GuiaDatosBiometricos_Web_Links.pdf, consultado por última vez el 28/02/2023.

La cual se esquematiza de la manera siguiente:

Biométrico	Descripción de reconocimiento
Huella dactilar	Es la más antigua y existen dos técnicas: (i) Basada en minucias y (ii) basada en correlación. Esta última requiere un registro más preciso pues se analiza el patrón global seguido por la huella dactilar.
Reconocimiento facial	El análisis se realiza a través de mediciones como la distancia entre los ojos, la longitud de la nariz o el ángulo de la mandíbula.
Reconocimiento de iris	Una cámara infrarroja escanea el iris y proporciona sus detalles. Los patrones del iris vienen marcados desde el nacimiento y rara vez cambian, son muy complejos y contienen una gran cantidad de información, más de 200 propiedades únicas.
Geometría de la mano	A través de una cámara se capturan imágenes en 3-D, se extraen características que incluyen las curvas de los dedos, su grosor y longitud, la altura y la anchura del dorso de la mano, las distancias entre las articulaciones y la estructura ósea.
Reconocimiento de retina	Se basa en la utilización del patrón de los vasos sanguíneos contenidos en la misma. Cada patrón es único incluso entre los gemelos idénticos y tiene una tasa de falsos positivos prácticamente nula.
Reconocimiento vascular	Se extrae el patrón biométrico a partir de la geometría del árbol de venas del dedo. Es interno y no deja rastro por lo que el robo de identidad es muy difícil.

Asimismo, debemos considerar lo establecido por el extinto Grupo de Trabajo del Artículo 29[61], los datos biométricos, en mayor o menor medida, son:

- **Universales,** ya que son datos con los que contamos todas las personas;
- **Únicos,** ya que no existen dos biométricos con las mismas características por lo que nos distinguen de otras personas;
- **Permanentes**, ya que se mantienen, en la mayoría de los casos, a lo largo del tiempo en cada persona, y
- **Medibles** de forma cuantitativa.

Aunado a lo anterior, la citada Guía contempla consideraciones como las siguientes:

- Los datos biométricos pueden usarse como medio para acceder a determinadas aplicaciones o dispositivos como la computadora o el celular, esto es como un medio de identificación y autentificación de una persona.

[61] El Grupo de Trabajo del artículo 29 fue el grupo de trabajo europeo independiente que se ha ocupado de cuestiones relacionadas con la protección de la privacidad y los datos personales en el marco de la abrogada Directiva Europea 95/46/CE, hasta el 25 de mayo de 2018, fecha de la entrada en aplicación del REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de la Unión Europea de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE, también denominado como Reglamento general de protección de datos; definición elaborada tomando como la referencia oficial contenida en el sitio: https://edpb.europa.eu/about-edpb/more-about-edpb/article-29-working-party_es, consultado por última ocasión el 28/02/2023.

- El dato biométrico relativo a una persona se puede señalar como un dato personal, pues reúne las dos condiciones que se deben cumplir para que cierta información se considere un dato personal:
  1. Debe referir a una persona física, y
  2. Debe identificar o hacer identificable a su titular.
- Si bien los datos biométricos no están mencionados de manera expresa en el listado de datos personales sensibles que se incluyen tanto en la Ley General, ello no implica que no se puedan considerar como tal bajo ciertas circunstancias. Para determinar tal característica, se requiere atender las condiciones del caso concreto, a fin de analizar si los datos biométricos en cuestión actualizan alguno de los siguientes tres supuestos que prevén la Ley Federal de Datos para considerar un dato personal como sensible:
  a) Que se refieran a la esfera más íntima de su titular;
  b) Que su utilización indebida pueda dar origen a discriminación, o
  c) Que su uso ilegítimo conlleve un grave riesgo para su titular.
- En los casos en los que un dato biométrico se considere sensible, se requerirá de una protección reforzada.
- En observancia a los principios de licitud, información, consentimiento y finalidad, así como al deber de seguridad se recomienda:
  - Conocer la normatividad que en lo específico regula y aplica a la actividad en la que son tratados los datos biométricos, a fin de verificar que la misma prevea el uso de este tipo de datos y en qué términos lo hace, o bien, que la misma no lo prohíba y en el caso analizar si el uso de los mismos está debidamente justificado según la finalidad de la que se trate.
  - Utilizar medios que estén permitidos por la ley para obtener los datos biométricos.
  - Tener especial cuidado en el tratamiento de datos biométrico, a fin de que éste se apegue a lo informado al titular y se privilegie en todo momento sus intereses con relación al uso de sus datos personales.
  - Informar expresamente en el aviso de privacidad que se recabarán datos biométricos, especificando su tipo, cuando estos sean sensibles, señalarlo de forma expresa. o Incluir en el aviso de privacidad las finalidades para las cuales serán tratados los datos biométricos, entre ellas el reconocimiento de los titulares, y en caso de que éstas requieran el consentimiento, señalarlo.
  - Identificar si el dato biométrico recolectado será tratado dentro de alguno de los supuestos previstos por los artículos 10 de la Ley Federal de Datos, en caso de que así sea, su tratamiento no requerirá consentimiento. No obstante, si el responsable pretende utilizar los datos biométricos para finalidades que no encuadren en las excepciones anteriormente señaladas, o que no resulten compatibles o análogas con aquéllas para

las cuales se recabaron los datos personales, será necesario que se obtenga el consentimiento del titular.

- Implementar las medidas físicas, técnicas y administrativas necesarias para garantizar que los datos biométricos estén protegidos del acceso, procesamiento, eliminación, pérdida o uso no autorizados.

Cabe precisar que la Ley General, sus Lineamientos Generales y demás disposiciones aplicables, son un conjunto de normas de carácter general que señalan al responsable las directrices a través de las cuales deberá de cumplir con las obligaciones ahí previstas.

En razón de lo anterior, cada responsable tendrá la plena facultad para establecer los parámetros en función de los cuales se determinen las muestras biométricas[62] y su debida integración a un sistema biométrico[63] determinado, lo que le permitirá al responsable llevar a cabo el proceso de reconocimiento o autenticación.

Lo anterior, en consideración a las características propias del responsable, a sus necesidades, así como en razón de diversos factores como la naturaleza de sus actividades, la finalidad del tratamiento, la naturaleza del biométrico a utilizar, la interoperabilidad entre sistemas biométricos, el costo, el impacto en la organización y demás circunstancias de operación. De esta manera, resulta relevante considerar que el sistema biométrico estará determinado en función del tipo de dato o datos biométricos elegidos por parte del responsable.

En virtud de lo anterior, se señalan las recomendaciones siguientes:

Recomendaciones en torno a datos biométricos

Clave	Recomendación
AIFA_Bio_001	Se recomienda identificar el tipo de datos personales sujetos a tratamiento y, con base en ello, dar el tratamiento que les corresponda, de conformidad con las precisiones realizadas previamente. Esto con la finalidad de asegurar el cumplimiento de los principios y deberes en la materia.
AIFA_Bio_002	Se recomienda buscar la manera de garantizar la implementación de medidas que aseguren que los datos personales cumplan con las características de ser exactos, completos, pertinentes, actualizados y

[62] Definidas como el "Prototipo de un dato biométrico", tomado la página 6 de la Guía para el Tratamiento de Datos Biométricos, emitida por el INAI, disponible en el siguiente vínculo electrónico: http://inicio.inai.org.mx/DocumentosdeInteres/GuiaDatosBiometricos_Web_Links.pdf, consultado por última vez el 28/02/2023.

[63] Definido como "... las aplicaciones tecnológicas que permiten el reconocimiento automático de una persona a través de sus datos biométricos", tomado la página 6 de la Guía para el Tratamiento de Datos Biométricos, emitida por el INAI, disponible en el siguiente vínculo electrónico: http://inicio.inai.org.mx/DocumentosdeInteres/GuiaDatosBiometricos_Web_Links.pdf, consultado por última vez el 28/02/2023.

	correctos que, para el caso de datos biométricos la exactitud en la recogida y al establecer el vínculo entre la persona y sus datos en el registro, permitirán prevenir la usurpación de identidad..
AIFA_Bio_003	Particularmente, por lo que hace a remisiones o transferencias de datos biométricos, se recomienda identificar la interoperabilidad entre las bases de datos de las que se pretende realizar dicho tratamiento, así como establecer medidas de seguridad adecuadas, pertinentes y suficientes proporcionales a la alta sensibilidad y riesgos que estos datos tienen por sus características.

IX. Conclusiones y recomendaciones.

En términos del artículo 30 de las Disposiciones administrativas el presente dictamen no tiene por efecto impedir la puesta en operación o modificación de la política pública, programa, sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología que implique un tratamiento intensivo o relevante de datos personales; ni validar el presunto cumplimiento de las obligaciones previstas en la Ley General y demás disposiciones aplicables, en perjuicio de las atribuciones conferidas al Instituto.

En ese entendido, se procede a emitir las siguientes:

RECOMENDACIONES NO VINCULANTES

Clave	Recomendación
[redacted]	[redacted]
[redacted]	[redacted]
AIFA_GR_003	Se sugiere que, dentro de la documentación sugerida, se incluya aquellos documentos que acrediten la realización del análisis de riesgos en el Sistema de Procesamiento que considere las posibles consecuencias negativas para los titulares que pudieran derivar de una vulneración de seguridad ocurrida.
[redacted]	[redacted]

Se eliminan 8 lineas, con fundamento en el artículo 110, fracción I de la LFTAIP; Décimo séptimo de los lineamientos Generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas, en relación con el artículo 5, fracción VI de la Ley de Seguridad Nacional; 47, Bis 4 de la Ley de Aviación Civil, 46 y 47 de la Ley de Aeropuertos y 152 del Reglamento de Aeropuertos.

Clave	Recomendación
	[redacted]

Principios de protección de datos personales

Recomendaciones entorno al principio de licitud

Clave	Recomendación
AIFA_LI_001	Se recomienda realizar una verificación de forma constante las reformas al marco normativo aplicable, tanto nacional como internacional, relacionadas con el tratamiento de datos biométricos para el tráfico de personas dentro de las instalaciones del Aeropuerto Internacional Felipe Ángeles, esto como servicio complementario en términos de la Ley de Aeropuertos y su Reglamento. De manera particular, el responsable deberá corroborar que el tratamiento de datos personales biométrico sea congruente y coherente con los estándares aplicables, como en el caso de los previstos por la OACI.
AIFA_LI_002	Se recomienda realizar un análisis sobre el tratamiento de datos personales en consideración con la normatividad que le aplica al sujeto obligado y se relacionada con el servicio complementario de tráfico de pasajeros y que apliquen a México a fin de considerar los alcances y finalidades de esto.
AIFA_LI_003	Se recomienda, realizar el tratamiento de datos personales en sistemas o plataformas informáticas en las que tenga poder de decisión sobre estos.
AIFA_LI_004	Se sugiere considerar lo manifestado en el principio de licitud con la finalidad de poder incluir lo respectivo en el instrumento jurídico celebrado para que la SEDENA a fin de que las figuras jurídicas sean apegadas la normatividad en materia de datos personales.
AIFA_LI_005	Se sugiere considerar lo manifestado en el principio de licitud y demás principios, a fin de poder plasmar lo referente en el instrumento jurídico celebrado para establecer SEDENA y las empresas Apollo Communications, S.A. de C.V., Química Apollo S.A de C.V., Vision-Box Soluções de Visão Por Computador S.A., y Amadeus IT Group, S.A. a fin de que puedan atende lo previsto en la normatividad de protección de datos personales y se considere con precisión los deberes en el marco del Sistema de Procesamiento.
[redacted]	[redacted]

Se eliminan 6 lineas, con fundamento en el artículo 110, fracción I de la LFTAIP; Décimo séptimo de los lineamientos Generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas, en relación con el artículo 5, fracción VI de la Ley de Seguridad Nacional; 47, Bis 4 de la Ley de Aviación Civil, 46 y 47 de la Ley de Aeropuertos y 152 del Reglamento de Aeropuertos.

	[redacted]
AIFA_LI_007	Se sugiere ceñirse a las figuras de responsable y encargado previstas en la Ley General y el apartado relativo para la celebración de la reestructuración del instrumento jurídico celebrado.
AIFA_LI_008	Se sugiere considerar lo manifestado en el presente principio en los instrumentos jurídicos celebrados con motivo del Sistema de Procesamiento y en el que se consideren los deberes del responsable y encargado previstas en la Ley General y en los Lineamientos en relación al cómputo en la nube.
AIFA_LI_009	Se sugiere que el AIFA en su carácter de responsable y en atención al Sistema de Procesamiento, se pueda considerar la emisión de instrumentos jurídicos necesarios para que las aerolíneas realicen el enrolamiento en mostrador, conforme lo previsto en el artículo 59 de la Ley General.
AIFA_LI_010	Se recomienda que el AIFA emita los instrumentos jurídicos necesarios para que las aerolíneas realicen el enrolamiento en mostrador, conforme lo previsto en el artículo 59 de la Ley General.
AIFA_LI_011	Respecto del enrolamiento de personas extranjeras en el Sistema de Procesamiento, se recomienda identificar la normatividad que permite efectuarlo, considerando en su caso los documentos emitidos por la OACI y la Ley General, los Lineamentos y demás legislación en la materia.
AIFA_LI_012	Se sugiere realizar un análisis sobre los documentos de identidad que se pretenden aceptar en el marco del Sistema de Procesamiento a fin de homologar los procedimientos de recabo descritos, asimismo, en caso de considerar viables la incorporación de otros documentos, se sugiere contemplar la normatividad aplicable, así como los principios y deberes establecidos en la Ley General, para poder llevar a cabo la correcta implementación del aludido sistema.

Recomendaciones en torno al principio de finalidad

Clave	Recomendación
AIFA_FI_001	Se recomienda considerar la totalidad de las finalidades que se pretenden realizar tanto en el aviso de privacidad integral como simplificado, de conformidad con los elementos para el cumplimiento del principio de información.

Se eliminan 4 lineas, con fundamento en el artículo 110, fracción I de la LFTAIP; Décimo séptimo de los lineamientos Generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas, en relación con el artículo 5, fracción VI de la Ley de Seguridad Nacional; 47, Bis 4 de la Ley de Aviación Civil, 46 y 47 de la Ley de Aeropuertos y 152 del Reglamento de Aeropuertos.

AIFA_FI_002	Se recomienda revisar a efecto de identificar claramente la totalidad de las finalidades que se pretendan realizar con motivo del tratamiento de datos, tomando en cuenta las consideraciones vertidas por este Instituto en el apartado de finalidad.
AIFA_FI_003	Se sugiere considerar lo manifestado en el principio de licitud a fin de poder identificar claramente la totalidad de las finalidades que se pretenden realizar con motivo del tratamiento de datos y verificar que éstas se encuentren de acuerdo a las atribuciones que facultan al AIFA.
AIFA_FI_004	Con relación a la posible finalidad de utilizar los datos personales recabados en el marco del Sistema de Procesamiento en materia de seguridad, se recomienda tomar en consideración lo respectivo, vertido en el principio de licitud.
AIFA_FI_005	Con base en la totalidad de las finalidades que se adviertan, se recomienda identificar todas aquellas en las que se requiere el consentimiento y aquellas que no lo requieren.
AIFA_FI_006	Se recomienda revisar e identificar si el tratamiento que se pretende llevar a cabo mediante el Sistema de Procesamiento tiene el alcance de que, eventualmente, atienda la finalidad de dar atención al requerimiento de autoridades competentes por causas de seguridad, inclusive de seguridad nacional. En caso de que así sea, se recomienda considerar: la expectativa razonable de privacidad del titular basada en la relación que tiene con éste; la naturaleza de los datos personales; las consecuencias del tratamiento posterior de los datos personales para el titular, y las medidas adoptadas para que el tratamiento posterior de los datos personales cumpla con las disposiciones previstas en la Ley General y sus Lineamientos generales.
AIFA_FI_007	Se identifica que conforme los estándares aplicables para el uso de datos biométricos en el ámbito aeroportuario, eventualmente podrían agregarse finalidades o las finalidades existentes podrían ser modificadas, por lo cual, el responsable deberá identificar los cambios aplicables requeridos de conformidad con la normatividad de protección de datos personales y, en su caso, verificar la procedencia de presentación de una nueva evaluación de impacto en la protección de datos personales; razón por la cual, deberán identificarse dichas finalidades potenciales en el marco de la normatividad y estándares aplicables, e identificar dentro del documento de seguridad, si forman parte del alcance del tratamiento, si se encuentran excluidas, o, en su caso, si podrán ser susceptibles de consideración de manera posterior, para lo cual, deberá señalarse en el plan de trabajo respectivo o, en su caso, en el programa de protección de datos institucional.

Recomendaciones en torno al principio de Lealtad

Clave	Recomendaciones
AIFA_LE_001	En atención a la expectativa razonable de privacidad referente a la confianza que el titular ha depositado en el responsable respecto a que sus datos personales sean tratados conforme a lo señalado en el aviso de privacidad, se recomienda que, a través de éste, se precise en cada caso, cuáles son los medios de obtención de los datos personales, atendiendo las recomendaciones efectuadas en torno a ese principio.
AIFA_LE_002	Se sugiere que, en caso de que se considere mantener diversos avisos de privacidad respecto al Sistema de Procesamiento, se recomienda hacer homologar que se trata del mismo tratamiento de datos personales y las mismas finalidades de tratamiento.
AIFA_LE_003	Se sugiere, cumplir con las recomendaciones emitidas en el apartado de derechos ARCO con el objetivo de generar una expectativa razonable de privacidad en los titulares.
AIFA_LE_004	Se sugiere que, además de las recomendaciones efectuadas en el principio de información y en el apartado de derechos ARCO, que se privilegie que los particulares tengan certeza de los elementos suficientes para conocer los datos que serán objeto de tratamiento de datos personales, los periodos de conservación y la destrucción después de que culminen los periodos de conservación respectivos.
AIFA_LE_005	Se sugiere considerar que, la posibilidad de que, de acuerdo a los diferentes perfiles de los titulares de datos personales, se considere que podrían requerir el acceso al PDE de forma posterior a las 24 horas siguientes a la salida del vuelo respectivo.
AIFA_LE_006	Se sugiere considerar procedimientos de revisión y evaluación constante del Sistema de Procesamiento, esto para evitar que se actualice la existencia de indicios de que el tratamiento de datos personales que efectúa diera lugar a una discriminación o trato injusto o arbitrario contra los titulares.
AIFA_LE_007	Se sugiere revisar la configuración de la plataforma vb orchestra para personalizar el límite de 24 horas para eliminar los datos personales a efecto de justificar la razón y el fin de dicho mecanismo, toda vez que puede generar una situación que pudiera ser desleal para los titulares al estar a discreción de quien tenga el acceso a esta configuración, y que sus datos sean almacenados más tiempo de lo informado.
AIFA_LE_008	Se recomienda considerar la implementación de medidas para garantizar el debido tratamiento y privilegiar los intereses y expectativa razonable de

	privacidad de los titulares, como por ejemplo políticas de privacidad, estándares, mejores prácticas, capacitación al personal, un sistema de supervisión y vigilancia del cumplimiento de la normativa en la materia, sanciones por incumplimiento, entre otros.

Recomendaciones en torno al principio de consentimiento

Clave	Recomendación
AIFA_Co_001	Se recomienda verificar y definir el tipo de consentimiento que se requiere, según las categorías de datos personales que se vayan a tratar o las disposiciones normativas que regulen el tratamiento.
AIFA_Co_002	Se recomienda habilitar los mecanismos necesarios para solicitar el consentimiento expreso y por escrito por parte de las y los titulares de los datos personales en términos de la normatividad aplicable, así como documentar su obtención, tomando en consideración los medios digitales que se emplean en el caso de la app y el quiosco. Lo anterior, tomando como referencia las diferentes modalidades con relación al tratamiento de datos personales entre los cuales se encuentran datos biométricos en su carácter de datos personales sensibles.

Recomendaciones en torno al principio de calidad

Clave	Recomendación
AIFA_CA_ 001	En el procedimiento de obtención de datos a través de los mostradores de documentación CUPPS-Vdesk en el que el agente valida visualmente que la identificación proporcionada corresponde al pasajero y procede con el escaneo del documento en el sistema, se recomienda verificar e implementar medidas que permitan garantizar que la información del titular que se está capturando sea verdadera y fiel a su situación a efecto de que sean exactos y pertinentes para que correspondan efectivamente al titular.
AIFA_CA_ 002	Se recomienda establecer medidas para que los datos personales se corrijan o completen, en las distintas bases de datos que estén a cargo del AIFA.
AIFA_CA_003	En atención a lo examinado, y en correspondencia con lo establecido en el apartado de derechos ARCO, se sugiere establecer mecanismos que acrediten las modificaciones que realicen los titulares con relación a su derecho de rectificación, como pudiera ser, a manera de orientación, la relación de constancias sobre las rectificaciones realizadas, sólo en los casos en que la misma haya sido procedente.

AIFA_CA_004	Se recomienda establecer los plazos de conservación de los datos personales considerando el límite de tiempo para que los titulares puedan enrolarse biométricamente a través de la app como el quiosco antes de su día de vuelo. Asimismo, deberá ser congruente con los plazos de conservación establecidos en los instrumentos de clasificación archivística y considerar un periodo de bloqueo.
AIFA_CA_005	Se recomienda que, al establecer un periodo de bloqueo se consideren las disposiciones legales establecidas en la Ley General de Archivos y las disposiciones aplicables en la materia de que se trate, los aspectos administrativos, contables, fiscales, jurídicos e históricos de la información.
AIFA_CA_006	Se recomienda considerar para el establecimiento del plazo de conservación, periodo de bloqueo y supresión, en caso de ser aplicable y constituirse como otra finalidad del tratamiento, el supuesto de requerimientos de las autoridades ante situaciones de transporte de drogas ilegales, casos de ebriedad o bajo el influjo de estupefacientes, psicotrópicos o enervantes, otros, así como de temas de seguridad.
AIFA_CA_007	Se recomienda elaborar los procedimientos para la conservación y supresión de los datos personales, así como documentarlos, considerando que podrán ser los establecidos en materia de archivos, si a través de los mismos se puede cumplir con la obligación prevista en la Ley General.
AIFA_CA_008	Se recomienda establecer la documentación que permita al responsable demostrar que los datos personales han sido suprimidos en atención a una solicitud de ejercicio del derecho de cancelación.
AIFA_CA_009	Se recomienda establecer políticas, métodos y técnicas orientadas a la supresión definitiva de los datos personales, no sólo de la plataforma vb orchestra, sino de todo el Sistema de Procesamiento, incluidos los sistemas de Amadeus y sus bases de datos AODB y Amadeus DAR, así como las bases de datos que pudieran estar alojadas en servicios de cómputo en la nube, considerando los atributos de irreversibilidad; seguridad y confidencialidad y favorable al medio ambiente.
AIFA_CA_010	Se sugiere tener en cuenta que el PDE, además de contar con datos personales, debe encontrarse previsto en el Catálogo de Disposición Documental, sujetándose a las previsiones previstas en la LGA, para que los titulares conozcan los periodos de conservación, además de las recomendaciones en torno al principio de calidad.

Recomendaciones en torno al borrado seguro

Clave	Recomendación
AIFA_TB_ 001	Se sugiere establecer métodos de borrado a nivel de base de datos que cumplan con los criterios mínimos para evitar la recuperación de la información.
AIFA_TB_002	Se sugiere apegarse a la normatividad aplicable en los Estados Unidos Mexicanos para la implementación de métodos de borrado seguro.
AIFA_TB_003	Se sugiere que el método o estándar implementado brinde la evidencia de la realización de una destrucción de activo primario (dato personal a nivel software) o activo de apoyo (hardware y/o software) lo cual daría garantía de la ejecución de un correcto borrado de datos personales, identificando el servidor público que intervino y el momento en que se realizó.
AIFA_TB_004	Se sugiere que en el ciclo de vida de datos se identifique y documente cómo ocurrirá el borrado de perfil de usuario que haya ingresado sus documentos digitalizados desde un dispositivo y su fotografía.
AIFA_TB_005	Se sugiere que, respecto a la evidencia de borrado, pueda identificarse con precisión cuando se eliminaron las galerías de preseguridad y abordaje, así como el método adoptado.
AIFA_TB_006	Se sugiere, en seguimiento a las recomendaciones sobre los derechos ARCO, que al momento de obtener los datos se especifique el mecanismo para ejercer el derecho de Cancelación de datos en el elemento biométrico del sistema de tratamiento, es decir, describiendo la eliminación de perfiles desde el dispositivo del usuario a través de la app o desde el mostrador o quiosco, según lo requiera el usuario.

Recomendaciones en torno al principio de proporcionalidad

Clave	Recomendación
AIFA_PRO_001	Se sugiere valorar, conforme al criterio de minimización, la pertinencia de utilizar los datos personales existentes en el pasaporte físico, electrónico y credencial para votar o aquellos documentos que pueden utilizarse en razón de que la finalidad principal del Sistema de Procesamiento es permitir el flujo ininterrumpido para el acceso de los pasajeros para pasar a los filtros de pre-seguridad y realizar el embarque a la aeronave de manera rápida y segura.
AIFA_PRO_002	Se sugiere establecer, en el aviso de privacidad, aquellos datos personales que serán recabados en función al medio utilizado para tales efectos, tomando en consideración lo señalado en el principio de proporcionalidad.

AIFA_PRO_003	Se sugiere valorar la eliminación del nombre del vendedor en la información que se recaba en Quioscos de autoservicio (CUSS) y Mostradores de documentación CUPPS-Vdesk, y en su almacenamiento.
AIFA_PRO_004	Se sugiere valorar, en el caso del PDE, su construcción con el menor uso de datos personales posibles de los titulares.
AIFA_PRO_005	Se sugiere valorar los periodos de conservación del PDE considerando que el Aeropuerto Internacional Felipe Ángeles es considerado una instalación estratégica, así como los periodos con los que cuentan las autoridades para la investigación de incidentes, accidentes y delitos; los cuales superan las 24 horas.
AIFA_PRO_006	Se sugiere valorar el PDE únicamente en función a la función de identificación de las personas para facilitar su abordaje, pues tiene implicaciones en materia de seguridad nacional que deben ser considerados como parte de su construcción, uso y conservación.

Recomendaciones en torno al principio de información

Clave	Recomendaciones
AIFA_INF_001	Se recomienda valorar la posibilidad de homologar el contenido de todos los avisos de privacidad que nos fueron remitidos como parte de la evaluación de impacto, a efecto de elaborar uno solo respecto al proceso general de procesamiento del flujo de salida nacional e internacional.
AIFA_INF_002	Se recomienda, a manera de mejora práctica, incluir en los avisos de privacidad integrales, o en su caso, el aviso de privacidad integral homologado, los medios y/o fuentes a través de los cuales se obtienen los datos personales, y asociar el dato personal con cada una de las fuentes.
AIFA_INF_003	Se recomienda verificar que el fundamento establecido en los avisos de privacidad integrales, o en su caso, el aviso de privacidad integral homologado contemple lo establecido en las consideraciones manifiestas por este Instituto en el apartado del principio de licitud del presente documento.
AIFA_INF_004	Se recomienda que en el fundamento legal que se señala en los avisos de privacidad integrales o en su caso, el aviso de privacidad integral homologado se precise su fecha de publicación o, en su caso, de la última reforma o modificación.
AIFA_INF_005	Se recomienda verificar que, en la redacción de los avisos de privacidad integrales, o en su caso, el aviso de privacidad integral homologado se redacte claramente la relación de los documentos de los cuales se obtendrán los datos personales.

AIFA_INF_006	Se recomienda verificar e incluir la fotografía (selfie), país de nacimiento" "país de nacionalidad", "foto del chip del pasaporte" y la "imagen del pasaporte" en el listado de datos personales respecto del proceso en el Mostrador convencional CUPPS-VDesk;
AIFA_INF_007	Se recomienda redactar clara y correctamente los términos que se emplean en los avisos de privacidad, sin usar palabras ambiguas como pudiera ser "biometría facial".
AIFA_INF_008	Se recomienda revisar la inclusión en los avisos de privacidad integrales o en su caso, el aviso de privacidad integral homologado los datos referentes a la imagen del pasaporte (incluida la imagen del pasajero) y el número de pasaporte como datos personales sensibles en función de lo manifestado en el Anexo 2 Experiencia sin contacto.
AIFA_INF_009	Se considera conveniente revisar lo dispuesto en el análisis realizado en el principio de finalidad respecto a las finalidades que persigue la implementación del Sistema a efecto de poder reflejarlo en los avisos de privacidad integrales y simplificados o en su caso, el aviso de privacidad integral y simplificado homologados.
AIFA_INF_010	Se considera conveniente revisar lo dispuesto en el análisis realizado en el apartado de transferencias a efecto de reflejar las transferencias que son efectuadas en los correspondientes avisos de privacidad.
AIFA_INF_011	Se recomienda establecer los mecanismos y medios disponibles para que el titular, en su caso, pueda manifestar su negativa para el tratamiento de sus datos personales para finalidades y transferencias de datos personales que requieren el consentimiento del titular.
AIFA_INF_012	Se recomienda que en los avisos de privacidad simplificados o en su caso, el aviso de privacidad simplificado homologado se informe el sitio, lugar o mecanismo donde se podrá consultar el aviso de privacidad integral.
AIFA_INF_013	Se recomienda que en los avisos de privacidad integrales o en su caso, el aviso de privacidad integral homologado se informen los mecanismos y medios habilitados para atender las solicitudes para el ejercicio de los derechos ARCO y para el de portabilidad, ni el procedimiento o medios para atenderlas.
AIFA_INF_014	Se recomienda que en los avisos de privacidad integrales o en su caso, el aviso de privacidad integral homologado se informe el domicilio completo de la unidad de transparencia, su número y extensión telefónica.

Recomendaciones en torno al principio de responsabilidad

Clave	Recomendación
AIFA RE 001	Se recomienda en su caso actualizar los programas de datos y capacitación al año 2023 considerando en el primero los resultados obtenidos en el análisis de brecha y de riegos.
AIFA_RE_002	Se recomienda actualizar el Programa de capacitación en materia de protección de datos en el que se considere contar con la documentación que acredite la aplicación y actualización de capacitación en materia de protección de datos personales a los servidores públicos involucrados en el procedimiento;
AIFA_RE_003	Se sugiere incluir en el Programa General de Capacitación módulos de sensibilización sobre el uso e importancia de los datos biométricos.
AIFA_RE_004	Se recomienda establecer una periodicidad para la supervisión y vigilancia interna y/o externa del sistema, como pudiera ser cada dos años o antes si es necesario por un cambio sustancial en el tratamiento.
AIFA_RE_005	Seria deseable que en el procedimiento de dudas y quejas se consideren; las áreas administrativas responsables de las dudas, quejas y sugerencias; los plazos de respuesta y la información de contacto.
[redacted]	[redacted]

Recomendaciones en torno al deber de seguridad

Clave	Recomendación
AIFA_SE_001	Se sugiere establecer puntualmente las medidas de seguridad físicas que serán aplicables al Sistema de Procesamiento, esto considerando los equipos utilizados, los medios de recabo de datos biométricos y los riesgos y vulnerabilidades que deriven del análisis de riesgo.
AIFA_SE_002	Se sugiere establecer puntualmente las medidas de seguridad administrativas que serán aplicables al Sistema de Procesamiento, esto

Se eliminan 8 lineas, con fundamento en el artículo 110, fracción I de la LFTAIP; Décimo séptimo de los lineamientos Generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas, en relación con el artículo 5, fracción VI de la Ley de Seguridad Nacional; 47, Bis 4 de la Ley de Aviación Civil, 46 y 47 de la Ley de Aeropuertos y 152 del Reglamento de Aeropuertos.

	considerando los equipos utilizados, los medios de recabo de datos biométricos y los riesgos y vulnerabilidades que deriven del análisis de riesgo.
AIFA_SE_003	Se sugiere establecer puntualmente las medidas de seguridad técnica que serán aplicables al Sistema de Procesamiento, esto considerando los equipos utilizados, los medios de recabo de datos biométricos y los riesgos y vulnerabilidades que deriven del análisis de riesgo.
AIFA_SE_004	Se sugiere identificar plenamente cada uno de los elementos del Sistema de Procesamiento, identificando por cada uno de ellos las medidas de seguridad administrativas, físicas y técnicas que son aplicables de conformidad con los riesgos identificados en cada uno.
AIFA_SE_005	Se sugiere precisar en el documento de seguridad el cargo de las personas, tanto del responsable como de los encargados, que se encuentren vinculados con el funcionamiento y mantenimiento del Sistema de Procesamiento.
AIFA_SE_006	Se sugiere vincular las medidas de seguridad que se implemente a la normatividad aplicable en la materia, como la Ley General y los Lineamientos generales.
AIFA_SE_007	Se sugiere, además de la certificación, identificar cómo se cumplen, las auditorias que se realizan y sus resultados.
AIFA_SE_008	Se sugiere que, además de la plataforma vb orchestra, se verifique que los restantes elementos del Sistema de Procesamiento cuenten con medidas de seguridad administrativas, físicas y técnicas.
AIFA_SE_009	Se sugiere precisar de forma puntual si lo descrito en transferencias se trata de tales o se relaciona con remisiones, atendiendo lo relativo al apartado de transferencias del presente dictamen, y una vez puntualizada esa circunstancia, impactarla en el inventario de datos personales.
AIFA_SE_010	Se sugiere precisar de forma puntual si "Point Consulting", se trata de un desarrollo tecnológico de alguno de los encargados, si se trata de una entidad aparte o una subcontratación y atendiendo lo relativo al apartado de transferencias del presente dictamen, impactar la transferencia o remisión, según sea el caso, en el inventario de datos personales.
AIFA_SE_011	Se sugiere establecer, en el Manual de Organización General o especifico, según corresponda, las funciones de dichos servidores públicos.
AIFA_SE_012	Se sugiere, como parte de las obligaciones contractuales establecidas en el principio de licitud, establecer las funciones específicas a realizar por las personas que designen los encargados para intervenir en el soporte, mantenimiento y demás tareas en relación al Sistema de Procesamiento,

	mismas que deberán ser verificables por parte de los servidores públicos del AIFA.
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]

Recomendaciones en torno al principio de confidencialidad

Clave	Recomendación
AIFA_CONF_001	Es importante que, en todo momento se tengan identificadas claramente las diferentes fases del tratamiento de datos personales considerando todas las finalidades a las que serán sometidos los datos personales y las personas que intervienen en cada etapa, esto pudiera aplicar al personal de las aerolíneas, a efecto de que se establezcan los procedimientos específicos para garantizar el resguardo de la confidencialidad de estos y evitar fuga de información o acceso indebido de los datos personales.
AIFA_CONF_002	Se recomienda la contemplación de cláusulas de confidencialidad pertinentes para tal efecto en los convenios de colaboración que se suscriban, considerando la sensibilidad de los datos, así como en su caso, las nuevas relaciones con encargados o terceros receptores.
AIFA_CONF_003	Se recomienda realizar un análisis de las personas que intervienen en el tratamiento de los datos personales ya sea por parte del responsable o en su carácter de encargados e inclusive sub encargados, a fin de determinar los controles y mecanismos mediante los cuales se garantizara el deber de confidencialidad de estos, esto con la finalidad de que se pueda efectuar el tratamiento de los datos personales a manera de que se garantice su protección más amplia.

Se eliminan 14 lineas, con fundamento en el artículo 110, fracción I de la LFTAIP; Décimo séptimo de los lineamientos Generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas, en relación con el artículo 5, fracción VI de la Ley de Seguridad Nacional; 47, Bis 4 de la Ley de Aviación Civil, 46 y 47 de la Ley de Aeropuertos y 152 del Reglamento de Aeropuertos.

Recomendaciones en torno al ejercicio de los Derechos ARCO

Clave	Recomendaciones
AIFA_ARCO_001	Se recomienda buscar y establecer los mecanismos necesarios con la finalidad de garantizar el debido ejercicio de los derechos ARCO, a través de los procedimientos pertinentes a fin de que la persona titular no se enfrente a barreras para su ejercicio.
AIFA_ARCO_002	Se recomienda considerar en el procedimiento de ejercicio de los derechos ARCO la posibilidad de personas en estado de interdicción.
AIFA_ARCO_003	Se sugiere establecer procedimientos internos para cumplir con sus funciones y para gestionar de manera eficiente las solicitudes de derechos ARCO.
AIFA_ARCO_004	Se recomienda analizar la procedencia del derecho a la portabilidad, verifique que se ajuste a los supuestos, parámetros y procedimientos establecidos en los Lineamientos que establecen los parámetros, modalidades y procedimientos para la portabilidad de datos personales.

Recomendaciones en torno a la relación responsable-encargado

Clave	Recomendación
AIFA_EN_001	Se recomienda definir conforme a la normatividad aplicable en materia de protección de datos personales las figuras que ostentan aquellos que intervienen en el tratamiento de los datos personales, conforme a su carácter de responsable, encargado o inclusive sub encargado, esto a efecto de que se garantice la seguridad mediante las cual se efectuara dicho tratamiento, para lo cual de igual manera una vez definidas estas figuras se puedan contar con los instrumentos jurídicos entre los diversos actores ya sea en términos de la Ley General cuando estas figuran se encuentren intrínsecamente ligadas por parte del AIFA, o cuando se vinculen entre empresas del sector privado conforme a lo estipulado en la normatividad para este sector, siendo la LFPDPPP.
AIFA_EN_002	Se recomienda observar el cumplimiento de las obligaciones en materia de datos personales relacionadas con la relación responsable-encargado e inclusive sub-encargado, en los convenios u otros instrumentos jurídicos, estableciendo cláusulas con las siguientes obligaciones del encargado: o Realizar el tratamiento de los datos personales conforme a las instrucciones del responsable;

	o Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por el responsable; o Implementar las medidas de seguridad conforme a los instrumentos jurídicos aplicables; o Informar al responsable cuando ocurra una vulneración a los datos personales que trata por sus instrucciones; o Guardar confidencialidad respecto de los datos personales tratados; o Suprimir o devolver los datos personales objeto de tratamiento una vez cumplida la relación jurídica con el responsable, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales; o Abstenerse de transferir los datos personales salvo en el caso de que el responsable así lo determine, o la comunicación derive de una subcontratación, o por mandato expreso de la autoridad competente; o Permitir al INAI o al responsable realizar verificaciones en el lugar o establecimiento donde lleva a cabo el tratamiento de los datos personales; o Colaborar con el INAI en las investigaciones previas y verificaciones que lleve a cabo en términos de lo dispuesto en la LGPDPPSO y los Lineamientos Generales, proporcionando la información y documentación que se estime necesaria para tal efecto, y o Generar, actualizar y conservar la documentación necesaria que le permita acreditar el cumplimiento de sus obligaciones.
AIFA_EN_003	Se recomienda establecer mecanismos para verificar que las empresas que prestan servicios de cómputo en la nube cumplen con sus obligaciones en torno al tratamiento de datos personales establecidas en el Contrato de servicios que fue compartido y documentar cualquier incumplimiento.

Recomendaciones en torno al cómputo en la nube

Clave	Recomendaciones
AIFA_CN_001	Se recomienda solicitar al proveedor de servicios sus Términos y condiciones que rigen el tratamiento del contenido, para asegurarse que el responsable tiene el control completo del contenido; que le permita cumplir con los principios y deberes aplicables que establece la Ley General y demás normatividad que resulte aplicable. En este sentido, resulta recomendable verificar que, dentro de dichos términos y condiciones, se permita al responsable limitar el tipo de tratamiento de los datos personales.

AIFA_CN_002	Se recomienda verificar que los proveedores de servicios sean transparentes sobre los subcontratados que utilizan para procesar la información sobre la que prestan los servicios.
AIFA_CN_003	Se recomienda que los Términos y condiciones del proveedor de servicios, no incluyan condiciones en la prestación del servicio que le autoricen o permitan asumir la titularidad o propiedad de la información sobre la que preste el servicio.
AIFA_CN_004	Se recomienda verificar que el proveedor de servicios implemente estándares de seguridad apropiadas en los servicios que los responsables utilizan para los datos personales.
AIFA_CN_005	Se recomienda verificar en los términos y condiciones u otros mecanismos del proveedor de servicios, la forma en la que el responsable podrá conocer de cambios o modificaciones de los términos o condiciones del proveedor
AIFA_CN_006	Se recomienda verificar que el proveedor de servicios permita al responsable eliminar su contenido bajo demanda. Esto tomando en consideración que, los responsables deberán de proceder a la supresión y eliminación de los datos personales sujetos a tratamiento, una vez concluida su finalidad.
AIFA_CN_007	Se recomienda verificar que el proveedor de servicios proporcione al responsable herramientas para controlar el acceso a su contenido en la nube, incluyendo datos personales.

Recomendaciones en torno a transferencias

Clave	Recomendación
AIFA_TR_001	Una vez que se definan las figuras con las cuales se ostentarían todos aquellos que intervienen en el tratamiento de los datos personales, en apego a la normatividad en materia de protección de datos personales, la Ley General en su carácter de Responsable, Encargado y Subencargado, se recomienda definir si se efectuarían transferencias o remisiones de datos, esto a efecto de que se observe la normatividad antes señalada e inclusive la normatividad del sector privado en el supuesto de que se efectúe transferencias o remisiones entre empresas de este sector.
AIFA_TR_002	Se recomienda establecer el procedimiento y mecanismos para solicitar el consentimiento, expreso y por escrito para la realización de las transferencias que se llevarán a cabo a través de las modalidades establecidas por parte del AIFA.

AIFA_TR_003	Se recomienda establecer en los convenios de colaboración cláusulas relativas al cumplimiento en materia de protección de datos personales, en el que se incluya lo siguiente: ○ Realizar tratamiento de datos personales, por las partes, en términos de las normatividades que les facultan para ello y de conformidad con el artículo 34 de la Ley General mediante el respectivo sistema de gestión y documento de seguridad en la que se adoptan estándares nacionales e internaciones, así como buenas prácticas en la materia y 19 de la Ley Federal de Datos y 57 y 59 del Reglamento, en el caso de responsables del sector privado. ○ Con relación al documento de seguridad reconocer que se tuvo conocimiento de los elementos que lo integran en lo que corresponda al tratamiento de datos que derive del cumplimiento del objeto del Convenio. ○ Establecer la responsabilidad de las partes sobre las bases de datos que se generen con motivo de la celebración del Convenio de colaboración, cuyo tratamiento deberá apegarse a la normatividad en la materia; así como llevar a cabo el cumplimiento de principios, deberes y obligaciones establecidas en la Ley General, Ley Federal de Datos y la normatividad que de estos derive. ○ Reconocer el carácter de cada una de las partes como responsables del tratamiento de datos personales de manera independiente en lo que respecta a su régimen de protección de datos personales. ○ Reconocer el tratamiento de datos personales de datos personales sensibles y la obligación de las partes de realizar las adecuaciones necesarias a fin de que las medidas de seguridad sean acordes atendiendo a las características particulares de la información. ○ Establecer el compromiso de notificar vulneraciones de datos personales, así como realizar las acciones encaminadas a realizar un proceso de revisión exhaustiva sobre las vulneraciones y determinar la afectación que puedan sufrir los titulares. ○ Establecer las obligaciones de las autoridades y sector privado, como terceros receptores de los datos personales: ▪ Llevar a cabo el tratamiento de datos personales en términos de lo establecido por la Secretaría en su aviso de privacidad y asumir el carácter de responsable a partir de que se materialice la transferencia de los datos personales, obligándose a proteger los

	datos personales conforme a los principios, deberes y demás obligaciones previstas en la Ley General, Ley Federal de Datos. ▪ Elaborar y poner a disposición de los titulares el/los aviso(s) de privacidad los cuales deberán ser validados por las partes para efectos de dar cumplimiento a lo establecido en el artículo 115 de los Lineamientos Generales y 36 de la Ley Federal y 68 del Reglamento, y cumplir con los elementos informativos obligatorios y en las modalidades que sea necesario. ▪ No compartir los datos personales con terceros, con excepción de las autoridades competentes. ▪ Conservar los datos personales de manera bloqueada hasta que se agoten los plazos legales que resulten aplicables, una vez que se dé cumplimiento a las obligaciones del Convenio y se agoten las finalidades que dieron origen al tratamiento de los datos personales. ▪ Contar con las medidas de seguridad necesarias para el cumplimiento de las obligaciones que derivan del deber de seguridad, especialmente aquellas que se refieren a los medios y mecanismos para realizar las comunicaciones de datos personales. o Reconocer el compromiso de las partes de no realizar ningún uso posterior de los datos personales que le son entregados o transferidos, una vez que se cumpla con las obligaciones del Convenio, y sólo conservar los datos personales de manera bloqueada hasta que se agote el plazo legal, procediendo a su borrado seguro. o Adoptar esquemas de mejores prácticas en protección de datos personales como pueden ser la implementación de acciones preventivas.
AIFA_TR_004	Se sugiere considerar en los convenios de colaboración el establecer una cláusula específica en la que se precise la responsabilidad sobre la atención del ejercicio de cualquiera de los derechos ARCO, considerando que el responsable es quien tenga en su posesión los datos del titular.

Recomendaciones en torno a los datos biométricos

Clave	Recomendación
AIFA_Bio_001	Se recomienda identificar el tipo de datos personales sujetos a tratamiento y, con base en ello, dar el tratamiento que les corresponda, de conformidad con las precisiones realizadas previamente. Esto con la finalidad de asegurar el cumplimiento de los principios y deberes en la materia.

AIFA_Bio_002	Se recomienda buscar la manera de garantizar la implementación de medidas que aseguren que los datos personales cumplan con las características de ser exactos, completos, pertinentes, actualizados y correctos que, para el caso de datos biométricos la exactitud en la recogida y al establecer el vínculo entre la persona y sus datos en el registro, permitirán prevenir la usurpación de identidad.
AIFA_Bio_003	Particularmente, por lo que hace a remisiones o transferencias de datos biométricos, se recomienda identificar la interoperabilidad entre las bases de datos de las que se pretende realizar dicho tratamiento, así como establecer medidas de seguridad adecuadas, pertinentes y suficientes proporcionales a la alta sensibilidad y riesgos que estos datos tienen por sus características.

X. Consideraciones finales.

PRIMERA. En términos de lo señalado en el apartado II, el presente dictamen se emite con la salvedad de que para su emisión se tomaron en cuenta los datos e información proporcionada por el AIFA, por lo que la responsabilidad respecto a las manifestaciones, abstenciones o eventuales omisiones, son responsabilidad exclusiva del AIFA como sujeto obligado en términos del artículo 1 párrafo quinto de la Ley General y del artículo 30 párrafo segundo de las Disposiciones administrativas.

De manera conjunta con la notificación del presente dictamen, podrá llevarse a cabo una reunión para la presentación y explicación del dictamen, así como de las recomendaciones no vinculantes contenidas en el mismo, ello, sin perjuicio de que, en caso de requerir aclaración respecto a algún elemento contenido en el presente dictamen, pueda formularse una consulta por escrito para tales efectos; en caso de requerir asesoría o aclaración por escrito, se le sugiere formular su solicitud dentro de los diez días siguientes a la notificación del presente dictamen, en términos de lo previsto por los artículos 9, 74 al 79, 89, fracciones II, XII, XVI, de la Ley General, 32 de la Ley Federal de Procedimiento Administrativo, aplicado de manera supletoria; y, 42, fracciones II, IV y V, del Estatuto Orgánico de este Instituto.

SEGUNDA. La Dirección General de Normatividad y Consulta, en términos de lo previsto por los artículos 32 de las Disposiciones administrativas, y 42 fracción V del Estatuto Orgánico, queda a su disposición para asesorarle en la implementación de las recomendaciones del presente dictamen de la evaluación de impacto en la protección de datos personales, en el entendido que, de considerarlas pertinentes, lleve a cabo su implementación a la brevedad respecto de las que resulte factible su implementación, así como aquellas, que por el momento no puedan ser

implementadas, pero sí registradas dentro del Plan de Trabajo o Programa de Protección de Datos Personales que corresponda.

TERCERA. Con independencia de las recomendaciones no vinculantes señaladas en el presente dictamen, es menester considerar que las mismas fueron realizadas tomando en cuenta la información remitida; por lo que, ante la implementación del sistema, y ante los posibles cambios normativos y técnicos que dicha implementación pueda demandar, se estaría frente a la obligación de valorar la elaboración y presentación de una nueva evaluación de impacto, en términos de lo dispuesto por el artículo 10 de las Disposiciones administrativas.

CUARTA. En caso de que se considere que en la citada evaluación de impacto existe o se contiene información susceptible de constituir información clasificada, la Dirección General pone a su disposición las documentales proporcionadas para la tramitación del presente dictamen, por medio del titular del área que la presentó o en su caso a los servidores públicos autorizados para recibir dicha información.

El presente documento se emite en términos de lo dispuesto por los artículos 25, primer párrafo, fracción XIII, segundo párrafo, 29 fracciones XXX y XL, y, 42 fracciones IV y XIII del Estatuto Orgánico, por parte del Director General de Normatividad y Consulta, Luis Ricardo Sánchez Hernández.

PA/LIPDR-EHS/PHM-FOMP/ALQP-PBM