

## PROGRAMA DE PROTECCIÓN DE DATOS PERSONALES.

---

**GRUPO AEROPORTUARIO, FERROVIARIO, DE SERVICIOS  
AUXILIARES Y CONEXOS, OLMECCA-MAYA-MEXICA, S.A. DE  
C.V.**

**Noviembre 2025.**

## Contenido

Capítulo I. <b>Presentación.</b> .....	3
Capítulo II. <b>Introducción.</b> .....	4
Capítulo III. <b>Glosario.</b> .....	6
Capítulo IV. <b>Marco Normativo.</b> .....	9
Capítulo V. <b>Alcance</b> .....	10
Capítulo VI. <b>Objetivos.</b> .....	12
Capítulo VII. <b>Responsabilidades del Comité de Transparencia.</b> .....	12
Capítulo VIII. <b>Líneas estratégicas para la gestión de datos personales.</b> .....	13
Estrategia I. <b>Sensibilización.</b> .....	13
Estrategia II. <b>Desarrollo de competencias.</b> .....	14
Estrategia III. <b>Implementación, operación, revisión, mantenimiento y mejora de las acciones diseñadas para el tratamiento y la seguridad de los datos personales.</b> .....	14
Capítulo IX. <b>Ciclo de Vida de los Datos Personales.</b> .....	15
Capítulo X. <b>Desarrollo de las Líneas Estratégicas para la Gestión de Datos Personales.</b> .....	16
Directriz I. <b>Sensibilización.</b> .....	16
Directriz II. <b>Desarrollo de Competencias.</b> .....	17
Directriz III. <b>Implementación, operación, revisión, mantenimiento y mejora de las acciones diseñadas para el tratamiento y la seguridad de los datos personales.</b> .....	17
Acción I. <b>Observancia obligatoria de los principios rectores.</b> .....	17
Acción II. <b>Cumplimiento de los deberes de Confidencialidad y Seguridad.</b> .....	17
Capítulo XI. <b>Desarrollo de las Medidas de Seguridad.</b> .....	20
Capítulo XII. <b>Mejora Continua del Programa.</b> .....	24
Capítulo XIII. <b>Sanciones.</b> .....	25
Capítulo XIV. <b>Publicación.</b> .....	26
Capítulo XV. <b>Apoyo e Impulso al Programa</b> .....	26
Capítulo XVI. <b>Interpretación.</b> .....	26
Capítulo XVII. <b>Revisión y Ajuste.</b> .....	26
Capítulo XVIII. <b>Vigencia.</b> .....	27



## **Capítulo I. Presentación.**

Los constantes avances tecnológicos, la inmediatez en la que transita la información y la creciente competencia, provoca que las empresas, tanto públicas como privadas, se vean en la necesidad de adaptarse rápidamente a los cambios y afrontar nuevos retos.

La tecnología no debe asumirse como un problema, sino como una posibilidad de que la información sea rápida, fluida, organizada, usada y almacenada a gran escala, en bases de datos sólidas.

Este gran flujo de información está compuesto de una cantidad importante de datos personales, por lo que es crucial comprender cómo la tecnología impacta la privacidad y, en consecuencia, tomar las medidas necesarias para proteger los datos personales en esta era digital. La tecnología moderna ha transformado la forma en que se recopilan, almacenan y utilizan los datos personales, generando tanto oportunidades como desafíos.

Es por lo anterior, que el Grupo Aeroportuario, Ferroviario de Servicios Auxiliares y Conexos, Olmeca-Maya-Mexica, S.A. de C.V. (GAFSACOMM), para efectos de comercialización *Grupo Mundo Maya*, busca, a través del presente Programa de Protección de Datos Personales, brindar herramientas prácticas de conocimiento, para que las personas servidoras públicas que laboran en él, puedan conocer e identificar en sus actividades y procedimientos cotidianos: qué son los datos personales, su importancia, los principios y deberes que deben aplicar para su tratamiento, cuáles son los riesgos que los amenazan, cómo protegerlos y en caso de no hacerlo, sensibilizarlos sobre el impacto que pueden provocar en las personas titulares de los datos y en la reputación de la organización, así como las sanciones a las que se pueden hacer acreedoras por no atender las disposiciones normativas.



## Capítulo II. **Introducción.**

El artículo 6, apartado "A", fracción II de la Constitución Política de los Estados Unidos Mexicanos, fija las bases respecto a la información de la vida privada y los datos personales, por lo que éstos serán protegidos en los términos y con las excepciones que fijen las leyes. Para tal efecto, otorga facultades suficientes a los sujetos obligados para su atención.

Con base en ello, se publicó, en el Diario Oficial de la Federación (DOF), el 26 de enero de 2017 la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, y posteriormente los Lineamientos Generales de Protección de Datos Personales para el Sector Público (Lineamientos Generales)<sup>1</sup>, instrumentos que señalan que todas las dependencias y entidades de la Administración Pública Federal, son considerados sujetos obligados, con el carácter de Responsable, motivo por el cual, siempre que obtengan y den tratamiento de datos personales, tienen la obligación de apegarse a los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad; así como establecer las medidas de seguridad de carácter administrativo, físico y técnico que garanticen la confidencialidad, integridad y disponibilidad de los datos personales.

En concordancia con la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, el 28 de septiembre de 2018, se publicó en el DOF, el Decreto por el que se promulga el Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal (Convenio 108) y su protocolo relativo a las Autoridades de Control y a los Flujos Transfronterizos de Datos, del cual México es parte, por lo que su observancia es de carácter vinculante.

Posteriormente, el 20 de diciembre de 2024 se publicó en el Diario Oficial de la Federación la Reforma en Materia de Simplificación Orgánica y el 20 de marzo de 2025, se expidieron las nuevas leyes generales en materia de transparencia, acceso a la información y protección de datos personales, a través de las cuales se extingue al Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), y sus funciones de Autoridad Garante en materia de protección de datos personales, fueron conferidas a la Unidad de Protección de Datos Personales, adscrita a la Secretaría Anticorrupción y Buen Gobierno.

Cabe mencionar que la expedición de la nueva Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPO), no trastocó los principios, deberes, obligaciones, derechos y procedimientos que rigen el tratamiento de la información de carácter personal, siendo el caso que, entre las acciones que deberán realizar los

<sup>1</sup> Los presentes Lineamientos Generales de Protección de Datos Personales para el Sector Público siguen en operación, no obstante, la extinción del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales; por lo que, en su momento, la Autoridad Garante emitirá las disposiciones normativas correspondientes.



responsables del tratamiento de datos personales, para cumplir con el deber de seguridad, está la elaboración de políticas y programas de protección de datos personales, obligatorios y exigibles al interior del GAFSACOMM.

Con base en las facultades otorgadas a citada autoridad, el 01 de octubre de 2025, este Grupo Aeroportuario fue incluido en el Padrón de Sujetos Obligados en materia de protección de datos personales competencia de la Secretaría Anticorrupción y Buen Gobierno, por lo cual esta Secretaría de Estado, funge como Autoridad responsable de garantizar el derecho a la protección de los datos personales en posesión de este Grupo Aeroportuario.



### Capítulo III. Glosario.

**Auditoría:** Proceso sistemático, independiente y documentado para obtener evidencias y evaluarlas de manera objetiva para determinar el grado de cumplimiento de los criterios preestablecidos para la misma.

**Autoridad Garante:** Secretaría Anticorrupción y Buen Gobierno, a través de la Unidad de Protección de Datos Personales.

**Aviso de privacidad:** Documento puesto a disposición de la persona titular de la información de forma física, electrónica o en cualquier formato generado por el GAFSACOMM, a partir del momento en el cual se recaben sus datos personales, con el objeto de informarle los propósitos del tratamiento de los mismos.

**Bases de datos:** Conjunto ordenado de datos personales bajo criterios determinados, con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización.

**Bloqueo:** Es el periodo en el que los datos personales no podrán ser objeto de tratamiento, hasta que haya transcurrido el plazo de prescripción legal o contractual de éstos, posteriormente se procederá a su cancelación.

**Consentimiento:** Manifestación de la voluntad libre, específica e informada de la persona titular de los datos, mediante la cual se efectúa el tratamiento de los mismos.

**Comité de Transparencia:** Instancia a la que hace referencia el artículo 39 de la Ley General de Transparencia y Acceso a la Información Pública.

**Datos personales:** Cualquier información concerniente a una persona física identificada o identificable. Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información. Los datos personales más relevantes para este Grupo pueden ser consultados en el Catálogo disponible en la siguiente liga:

<https://grupomundomaya.com/ObligacionesDeTransparencia/UnidadDeTransparencia/Cat%C3%A1logo%20de%20Datos%20Personales.pdf>

**Datos personales sensibles:** Aquellos que se refieran a la esfera más íntima de la persona titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para su integridad. De manera enunciativa más no limitativa, se consideran sensibles los datos personales que puedan revelar aspectos como origen racial o étnico, estado de



salud presente o futuro, información genética, creencias religiosas, filosóficas, morales y opiniones políticas y preferencia sexual.

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

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

**Fuentes de acceso público:** Aquellas bases de datos, sistemas o archivos que por disposición de ley puedan ser consultadas públicamente cuando no exista impedimento por una norma limitativa y sin más exigencia que, en su caso, el pago de una contraprestación, tarifa o contribución. No se considerará fuente de acceso público cuando la información contenida en la misma sea obtenida o tenga una procedencia ilícita, conforme a las disposiciones establecidas por la presente Ley y demás normativa aplicable.

**GAFSACOMM y/o Grupo Aeroportuario:** Grupo Aeroportuario, Ferroviario de Servicios Auxiliares y Conexos, Olmeca-Maya-Mexica, S.A. de C.V., para efectos de comercialización *Grupo Mundo Maya*.

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

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

**Persona Encargada:** Persona física o jurídica, pública o privada, ajena al Grupo, que sola o conjuntamente con otras, trate datos personales a nombre y por cuenta del GAFSACOMM, como Responsable.

**Persona Titular:** Sujeto a quien corresponden los datos personales.

**Programa:** Programa de Protección de Datos Personales.

**Remisión:** Toda comunicación de datos personales realizada exclusivamente entre el Responsable y la persona encargada, dentro o fuera del territorio mexicano.





**Responsable:** Para el presente documento es el GAFSACOMM, al ser un sujeto obligado, que decide sobre el tratamiento de los datos personales que posee.

**Revisión:** Actividad estructurada, objetiva y documentada, llevada a cabo con la finalidad de constatar el cumplimiento continuo de los contenidos establecidos en este Programa.

**Riesgo:** Combinación de la probabilidad de un evento y su consecuencia desfavorable.

**Sujeto obligado:** Cualquier autoridad, agencia, comisión, comité, corporación, ente, entidad, institución, órgano, organismo o equivalente de los poderes Ejecutivo, Legislativo y Judicial de los tres niveles de gobierno, órganos constitucionalmente autónomos, partidos políticos, fideicomisos y fondos públicos, así como cualquier persona física, moral o sindicato que reciba y ejerza recursos públicos o realice actos de autoridad en los referidos niveles de gobierno.

**Supresión y/o cancelación:** La baja archivística de los datos personales conforme a la normativa archivística aplicable, que resulte en la eliminación, borrado o destrucción de los datos personales bajo las medidas de seguridad previamente establecidas por el GAFSACOMM.

**Transferencias:** Toda comunicación de datos personales dentro o fuera del territorio mexicano, realizada a persona distinta de la persona titular, del GAFSACOMM o la persona encargada.

**Tratamiento:** Cualquier operación o conjunto de operaciones efectuadas mediante procedimientos manuales o automatizados aplicados a los datos personales, relacionadas con la obtención, uso, registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de datos personales.

**Unidad Administrativa:** Área y/o Unidad de Negocio, a la que se le confiere atribuciones específicas en el Manual de Organización General del GAFSACOMM.

**Unidad de Transparencia (U.T.):** Instancia a la que hace referencia el artículo 41 de la Ley General de Transparencia y Acceso a la Información Pública.





#### **Capítulo IV. Marco Normativo**

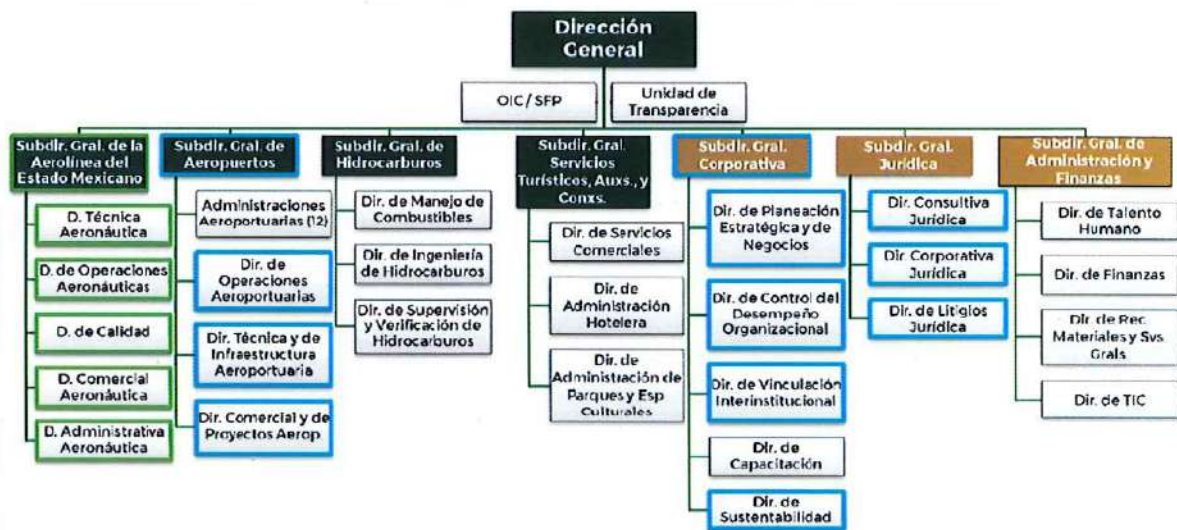
- Constitución Política de los Estados Unidos Mexicanos.
- Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal, hecho en Estrasburgo, Francia, el veintiocho de enero de mil novecientos ochenta y uno.
- Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, publicada en el Diario Oficial de la Federación el 20 de marzo de 2025.
- Ley General de Transparencia y Acceso a la Información Pública, publicada en el Diario Oficial de la Federación el 20 de marzo de 2025.
- Ley General de Responsabilidades Administrativas, publicada en el Diario Oficial de la Federación el 18 de julio de 2016, y sus reformas posteriores.
- Ley General de Archivos, publicada en el Diario Oficial de la Federación el 15 de junio de 2016, y sus reformas posteriores.
- Lineamientos Generales de Protección de Datos Personales para el Sector Público, publicados en el Diario Oficial de la Federación el 26 de enero de 2018, y sus reformas posteriores.
- Manual de Organización General del Grupo Aeroportuario, Ferroviario, de Servicios Auxiliares y Conexos Olmeca-Maya-Mexica, S.A. de C.V., publicado en el Diario Oficial de la Federación el 04 de agosto de 2025.



## Capítulo V. Alcance

El presente Programa de Protección de Datos Personales, es de observancia obligatoria para todas las Unidades Administrativas que conforman el GAFSACOMM, que realizan tratamientos de datos personales en ejercicio de sus atribuciones y funciones.

En este sentido, las Unidades Administrativas a las que se hace referencia, son de conformidad con el Manual de Organización General del GAFSACOMM<sup>2</sup>, las siguientes<sup>3</sup>:



El Grupo Aeroportuario administra un total de 43 Unidades de Negocio, consistentes en 12 aeropuertos, 7 hoteles, 4 parques, 2 museos y 18 estaciones de combustible, los cuales se detallan a continuación:

Aeropuertos.	Hoteles.	Parques.	Museos.	Estaciones de Combustible.
1. Campeche.	1. Calakmul.	1. Del Jaguar.	1. De los Ferrocarriles.	1. Campeche.

<sup>2</sup> El Manual de Organización General del GAFSACOMM, S.A. de C.V., publicado en el Diario Oficial de la Federación el 04 de agosto de 2025, se encuentra vigente; no obstante, se contempla una actualización de las Unidades Administrativas y de sus funciones, a fin de que sea concordante con la estructura orgánica vigente.

<sup>3</sup> Cabe mencionar que la empresa de participación estatal mayoritaria denominada Aerolínea del Estado Mexicano, S.A. de C.V., conservará su personalidad jurídica y patrimonio propios, en términos de las disposiciones jurídicas aplicables, de forma independiente a las de este Grupo Aeroportuario, de conformidad con el resolutive Tercero de la "Resolución por la que se modifica la diversa mediante la cual se autoriza la desincorporación por fusión de las empresas de participación estatal mayoritaria denominadas Aeropuerto Internacional de Palenque, Señor Pakal, S.A. de C.V.; Aeropuerto Internacional de Chetumal, Cuna del Mestizaje, S.A. de C.V.; Aeropuerto Internacional de Tulum, Zamá, S.A. de C.V., y Aerolínea del Estado Mexicano, S.A. de C.V., con el Grupo Aeroportuario, Ferroviario, de Servicios Auxiliares y Conexos, Olmeca-Maya-Mexica, S.A. de C.V., como entidad fusionante, publicada el 17 de agosto de 2023", publicada en el DOF el 02 de mayo de 2025.



Aeropuertos.	Hoteles.	Parques.	Museos.	Estaciones de Combustible.
2. Chetumal.	2. Chichen Itzá.	2. . La Ceiba.	2. Paleontológico de Santa Lucía Quinamétzin.	2. Chetumal.
3. Ciudad Ixtepec.	3. Edzná.	3. La Plancha.		3. Ciudad Ixtepec.
4. Ciudad Victoria.	4. Nuevo Uxmal.	4. Nuevo Uxmal.		4. Ciudad Victoria.
5. Del Norte.	5. Palenque.			5. Del Norte.
6. Nogales.	6. Tulum.			6. Nogales.
7. Nuevo Laredo.	7. Tulum Aeropuerto.			7. Nuevo Laredo.
8. Palenque.				8. Palenque.
9. Puebla.				9. Puebla.
10. Tamiún.				10. Tamiún.
11. Tulum.				11. Tulum.
12. Uruapan.				12. Uruapan.
				13. AIFA.
				14. Lado Aire AIFA.
				15. Lado Tierra Glorieta AIFA.
				16. Lado Tierra Perimetral AIFA.
				17. Lado Aire Tulum.
				18. Lado Tierra Tulum.



## **Capítulo VI. Objetivos.**

El presente programa tiene los siguientes objetivos:

1. Cumplir con las obligaciones que establece la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y los Lineamientos Generales, así como la normatividad que derive de los mismos.
2. Establecer directrices y proporcionar las herramientas necesarias, para garantizar la protección de los datos personales en posesión de las Unidades Administrativas y de Negocios que integran el GAFSACOMM, por medio de la sensibilización, capacitación, implementación, operación, revisión, mantenimiento y mejora de las acciones diseñadas para el tratamiento y la seguridad de los datos personales.
3. Promover la adopción de mejores prácticas en materia de protección de datos personales, a fin de lograr una mayor participación de las personas servidoras públicas que integran el Grupo, en el ejercicio de los derechos ARCOP, así como proporcionar a la ciudadanía la certeza de que sus datos personales en posesión del GAFSACOMM, están siendo tratados de conformidad con lo establecido en el marco normativo.
4. Asesorar a las unidades administrativas responsables y personas encargadas de dar cumplimiento a la normativa en materia de protección de datos personales.

## **Capítulo VII. Responsabilidades del Comité de Transparencia.**

De conformidad con lo establecido en los artículos 77 y 78, fracción I, de la LGPDPPSO, así como en los artículos 47, segundo párrafo, y 48 de los Lineamientos Generales, el Comité de Transparencia funge como órgano de verificación y validación en materia de protección de datos personales al interior del GAFSACOMM.

En consecuencia, el Comité tendrá la responsabilidad de supervisar el cumplimiento del presente Programa y verificar que las acciones implementadas por las Unidades Administrativas y de Negocios, se ajusten a las disposiciones aplicables. En este sentido, el Comité contará únicamente con las siguientes atribuciones respecto de este Programa:

- I. Revisar y validar las propuestas de modificación o mejora al Programa que formule la Unidad de Transparencia, con base en los resultados obtenidos durante su implementación.





- II. Verificar que las Unidades Administrativas y de Negocios del Grupo, implementen adecuadamente las disposiciones del Programa, con base en los informes y evidencias que remita la Unidad de Transparencia.
- III. Recibir y analizar el informe anual presentado por la Unidad de Transparencia, relativo al nivel de cumplimiento del Programa en el ejercicio inmediato anterior.
- IV. Aprobar, en su caso, el Programa Anual de Capacitación, elaborado por la Unidad de Transparencia, pudiendo solicitar el apoyo de las áreas técnicas que estime pertinentes.
- V. Las demás que de manera expresa se establezcan en la normatividad, en el presente Programa y que correspondan en el ámbito de sus atribuciones.

Entre los elementos que pueden incorporarse en el informe se encuentran:

- a) Estadística e información general sobre el cumplimiento de las obligaciones mencionadas en el presente Programa.
- b) Acciones realizadas por el Comité de Transparencia y la Unidad de Transparencia para cumplir con las obligaciones que establece el Programa.
- c) Los resultados de las revisiones y auditorías.

#### **Capítulo VIII. Líneas estratégicas para la gestión de datos personales.**

Las estrategias contenidas en el presente Programa de Protección de Datos Personales del GAFSACOMM, se encuentran alineadas a la normativa institucional, las cuales serán desarrolladas bajo la coordinación de la Unidad de Transparencia, y la tutela del Comité de Transparencia del Grupo. Dichas estrategias fueron diseñadas, a partir del análisis de los mecanismos para el correcto tratamiento de datos personales. En tal virtud, las estrategias del presente Programa son:

##### **Estrategia I. Sensibilización.**

La Unidad de Transparencia emprenderá campañas de sensibilización, promoción y difusión en materia de datos personales, con la finalidad de concientizar a las personas servidoras públicas sobre la importancia de proteger la información personal que tratan, fomentando así una cultura organizacional comprometida con el cuidado y manejo responsable de los





datos, permitiendo incentivar el cumplimiento de las normativas vigentes y la confianza de los ciudadanos.

### **Estrategia II. Desarrollo de competencias.**

La Unidad de Transparencia compartirá la calendarización sobre los temas de capacitación en materia de protección de datos personales y fomentará la participación, con la finalidad de que las personas servidoras públicas cuenten con herramientas adecuadas y conocimientos efectivos, sobre mejores prácticas para la protección de los datos personales y la normatividad que los regula.

### **Estrategia III. Implementación, operación, revisión, mantenimiento y mejora de las acciones diseñadas para el tratamiento y la seguridad de los datos personales.**

La Unidad de Transparencia, en el ámbito de su competencia, realizará un acompañamiento continuo, para el adecuado desarrollo de actividades que deberán realizar las personas servidoras públicas, en cuanto al tratamiento de datos personales, ajustándose a los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad, así como a las acciones para cumplir con los deberes de seguridad y confidencialidad, que en todo momento deberán de responder al marco normativo.

Por lo anterior, es fundamental que las personas servidoras públicas tengan pleno dominio de las obligaciones y acciones que se deben de implementar, en cuanto a la elaboración de los inventarios de tratamiento, avisos de privacidad e integración del documento de seguridad, que es el instrumento que tiene como objeto primordial garantizar la confidencialidad, seguridad, integridad y disponibilidad de los datos personales que obran en poder de las diversas Unidades Administrativas del GAFSACOMM.





## Capítulo IX. Ciclo de Vida de los Datos Personales.

El ciclo de vida de los datos personales comprende las distintas etapas por las que transita la información de las personas titulares, desde el momento en que es obtenida hasta su supresión. Entender este ciclo ayudará a identificar las fases del tratamiento de datos personales, así como implementar buenas prácticas que aseguren la confidencialidad, integridad y disponibilidad de la información durante todo su ciclo de vida.

Conforme a los tratamientos de datos personales realizados por el GAFSACOMM, a través de sus áreas, se identifican las siguientes etapas de ciclo de vida:

- I.** Obtención.
- II.** Almacenamiento.
- III.** Uso.
- IV.** Divulgación, en ciertos casos.
- V.** Bloqueo.
- VI.** Cancelación/Supresión.





## Capítulo X. Desarrollo de las Líneas Estratégicas para la Gestión de Datos Personales.

### Directriz I. Sensibilización.

<p><b>Derecho Constitucional.</b></p> <p>➔</p>	<p>Que las personas servidoras públicas del GAFSACOMM, sean conscientes, receptivas y empáticas acerca de la importancia de proteger, promover y difundir el derecho a la <b>privacidad</b>; esto es, la capacidad de decidir qué información se comparte con otros y cómo se utiliza. En esencia, la <b>privacidad</b> protege el ámbito personal y la intimidad de cada persona, a través de la <b>confidencialidad</b>, la cual garantiza que la información de la persona titular no sea divulgada sin su <b>consentimiento</b>.</p>
<p><b>Principios Rectores.</b></p> <ul style="list-style-type: none"> <li>• Consentimiento.</li> <li>• Información.</li> <li>• Finalidad.</li> <li>• Licitud.</li> </ul> <p>➔</p>	<p>Para cumplir con este derecho constitucional, la Unidad de Transparencia, asesorará a las Unidades Administrativas y de Negocios, respecto a la importancia y el objeto de elaborar los <b>Avisos de Privacidad</b> correspondientes, conforme a sus <b>procesos y ámbitos de competencia</b>; asimismo, sobre la importancia de hacer del conocimiento a la persona titular, qué datos serán recabados y para qué <b>finalidad</b> serán tratados, para que pueda expresar su <b>consentimiento</b>. Con ello, las personas titulares estarán en condiciones de tomar decisiones informadas y, de ser el caso, ejercer sus derechos <b>ARCOP</b>.</p>
<ul style="list-style-type: none"> <li>• Proporcionalidad.</li> <li>• Calidad.</li> </ul> <p>➔</p>	<p>Promover que las personas servidoras públicas traten los datos personales, bajo la premisa <b>"privilegiar los intereses de la persona titular y su expectativa razonable de privacidad"</b>, por lo que además de informar en el Aviso de Privacidad, qué datos recabará y para que fines, únicamente solicitará aquellos <b>datos que resulten necesarios</b>, adecuados y relevantes en relación con las <b>finalidades</b> para las cuales se obtuvieron, éstas deben ser claras, específicas y sin lugar a confusión; asimismo, se deberá revisar que los datos que se recaben estén exactos, completos, correctos y actualizados, con el propósito de que no se altere la veracidad de la información.</p>
<ul style="list-style-type: none"> <li>• Calidad (plazo de conservación).</li> </ul> <p>➔</p>	<p>Se dotará de información necesaria, respecto al <b>ciclo de vida</b> de los datos personales, para que una vez que éstos hayan dejado de ser útiles, para las finalidades que fueron recabados, las personas servidoras públicas, tengan conocimiento que se deberá cumplir con un procedimiento para la conservación, bloqueo y supresión de los datos personales, respecto de cada tratamiento realizado, considerando los plazos y disposiciones legales establecidas en la Ley.</p>
<ul style="list-style-type: none"> <li>• Responsabilidad.</li> </ul> <p>➔</p>	<p>El principio de responsabilidad cierra el círculo con relación a los principios que regulan la protección de los datos personales, el cual implica la obligación del GAFSACOMM, de velar por el cumplimiento del resto de los principios, adoptar las medidas necesarias para su aplicación, y demostrar ante las personas titulares y la Autoridad Garante, que cumple con sus obligaciones en torno a la protección de los datos personales.</p>



**Directriz II. Desarrollo de Competencias.**

La Unidad de Transparencia, llevará a cabo **el desarrollo de competencias**, a través del Programa de Capacitación, el cuál será proyectado al inicio de cada año, con base en el levantamiento de necesidades vinculadas al tratamiento de datos personales, relacionados con las labores cotidianas que realizan las Unidades Administrativas y de Negocios del Grupo, generando con ello un proceso de **capacitación continua**, con carácter formativo, el cual no se limita a un momento específico, sino que, constituye un proceso dinámico y permanente.

Asimismo, se otorgarán asesorías permanentes, talleres, guías, manuales y campañas de sensibilización que ofrezcan información específica, con el fin de apoyar a todas las Unidades Administrativas y de Negocios, en el diseño de acciones concretas orientadas a la protección de datos personales.

Para realizar citadas acciones, se utilizarán las herramientas tecnológicas disponibles, como Microsoft Teams, correo institucional, el Apartado virtual de Protección de Datos Personales del Grupo Aeroportuario, entre otros apartados.

Con esta programación de competencias, además de abonar a la protección de datos personales, se propiciarán las buenas prácticas institucionales, en el manejo de la información en general.

**Directriz III. Implementación, operación, revisión, mantenimiento y mejora de las acciones diseñadas para el tratamiento y la seguridad de los datos personales.****Acción I. Observancia obligatoria de los principios rectores.**

Las personas servidoras públicas Responsables de los sistemas de tratamiento de datos personales, deberán adoptar las medidas necesarias para evitar que se produzca una vulneración a los mismos, para ello deberán respetar los **principios rectores** de la protección de datos personales, los cuales constituyen el pilar mediante el cual se articula este derecho y cuya observancia es de carácter obligatoria para todo aquel que intervenga en el **tratamiento de datos personales**, desde el momento de su obtención hasta la destrucción de los mismos.

**Acción II. Cumplimiento de los deberes de Confidencialidad y Seguridad.**

**A. Deber de Confidencialidad.** Se deben de establecer controles o mecanismos que tengan por objeto que todas aquellas personas servidoras públicas que traten datos personales, **en**



**cualquier fase del tratamiento**, mantengan en secreto la información, así como evitar que sea revelada a personas no autorizadas y prevenir la divulgación no autorizada de la misma. Las personas servidoras públicas **tienen la obligación** de guardar la debida confidencialidad respecto de los datos personales que son tratados en sus Unidades Administrativas, para evitar causar un daño a la persona titular. De no ser así, un tercero no autorizado podría tener acceso a determinada información y hacer mal uso de esta.

Para dar cumplimiento a este deber, el Grupo Aeroportuario a través de la Unidad de Transparencia, ha puesto a disposición de las personas servidoras públicas, la Carta de Confidencialidad, que es el instrumento mediante el cual se establecen los controles dirigidos a asegurar la confidencialidad que deben guardar todas las personas que intervienen en cualquier fase del tratamiento de datos personales.

Dicha Carta puede ser consultada en el Apartado virtual de Protección de Datos Personales, el cual se encuentra en la siguiente dirección:  
<https://grupomundomaya.com/ObligacionesDeTransparencia/UnidadDeTransparencia/Carta%20de%20Confidencialidad.pdf>,

**B. Deber de Seguridad.** La LGPDPSO establece que para una efectiva protección de los datos personales, es necesaria la implementación de un Sistema de Gestión de Seguridad de Datos Personales (Sistema de Gestión), el cual permite **planificar, implementar, monitorear y mejorar** las medidas de seguridad de carácter **administrativo, físico y técnico**, a través de una serie de actividades interrelacionadas **y documentadas**, tomando en consideración los estándares nacionales e internacionales, en materia de protección y seguridad de los datos personales.

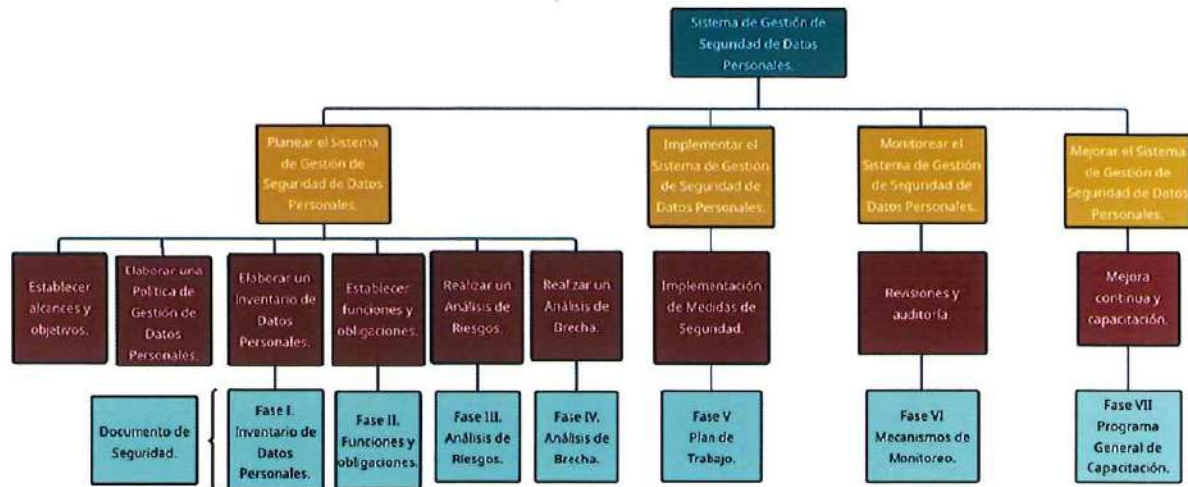
Las personas servidoras públicas con independencia del tipo de sistema en el que se encuentren los datos personales o el tipo de tratamiento que se efectúe, deberán establecer y mantener citadas medidas de seguridad, que permitan proteger dichos datos **contra daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado**, así como garantizar su confidencialidad, integridad y disponibilidad. Esta obligación aplica a los datos personales que conozca y/o a los que tenga acceso durante la relación laboral con el GAFSACOMM, y continuará vigente incluso después de que dicha relación concluya.

A fin de tener claridad sobre las acciones de implementación para la seguridad de los datos personales, se ha considerado importante hacer la distinción entre el Sistema de Gestión y el Documento de Seguridad.

El Sistema de Gestión funciona a través de un ciclo de mejora continua, dividido en 4 fases que consideran 9 pasos o actividades para la seguridad de los datos personales:







Mientras que, el Documento de Seguridad es el instrumento que registra las medidas de seguridad, las cuales ya están contempladas en el Sistema de Gestión, por lo que se concluye lo siguiente:

- a) El Documento de Seguridad surge como consecuencia de la documentación de algunos pasos de la implementación del Sistema de Gestión.
- b) Para la elaboración del **Documento de Seguridad**, resulta indispensable la participación de las personas servidoras públicas Responsables del tratamiento de los datos personales de todas las Unidades Administrativas y de Negocios, en el ámbito de su competencia quienes, para este fin, serán coordinadas por el personal de la Unidad de Transparencia quien orientará y verificará la Integración del documento, mismo que se conformará por las siguientes etapas:
  - I. El inventario de datos personales;
  - II. Funciones y obligaciones de las personas que tratan datos;
  - III. El análisis de Riesgo;
  - IV. El análisis de Brecha;
  - V. El Plan de Trabajo;
  - VI. Los Mecanismos de monitoreo y revisión de las medidas de seguridad, y
  - VII. El Programa General de Capacitación.



## **Capítulo XI. Desarrollo de las Medidas de Seguridad.**

### **A. Inventario de Datos Personales.**

Al momento de iniciar la elaboración del Documento de Seguridad y de los inventarios de datos personales con los diferentes tratamientos realizados en las Unidades Administrativas y/o de Negocios del Grupo Aeroportuario, las personas servidoras públicas encargadas del tratamiento deben dar respuesta a los siguientes cuestionamientos:

#### **A.1. ¿Cómo se obtienen los datos personales?**

A continuación, se han identificado algunos medios, a través de los cuales se puede obtener la información:

- Directamente de la persona titular.
- De manera personal, con la presencia física de la persona titular de los datos personales o su representante.
- Vía telefónica.
- Por correo electrónico.
- Por internet o sistema informático.
- Por escrito presentado directamente en las oficinas del Grupo Aeroportuario y /o de sus Unidades de Negocio.
- Por escrito enviado por mensajería.
- Por transferencia.
- De una fuente de acceso público

#### **A.2. ¿Qué tipo de datos personales se tratan?, ¿son sensibles?**

Una vez identificada la fuente de obtención, se sugiere hacer un listado de los datos personales que se recaban y utilizan para las distintas actividades que realizan las personas servidoras públicas, en el marco de sus facultades y atribuciones legalmente conferidas, siendo importante la distinción de los datos personales sensibles.

#### **A.3. ¿Para qué finalidades se utilizan los datos personales?**

En este punto, será necesario identificar cada una de las finalidades para las cuales se requieren los datos personales. Estas finalidades deben ser concretas, explícitas, lícitas y legítimas, y las mismas se deben correlacionar de manera directa con las actividades que se realizan en las Unidades Administrativas y de Negocios. Asimismo, por cada una de las





finalidades identificadas es necesario recabar el consentimiento de la persona titular de los datos personales, ya sea tácito, expreso y/o expreso por escrito.

**A.4. ¿Quién tiene acceso a la base de datos o archivos (sistemas de tratamiento) y a quién se comunican los datos personales al interior del Sujeto Obligado?**

Se deberá identificar a las personas servidoras públicas que tienen acceso a los datos personales y para qué fin. En este apartado, se deberá especificar el nombre, cargo y las funciones que cada uno realiza en el tratamiento de datos personales, con el objeto de asignar los siguientes roles: propietario, administrador, ejecutor y custodio.

**A.5. ¿Intervienen personas encargadas en el tratamiento de los datos personales?**

Las personas encargadas de datos personales son la persona física o jurídica, pública o privada, ajena al Grupo, que sola o, en conjunto con otras, trata datos personales a nombre y por cuenta del GAFSACOMM, en su carácter de Responsable del tratamiento.

Lo anterior puede ejemplificarse con un proveedor (persona física o moral) que presta servicios de procesamiento de nómina, para lo cual el GAFSACOMM, **tendrá que comunicar los datos personales** de todas las personas servidoras pública, con el fin de dispersar los recursos económicos. El proveedor tratará los datos personales cumpliendo con todos los principios y deberes como si fuera el GAFSACOMM. A esta comunicación de datos se le identifica como **"remisión"**.

Asimismo, será necesario identificar el nombre de la persona Encargada y el número de contrato, pedido o convenio correspondiente.

**A.6. ¿Qué transferencias se realizan o se podrían realizar de los datos personales y con qué finalidad?**

A diferencia de la "remisión" mencionada en el punto anterior, la "transferencia" de datos debe de comunicarse con persona **distinta** a la persona titular, al GAFSACOMM y/o persona encargada.

**A.7. ¿Se difunden los datos personales?**

La difusión de datos personales se refiere a la acción de divulgar o compartir información personal de un individuo **sin su consentimiento**, ya sea de manera intencional o accidental.





Esta divulgación puede tomar diversas formas, desde la publicación en redes sociales hasta la comunicación de datos a terceros. La difusión no consentida de datos personales puede tener graves consecuencias para la privacidad y seguridad de la persona afectada y sanciones para el servidor público que vulnere los datos personales.

Por lo tanto, se debe señalar si los datos personales se difunden y el fundamento jurídico, para hacerlo.

#### **A.8. ¿Cuál es el plazo de conservación de los datos personales?**

Este plazo tendrá que estar definido en los instrumentos de clasificación archivística, por lo que es necesario identificar a qué serie documental pertenecen los archivos o bases de datos en los que están contenidos los datos personales.

#### **A.9. ¿Cómo se suprimen los datos personales?**

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.

Las personas servidoras públicas deberán de adoptar medidas necesarias para mantener exactos, completos, correctos y actualizados los datos personales en su posesión, esto es, políticas, métodos y técnicas orientadas a la supresión definitiva de éstos, de tal manera que la probabilidad de recuperarlos o reutilizarlos sea mínima.

Se deberán de considerar los siguientes atributos en 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 antes citados.
- III. **Favorable al medio ambiente:** Que el método utilizado produzca el mínimo de emisiones y desperdicios que afecten el medio ambiente.

Una vez que concluya el plazo de conservación de estos, 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.



Posterior a atender los anteriores cuestionamientos, se deberá realizar un análisis de riesgo y un análisis de brecha de los datos personales, que consiste en lo siguiente:

#### **B. Análisis de Riesgo.**

Se **deben identificar escenarios de riesgo**, tomando en consideración las amenazas y vulnerabilidades existentes para los datos personales.

Para mayor precisión, el artículo 26 de la Ley General, establece una serie de medidas de seguridad que deben ser consideradas para su implementación, siendo aquellas de carácter administrativo, físico y técnico para la protección de los datos personales, con la finalidad de garantizar la confidencialidad, integridad y disponibilidad de los datos, protegiendo los mismos contra daño, pérdida, alteración, destrucción o una utilización no autorizada de los mismos.

La Unidad de Transparencia, en este rubro, realizará mesas de trabajo para asesorar en lo conducente a las Unidades Administrativas.

#### **C. Análisis de Brecha.**

Se refiere al **proceso de evaluación** de citadas medidas de seguridad administrativas, físicas y técnicas, ya existentes y las que operan correctamente en la organización, **contra** las que serían necesarias tener para **mitigar los riesgos** de seguridad identificados en este análisis, así como las nuevas medidas de seguridad que podrían reemplazar a uno o más controles implementados actualmente.

#### **D. Plan de trabajo.**

Después de realizar los análisis correspondientes de riesgos y de brecha, se debe elaborar un plan de trabajo con la finalidad de implementar las medidas de seguridad faltantes, así como para el cumplimiento cotidiano de las políticas de tratamiento de los datos personales.

#### **E. Mecanismos de Monitoreo y Supervisión.**

De conformidad con los artículos 24 fracción V y 27 fracción VII de la Ley General, el Responsable del tratamiento deberá establecer un sistema de supervisión y vigilancia interna y/o externa, incluyendo auditorías, para comprobar el cumplimiento de las políticas de protección de datos personales y las medidas de seguridad implementadas, así como las amenazas y vulneraciones a las que están sujetos los datos personales. Dichas políticas,



programas, y mecanismos deberán revisarse al menos cada dos años, a excepción de que se lleven a cabo cambios sustanciales en el tratamiento de datos personales.

En ese sentido, el Responsable deberá monitorear de manera continua 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 aquellas 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.

Para tales efectos, el GAFSACOMM implementó los *Mecanismos de Supervisión y Vigilancia en Materia de Datos Personales*, que tienen como finalidad la prevención y la actuación inmediata de eventuales vulneraciones en el tratamiento de datos personales.

Este proceso se secciona en 3 fases:

- A. Mecanismos de Monitoreo y Supervisión;
- B. Mecanismos de Auditoría, y
- C. Mecanismos ante Vulneraciones Concretadas.

Dichos Mecanismos pueden ser consultados en la siguiente liga electrónica:  
<https://grupomundomaya.mx/ObligacionesDeTransparencia/UnidadDeTransparencia/Mecanismos%20de%20Supervisi%C3%B3n%20y%20Vigilancia.pdf>

## Capítulo XII. **Mejora Continua del Programa.**

Con la finalidad de comprobar el cumplimiento del programa, se realizarán las siguientes acciones:

La Unidad de Transparencia requerirá a las Unidades Administrativas y/o de Negocios, la elaboración del aviso de privacidad integral y simplificado, cuando de acuerdo con sus





actividades, funciones y atribuciones realicen tratamiento de datos personales y fomentará que éstas tomen en cuenta las áreas de oportunidad para las medidas de seguridad físicas, administrativas y técnicas, mismas que quedarán establecidas en el Documento de Seguridad.

Una vez que la Unidad de Transparencia cuente con el inventario de datos personales, realizará las recomendaciones que estime conveniente en materia de protección de datos personales, teniendo como finalidad fundamental que las unidades administrativas adopten acciones preventivas y correctivas:

**1. Acciones preventivas que deberán documentarse:** Son aquellas encaminadas a **prever** cualquier incumplimiento a lo establecido en el presente Programa. Por lo que se podrán realizar las siguientes actividades:

- a. Analizar y revisar las posibles causas de incumplimiento;
- b. Determinar qué otras causas de incumplimiento podría desencadenarse a partir de ciertas situaciones de riesgo para el tratamiento de datos personales;
- c. Evaluar las acciones necesarias para evitar que el incumplimiento ocurra;
- d. Determinar e implementar estas acciones;
- e. Documentar los resultados de las acciones tomadas; y
- f. Revisar la eficacia de las acciones preventivas tomadas.

**2. Acciones correctivas que deberán documentarse.** Son aquellas encaminadas a **eliminar** las causas de incumplimiento con relación a lo previsto en el presente Programa. Para las acciones correctivas se podrán llevar a cabo las siguientes actividades:

- a. Analizar y revisar el incumplimiento;
- b. Determinar las causas que dieron origen al incumplimiento;
- c. Evaluar las acciones necesarias para evitar que el incumplimiento vuelva a ocurrir;
- d. Proponer acciones correctivas y establecer un plazo para su cumplimiento;
- e. Documentar resultados de las acciones tomadas; y
- f. Revisar la eficacia de las acciones correctivas tomadas.

### Capítulo XIII. Sanciones.

Cuando la Unidad de Transparencia, tenga conocimiento del incumplimiento de alguna obligación prevista en este Programa, deberá de realizar un exhorto al área, para llevar a cabo las acciones que resulten pertinentes, con el objeto de modificar dicha actuación y evitar incumplimientos futuros o situaciones de riesgo que pudieran ocasionar.





De igual manera, de conformidad con el artículo 105 de los Lineamientos Generales, cuando algún área se niegue a colaborar con la Unidad de Transparencia en la atención de las solicitudes para el ejercicio de los derechos ARCOP, ésta dará aviso al superior jerárquico para que le ordene realizar sin demora las acciones conducentes.

Si persiste la negativa de colaboración, la Unidad de Transparencia lo hará del conocimiento del Comité de Transparencia para que, a su vez, dé vista al Órgano Interno de Control y, se dé inicio el procedimiento de responsabilidad administrativo respectivo.

Por último, las personas servidoras públicas que estén a cargo del tratamiento de datos personales, deberán tener presente que será motivo de sanción las causales establecidas en el artículo 132 de la Ley General.

#### **Capítulo XIV. Publicación.**

El presente Programa estará disponible en el Apartado Virtual de Protección de Datos Personales, del sitio web del Grupo Mundo Maya, ubicado en la siguiente liga, <https://grupomundomaya.com/ProteccionDeDatosPersonales.html>.

#### **Capítulo XV. Apoyo e Impulso al Programa**

El presente Programa se deberá hacer del conocimiento de las Subdirecciones Generales y Unidades de Negocio del GAFSACOMM, a fin de impulsar la debida implementación de éste, en todas las áreas.

#### **Capítulo XVI. Interpretación.**

Los aspectos no contenidos en el presente Programa o que puedan prestarse a diversas interpretaciones, serán discernidos por la U.T.

#### **Capítulo XVII. Revisión y Ajuste.**

La Unidad de Transparencia, será el responsable de mantener actualizado el contenido del presente Programa, de acuerdo con la legislación vigente en la materia.





### **Capítulo XVIII. Vigencia.**

El presente Programa de Protección de Datos Personales estará vigente desde el día siguiente de su aprobación por el Comité de Transparencia del GAFSACOMM.

### **TRANSITORIOS.**

**PRIMERO.** El presente Programa entrará en vigor el día siguiente de su aprobación y deberá publicarse en el Portal Institucional, dentro de los quince días hábiles, posteriores a su aprobación por el Comité.

**SEGUNDO.** La Unidad de Transparencia, publicará y difundirá el Programa en el Apartado Virtual de Protección de Datos Personales de la página Web Institucional, así como al interior del GAFSACOMM.

El Comité de Transparencia del Grupo, de conformidad con lo dispuesto en los artículos 40 de la Ley General de Transparencia y Acceso a la Información Pública y 78 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados; aprobó mediante **Acuerdo CT/14-EXT/20-11-2025-02** en la sesión de fecha **20 de noviembre de 2025**, el presente "Programa de Protección de Datos Personales".



**Licenciado Marcos Santos Acosta**  
Titular de la Unidad de Transparencia y  
Presidente del Comité de Transparencia del  
GAFSACOMM.



**Maestro Luis de la Vega Briones**  
Responsable del Área Coordinadora de  
Archivos del GAFSACOMM.



**Licenciada Angélica Yadira  
de Fuentes Aguirre**  
Suplente del Titular del Órgano Interno  
de Control en el GAFSACOMM.