PROGRAMA EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES DE GRUPO AEROPORTUARIO DE LA CIUDAD DE MÉXICO S.A. DE C.V. (GACM)

Contenido

I. Presentación

El presente Programa en materia de Protección de Datos Personales en observancia a lo previsto en los artículos 30 fracciones I y II de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO) y 47 de los Lineamientos generales de protección de datos personales para el sector público (Lineamientos generales), así como al principio de responsabilidad, se erige como un documento de observancia general al interior de Grupo Aeroportuario de la Ciudad de México, S.A. de C.V. (GACM), que establece los elementos y actividades de dirección, operación y control de todos los procesos que, en el ejercicio de las funciones y atribuciones de las áreas de la entidad impliquen un tratamiento de los datos personales que se encuentren en su posesión, y con ello, garantizar su protección de manera sistemática, continua y en apego a los principios y valores de la entidad establecidos en el Código de Ética de la Administración Pública Federal y Código de Conducta de GACM..

Por tanto, busca constituirse como el documento rector bajo un enfoque de sistema de gestión en materia de protección de datos personales, del cual se deriva el documento de seguridad, políticas y procedimientos en la materia.

De conformidad con el artículo 34 de la LGPDPPSO, un sistema de gestión es un conjunto de elementos y actividades interrelacionadas para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el tratamiento y seguridad de los datos personales, así como, el cumplimiento de los principios, deberes y obligaciones previstos en dicha ley y las demás disposiciones que resulten aplicables en la materia.

El sistema de gestión[1] en el que se basa este programa se apoya en el documento orientador[2] publicado por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), para su elaboración el cual considera cuatro fases (planificar, hacer, verificar y actuar), que a continuación se describen:

[1] El sistema de gestión que se desarrolla atiende lo dispuesto en la ISO/IEC 29100:2011 Information technology – Security techniques – Privacy framework.

[2] http://inicio.ifai.org.mx/SitePages/Documentos-de-Interes.aspx?a=m4

	Elemento	Fase del ciclo PHVA	Actividades
PROCESO	**Metas**	**P**lanificar	Identificar políticas, objetivos, riesgos, planes, procesos y procedimientos necesarios para obtener el resultado esperado por el responsable o encargado (meta).
	Medios de acción	**H**acer	Implementar y operar las políticas, objetivos, planes, procesos y procedimientos establecidos en la fase anterior.
		Verificar	Evaluar y medir los resultados de lo implementado, a fin de verificar el adecuado funcionamiento del sistema de gestión y el logro de la mejora esperada.
		Actuar	Adoptar medidas correctivas y preventivas en función de los resultados y de la revisión realizada, o de otra información relevante, para lograr la mejora continua.

II. Objetivos

El presente programa tiene como objetivos los siguientes:

1. Proveer el marco de trabajo necesario para la protección de los datos personales en posesión del GACM;
2. Cumplir con los principios, obligaciones y deberes establecidos en la LGPDPPSO y los Lineamientos generales, así como la normatividad que derive de los mismos;
3. Establecer los elementos y actividades de dirección, operación y control de los procesos que impliquen el tratamiento de datos personales, a efecto de protegerlos de manera sistemática y continua; y
4. Promover la adopción de mejores prácticas en la protección de datos personales.

III. Responsabilidades

Los artículos 83 y 84, fracción I de la LGPDPPSO y 47, segundo párrafo y 48 de los Lineamientos generales, señalan que el Comité de Transparencia es la autoridad máxima en materia de protección de datos personales y que tiene entre sus funciones la de coordinar, supervisar y realizar las acciones necesarias para garantizar el derecho a la protección de los datos personales en la organización del responsable.

Por su parte, la Unidad de Transparencia (UT) se coordinará con la Subdirección de Sistemas y Procesos, y la Subdirección de Riesgos, que por su naturaleza tienen una relación directa con los procesos internos para la protección de datos personales, para lo siguiente:

I. Elaborar, implementar, difundir y dar seguimiento al programa dentro de la entidad;
II. Proponer cambios y mejoras a partir de la experiencia en su implementación;
III. Asesorar a las áreas en la implementación del programa;
IV. Presentar un informe anual al Comité de Transparencia, en el que se describan las acciones realizadas para cumplir con lo dispuesto en el programa; y
V. Las demás que de manera expresa señale el propio programa.

El informe al que refiere la fracción IV anterior, deberá presentarse en el primer trimestre del año y referirá al ejercicio inmediato anterior. Los elementos mínimos que deberán de incluirse son:

- Acciones realizadas por la Unidad de Transparencia en coordinación con la Subdirección de Sistemas y Procesos, y la Subdirección de Riesgos, para cumplir con las obligaciones específicas que establece el programa.

- Información general sobre el cumplimiento de las obligaciones señaladas en el programa, por parte de las áreas.

- Los resultados de las revisiones y mejoras que deban instrumentarse a partir de la implementación del programa.

Adicionalmente, para el desarrollo de las acciones señaladas, la Unidad de Transparencia se apoya en el Oficial de Protección de Datos Personales, en términos de los artículos 85 segundo párrafo de la LGPDPPSO; 121 y 122 de los Lineamientos generales.

Por su parte, las áreas deberán realizar las acciones necesarias para cumplir con las obligaciones establecidas en el presente programa, y documentos derivados del mismo, así como acuerdos del Comité y requerimientos específicos en la materia por parte de la Unidad de Transparencia, para lo cual deberán asignar los recursos materiales y humanos necesarios, y prever lo que se requiera en sus programas de trabajo.

Adicional a la aprobación del programa por parte del Comité de Transparencia en atención al numeral 47 de los Lineamientos generales, éste **se hará del conocimiento** a la alta dirección, a fin de asegurar su óptimo cumplimiento.

El programa **será de observancia obligatoria para todas las personas servidoras públicas del sujeto obligado** que en el ejercicio de sus funciones traten datos personales.

IV. Alcance

El programa es aplicable a todas las áreas que realicen tratamientos de datos personales.

Asimismo, en virtud de los objetivos del programa establecidos en el marco de la LGPDPPSO, se cubrirán todos los principios, deberes y obligaciones que establece dicha norma para los responsables del tratamiento.

Quedan exceptuados de la aplicación de este programa, los datos personales que se encuentren en los supuestos referidos en los numerales 70 de la LGPDDPSO, 120 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP) y 117 de la Ley Federal de Transparencia y Acceso a la Información Pública (LFTAIP).

Las áreas que integran la organización al 30 de mayo de 2022, y que deberán observar el programa son las siguientes:

- Dirección General
- Dirección Corporativa de Administración
- Dirección Corporativa Jurídica
- Dirección Corporativa de Finanzas
- Dirección Corporativa de Construcción Lado Aire y Edificios Auxiliares
- Dirección Corporativa de Construcción Lado Tierra
- Dirección Corporativa de Coordinación de Estrategia
- Dirección Corporativa Técnica
- Dirección de Relaciones Institucionales y Programas Sociales
- Subdirección de Transparencia y Datos Abiertos
- Subdirección de Riesgos

Nota: A la fecha, GACM se encuentra en proceso de actualización de puestos y perfiles, se destaca que la Dirección de Relaciones Institucionales y Programas Sociales actualmente no cuenta con personal y se encuentra en encargaduría de la Titular de la Dirección Corporativa de Administración; mientras que la Dirección Corporativa de Construcción Lado Aire y Dirección Corporativa Técnica están bajo la responsabilidad del encargado de la Dirección Corportiva de Contrucción Lado Tierra.

V. Instrumentos de Gestión de los Datos Personales

Los dos principales instrumentos utilizados y que deben ser observados por las áreas para cumplir con los principios, deberes y obligaciones que prevé la LGPDPPSO son las *Políticas de Protección de Datos Personales* y el *Documento de Seguridad en materia de protección de datos personales*.

a. Políticas de Protección de Datos Personales

El artículo 33 fracción I de la LGPDPPSO establece que, para mantener las medidas de seguridad para la protección de los datos personales, el responsable deberá realizar entre diversas actividades la de 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.

Ahora bien, las *Políticas de Protección de Datos Personales del GACM* se integran de la siguiente manera:

I. Introducción
II. Objetivo
III. Marco normativo
IV. Principios, deberes, derechos y demás obligaciones en la materia
    A. Principios
    B. Deberes
    C. Derechos
V. Roles y responsabilidades específicas de las personas servidoras públicas
VI. Aviso de privacidad y ciclo de vida de los datos personales
    A. Aviso de privacidad
    B. Ciclo de vida de los datos personales
VII. Monitoreo y revisión de medidas de seguridad
    A. Mecanismos de monitoreo

b. Documento de Seguridad en materia de protección de datos personales

El Documento de Seguridad es el 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.

El artículo 35 de la LGPDPPSO determina que el responsable deberá elaborar un documento de seguridad que contenga, al menos, lo siguiente:

- El inventario de datos personales y de los sistemas de tratamiento;
- Las funciones y obligaciones de las personas que traten datos personales;
- El análisis de riesgos;
- El análisis de brecha;

- El plan de trabajo;
- Los mecanismos de monitoreo y revisión de las medidas de seguridad, y
- El programa general de capacitación.

En GACM el *Documento de Seguridad* se integra de la siguiente manera:

I. Introducción
II. Marco normativo
III. Objetivo
IV. Ámbito de aplicación
V. Inventario de datos personales y de los sistemas de tratamiento
VI. Funciones y obligaciones de las personas que traten datos personales
VII. Análisis de riesgos, análisis de brecha y Plan de Trabajo
VIII. Los mecanismos de monitoreo y revisión de las medidas de seguridad
IX. El programa general de capacitación
X. Actualización del documento de seguridad
XI. Glosario

APÉNDICE I. Metodología de gestión de riesgos para datos personales y análisis brecha.

Ahora bien, para instrumentar el Documento de Seguridad se deben considerar los puntos señalados en el artículo 35 de la LGPDPPSO por lo que cada apartado se deberá construir observando lo siguiente:

A. Inventario de tratamientos de datos personales

Para el debido cumplimiento de las obligaciones cada una de las áreas realiza un diagnóstico de los tratamientos de datos personales que llevan a cabo.

El diagnóstico en mención se basa en la elaboración de un inventario con la información básica de cada tratamiento de datos personales reportados por cada una de las áreas del GACM.

Por inventario de tratamientos de datos personales se entenderá el control documentado que se llevará de los tratamientos que realizan las áreas del GACM, con orden y precisión.

El inventario de datos personales al que hace referencia la LGPDPPSO en los artículos 33, fracción III, 35, fracción I, y 58 de los Lineamientos Generales, identifica los siguientes elementos relevantes:

- ¿Qué tratamientos de datos personales realiza la unidad administrativa?

- ¿Qué unidad administrativa está a cargo de estos procesos y que por tanto sea la administradora de las bases de datos o archivos que se generen con motivo de dichos tratamientos?

Una vez identificados los tratamientos de los cuales está a cargo la unidad administrativa, se determinó lo siguiente, de acuerdo con el ciclo de vida de los datos personales.

1) ¿Cómo se obtienen los datos personales?

- Directamente del titular
    - De manera personal, con la presencia física del titular de los datos personales o su representante, en su caso
    - Vía telefónica

  - Por correo electrónico
  - Por internet o sistema informático
  - Por escrito presentado directamente en las oficinas del sujeto obligado
  - Por escrito enviado por mensajería
- Mediante una transferencia
  - Quién transfiere los datos personales y para qué fines
  - Medios por los que se realiza la transferencia
- De una fuente de acceso público

2) ¿Qué tipo de datos personales se tratan? ¿son sensibles?
3) ¿Dónde se almacenan y realiza el tratamiento de los datos personales?
4) ¿Para qué finalidades se utilizan los datos personales?
5) ¿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?
6) ¿Intervienen encargados en el tratamiento de los datos personales?
7) ¿Qué transferencias se realizan o se podrían realizar de los datos personales y con qué finalidad?
8) ¿Se difunden los datos personales?
9) ¿Cuál es el plazo de conservación de los datos personales?

B. Las funciones y obligaciones de las personas que traten datos personales

El artículo 33, fracción II de la Ley General establece como una de las actividades a realizar para implementar y mantener medidas de seguridad para la protección de datos personales, la definición de las funciones y obligaciones del personal involucrado en el tratamiento de datos personales.

Se considera importante definir los roles y funciones de las personas que tratan datos personales al interior del GACM puesto que en ellas se centran los riesgos y posibles vulneraciones.

C. El análisis de riesgos

El artículo 33, fracciones IV de la Ley General establece como una de las actividades a realizar para implementar y mantener medidas de seguridad para la protección de datos personales, la elaboración de un análisis de riesgo.

El análisis de riesgos es el proceso que integra los principios y prácticas de salud y seguridad aceptadas en GACM para el tratamiento de datos personales. Se trata de un procedimiento documentado que consiste en identificar los peligros y evaluar los riesgos potenciales antes y durante el tratamiento de los datos personales, estableciendo los mecanismos para la valoración de probabilidad e impacto; es considerado uno de los pasos más importantes para la identificación de los posibles problemas que podrían surgir en la organización, también conocidos como riesgos.

D. El análisis de brecha

El artículo 33, fracción V de la Ley General establece como una de las actividades a realizar para implementar y mantener medidas de seguridad para la protección de datos personales, la realización de un análisis de brecha.

El análisis de brecha en materia de protección de datos personales es un método para evaluar las diferencias entre el desempeño real y el desempeño esperado en el tratamiento de los datos personales al interior del GACM. El término “brecha” se refiere al espacio entre “donde estamos ahora” (el estado actual) y donde “queremos estar” (el estado objetivo), estableciendo las principales acciones para alcanzar el estado objetivo.

E. El plan de trabajo

El artículo 33, fracción VI de la Ley General establece como una de las actividades a realizar 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, la elaboración de un plan de trabajo.

F. Monitoreo y revisión de las medidas de seguridad

El artículo 33, fracción VII de la Ley General establece como una de las actividades para implementar y mantener medidas de seguridad para la protección de datos personales, el monitoreo y revisión de manera periódica de las medidas de seguridad implementadas, así como las amenazas y vulneraciones a las que están sujetos los datos personales.

G. El programa general de capacitación

Con relación al programa de capacitación, la fracción VIII del artículo 33 de la Ley General señala que, para establecer y mantener las medidas de seguridad para la protección de los datos personales, el responsable deberá 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.

VI. Revisiones

Con objeto de monitorear y revisar la eficacia y eficiencia del sistema de gestión en que se basa este Programa vinculante al interior del sujeto obligado, en el Documento de Seguridad se establecen las acciones de monitoreo y revisión respectivas:

Las revisiones podrán ser:

- **Internas:** deberán realizarse por la Unidad de Transparencia en coordinación con la Subdirección de Sistemas y Procesos, y la Subdirección de Riesgos.
- **Externas:** a través de una contratación, convenio u otro mecanismo de colaboración con un tercero.

Las revisiones externas podrán realizarse a través del INAI, organismos internacionales expertos en la materia, entre otros.

Revisiones a realizar	
Obligaciones	El responsable deberá contar con un Plan de trabajo que incluya las acciones de monitoreo y revisión del programa, políticas y documento de seguridad en materia de protección de datos personales del GACM. Este Plan de trabajo es el que refiere el Documento de Seguridad en materia de protección de datos personales.
Actividades para su cumplimiento	**Actividad 1** Elaborar un Plan de trabajo que incluya las acciones de monitoreo y revisión de este programa, políticas y documento de seguridad el cual deberá ser sometido y aprobado por el Comité de Transparencia. En el Plan de trabajo se deberá incluir como mínimo lo siguiente: • Acción • Responsable • Fecha de ejecución El Plan de trabajo podrá contener revisiones integrales o parciales en función de las necesidades de la institución. Integrales: • Ante una reestructura general del GACM o cambio en la normatividad en materia. • Ante una vulneración al tratamiento de los datos personales que de manera horizontal involucre varios procesos al interior del GACM. • Cuando así lo considere la Unidad de Transparencia en coordinación con la Subdirección de Sistemas y Procesos, y Riesgos. Parciales: • Cuando de manera específica se observe la necesidad de revisar ya sea el programa, políticas o documento de seguridad, o un procedimiento. • Cuando así lo considere la Unidad de Transparencia en coordinación con la Subdirección de Sistemas y Procesos y Riesgos. La primera revisión se llevará a cabo de forma anual y las subsecuentes cada dos años.

Revisiones a realizar	
	Las actualizaciones al programa, políticas o documento de seguridad se derivarán de los resultados de las revisiones implementadas, y adicionalmente, se observará lo establecido en el artículo 36 de la LGPDPPSO, para el caso del Documento de Seguridad. **Actividad 2** • Ejecutar el Plan de trabajo aprobado por el Comité de Transparencia. **Actividad 3** • Presentación de resultados al Comité de Transparencia y plan de atención. • La Unidad de Transparencia en coordinación con la Subdirección de Sistemas y Procesos, y la Subdirección de Riesgos propondrá al Comité de Transparencia el tipo de medida y el plazo. • El Comité de Transparencia aprobará el plan de atención. **Actividad 4** • Implementación de medidas preventivas y/o correctivas resultantes. • La Unidad de Transparencia deberá documentar las medidas preventivas o correctivas realizadas para la mejora continua.
Unidad administrativa responsable del cumplimiento	La Unidad de Transparencia en coordinación con la Subdirección de Sistemas y Procesos, y la Subdirección de Riesgos.
Medios para acreditar el cumplimiento	**Actividad 1** • Plan de trabajo aprobado por el Comité de Transparencia. **Actividad 2** • Reportes de las revisiones.

Revisiones a realizar	
	Actividad 3 • Informe de resultados. **Actividad 4** • Evidencia documental de la implementación.
Artículos vinculados: 30 fracciones IV y V, 33 Fracción VII de la LGPDPPSO y 47, 62 y 63 de los Lineamientos generales.	

VII. Acciones para la mejora continua

GACM adoptará las medidas preventivas y correctivas resultado de las revisiones realizadas u obtenidas por otras fuentes de información.

Los puntos de mejora de la implementación del programa podrán ser de dos tipos:

1. Acciones preventivas: son aquéllas encaminadas a evitar cualquier *no conformidad* (no cumplimiento) con relación a lo establecido en este programa.

2. Acciones correctivas: son aquéllas encaminadas a eliminar las causas de la *no conformidad* con relación a lo previsto en este programa.

Transitorios

Una vez aprobado el Programa en materia de protección de datos personales de Grupo Aeroportuario de la Ciudad de México S.A. de C. V., por el Comité de Transparencia de la Entidad, la UT lo hará del conocimiento de los titulares de las áreas, así como de los enlaces de transparencia.

El presente documento deberá actualizarse cuando se configuren al menos uno de los siguientes supuestos: a) cuando la estructura orgánica del GACM sufra algún cambio; b) como resultado de un proceso de mejora y c) cuando la normativa aplicable lo requiera.

Excepcionalmente, cuando se presente algún suceso o acontecimiento de fuerza mayor o caso fortuito que modifique este programa, la UT enviará las comunicaciones correspondientes a los titulares de las áreas, notificando las disposiciones que emitan las autoridades competentes.

VI. Sanciones

Cuando el Comité de Transparencia tenga conocimiento del incumplimiento de alguna obligación prevista en este programa, deberá realizar a la unidad administrativa correspondiente un exhorto para que lleve a cabo las acciones que resulten pertinentes con objeto de modificar dicha situación y evitar incumplimientos futuros o situaciones de riesgo que los pudieran ocasionar.

De manera adicional, es importante que las personas servidoras públicas que están a cargo del tratamiento de datos personales tengan presente que de conformidad con el artículo 163 de la LGPDPPSO serán causas de sanción por incumplimiento de las obligaciones establecidas en dicha ley, las siguientes:

a) Actuar con negligencia, dolo o mala fe durante la sustanciación de las solicitudes para el ejercicio de los derechos ARCO;

b) Incumplir los plazos de atención previstos en la LGPDPPSO para responder las solicitudes para el ejercicio de los derechos ARCO o para hacer efectivo el derecho de que se trate;

c) Usar, sustraer, divulgar, ocultar, alterar, mutilar, destruir o inutilizar, total o parcialmente y de manera indebida datos personales, que se encuentren bajo su custodia o a los cuales tengan acceso o conocimiento con motivo de su empleo, cargo o comisión;

d) Dar tratamiento, de manera intencional, a los datos personales en contravención a los principios y deberes establecidos en la LGPDPPSO;

e) No contar con el aviso de privacidad, o bien, omitir en el mismo alguno de los elementos a que refiere el artículo 27 de la LGPDPPSO, según sea el caso, y demás disposiciones que resulten aplicables en la materia;

f) Clasificar como confidencial, con dolo o negligencia, datos personales sin que se cumplan las características señaladas en las leyes que resulten aplicables. La sanción sólo procederá cuando exista una resolución previa, que haya quedado firme, respecto del criterio de clasificación de los datos personales;

g) Incumplir el deber de confidencialidad establecido en el artículo 42 de la LGPDPPSO;

h) No establecer las medidas de seguridad en los términos que establecen los artículos 31, 32 y 33 de la LGPDPPSO;

i) Presentar vulneraciones a los datos personales por la falta de implementación de medidas de seguridad según los artículos 31, 32 y 33 de la LGPDPPSO;

j) Llevar a cabo la transferencia de datos personales, en contravención a lo previsto en la LGPDPPSO;

k) Obstruir los actos de verificación de la autoridad;

l) Crear bases de datos personales en contravención a lo dispuesto por el artículo 5 de la LGPDPPSO;

m) No acatar las resoluciones emitidas por el Instituto; y

n) Omitir la entrega del informe anual y demás informes a que se refiere el artículo 44, fracción VII de la LGTAIP, o bien, entregar el mismo de manera extemporánea.

Las causas de responsabilidad previstas en las fracciones I, II, IV, VI, X, XII, y XIV, así como la reincidencia en las conductas previstas en el resto de las fracciones, serán consideradas como graves.

Asimismo, de conformidad con el artículo 105 de los Lineamientos Generales, cuando alguna unidad administrativa se niegue a colaborar con la Unidad de Transparencia en la atención de las solicitudes para el ejercicio de los derechos ARCO, 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, contraloría o instancia equivalente y, en su caso, dé inicio el procedimiento de responsabilidad administrativo respectivo.

Cabe destacar que las sanciones de carácter económico no podrán ser cubiertas con recursos públicos.

Las responsabilidades que resulten de los procedimientos administrativos correspondientes son independientes de las del orden civil, penal o de cualquier otro tipo que se puedan derivar de los mismos hechos.

La Unidad de Transparencia tomará las medidas necesarias para que las personas servidoras públicas del sujeto obligado conozcan esta información.

Glosario

Para los efectos de este Documento, además de las definiciones previstas en el artículo 3 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, se entenderá por:

1. **Análisis de brecha**: Herramienta de análisis para comparar el estado y desempeño de las medidas de seguridad existentes de los sistemas de datos personales respecto de las faltantes, a partir de puntos de referencia seleccionados en una situación o momento dado.

2. **Análisis de riesgo**: Estudio de las posibles amenazas, vulnerabilidades y eventos no deseados que puedan producir afectaciones a los derechos patrimoniales o morales del titular de los datos personales.

3. **Aviso de privacidad**: Documento de forma física, electrónica o en cualquier formato, que es generado por el responsable y puesto a disposición de los titulares de los datos personales, a partir del momento en el cual se recaben sus datos personales, con el objeto de informarle los propósitos del tratamiento de los mismos.

4. **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.

5. **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.

6. **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.

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

8. **Encargado**: Persona física o jurídica, pública o privada, ajena a la organización de GACM, que sola o conjuntamente con otras trate datos personales a nombre y por cuenta del GACM.

9. **Evaluación de impacto en la protección de datos personales**: Evaluación mediante la cual los sujetos obligados que pretendan poner en operación o modificar políticas públicas, programas, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento intensivo o relevante de datos personales, valoran los impactos reales respecto de determinado tratamiento de datos personales, a efecto de identificar y mitigar posibles riesgos relacionados con los principios, deberes y derechos de los titulares, así como los deberes de los responsables y encargados, previstos en la normativa aplicable.

10. **Inventario de datos personales**: Catálogo de sistemas de datos con independencia de su forma de almacenamiento.

11. **Medidas de seguridad administrativas**: Políticas y procedimientos para la gestión, soporte y revisión de la seguridad de la información a nivel organizacional, la identificación, clasificación y borrado seguro de la información, así como la sensibilización y capacitación del personal, en materia de protección de datos personales.

12. **Medidas de seguridad físicas**: Conjunto de acciones y mecanismos para proteger el entorno físico de los datos personales y de los recursos involucrados en su tratamiento.

13. **Medidas de seguridad técnicas**: Conjunto de acciones y mecanismos que se valen de la tecnología relacionada con hardware y software para proteger el entorno digital de los datos personales y los recursos involucrados en su tratamiento.

14. **Remisión**: Toda comunicación de datos personales realizada exclusivamente entre el responsable y encargado, dentro o fuera del territorio mexicano.

15. **Revisión**: implica la verificación periódica de las medidas de seguridad implementadas, así como las amenazas y vulneraciones identificadas por GACM; esto incluye los documentos que conforman el Sistema de Gestión de la institución. Lo anterior, con el objetivo de fortalecer, a través de un ciclo de mejora continua, la protección de los datos personales que resguarda esta entidad.

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

17. **Servidor público vinculado**: El o los servidores públicos designados por los titulares de las áreas, encargados del tratamiento de datos personales.

18. **Sistema de datos**: Archivo físico o electrónico que contenga datos personales que se hayan recabado para el ejercicio de las funciones de las áreas.

19. **Sistema de gestión**: Conjunto de elementos y actividades interrelacionadas para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el tratamiento y seguridad de los datos personales, el cual se integra por el programa de Protección de datos personales, las Políticas de protección de datos personales y el Documento de seguridad en materia de protección de datos personales de GACM.

20. **Sistema Informático**: Conjunto de componentes de software interrelacionados, cuyo fin es el tratamiento de datos personales, mediante procedimientos automatizados.

21. **Sujeto obligado**: Cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos, del ámbito federal.

22. **Titular**: Persona física a quien corresponden los datos personales.

23. **Transferencias:** Toda comunicación de datos personales dentro o fuera del territorio mexicano, realizada a persona distinta del titular, del responsable o del encargado.

24. **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.

25. **Unidad administrativa**: Área a la que se le confiere atribuciones específicas en el reglamento interno, estatuto orgánico o instrumento normativo equivalente que sea superior a un manual de organización.

Actualizaciones del Programa

Fecha de aprobación	11 de noviembre de 2020
Fecha 1ª actualización	22 de junio de 2022