**GUÍA INTERNA DE PROTECCIÓN DE DATOS PERSONALES**

**Agencia Espacial Mexicana**

1. **INTRODUCCIÓN**

La Agencia Espacial Mexicana (AEM) es un organismo público descentalizado, sectorizado y coordinado por la Secretaría de Infraestructura, Comunicaciones y Transportes (SICT), de conformidad a lo establecido en el artículo 1 de la Ley que crea la Agencia Espacial Mexicana**[[1]](#footnote-1)**, en términos de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (en lo sucesivo Ley General) y los Lineamientos Generales de Protección de Datos Personales para el Sector Público (en lo sucesivo Lineamientos Generales), es un sujeto obligado en materia de protección de datos personales, responsable**[[2]](#footnote-2)** del tratamiento que de a estos, en el ejercicio de las atribuciones que tiene conferidas, para lo cual debera cumplir las obligaciones de la Ley General y Lineamientos antes referidos y demas normativa aplicable. Por lo tanto, es responsable de proteger los datos personales que trate, garantizando los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad, así como del cumplimiento de las disposiciones derivadas de la Ley General antes invocada.

Al respecto, el presente documento constituye una polftica interna de la Agencia Espacial Mexicana, en observancia al principio de responsabilidad, derivado del que en su caracter de responsable deberá adoptar políticas e implementar mecanismos para asegurar y acreditar el cumplimiento de los principios, deberes y demas obligaciones establecidas en las disposiciones en materia de protección de datos personales.

Dichos mecanismos tendran como objetivo el establecimiento de los elementos y actividades de dirección, operación y control de todos los procesos que, en el ejercicio de sus funciones y atribuciones, impliquen un tratamiento de datos personales a efecto de proteger estos de manera sistematica y continua. Los que deberan ser aprobados, coordinados y supervisados por el Comite de Transparencia de la AEM**[[3]](#footnote-3)**.

En este sentido, la instrumentación de la presente Guía se facilitará a las personas Titulares de las Unidades Administrativas de la AEM la realización de tratamientos de datos personales en total apego a los principios, deberes y obligaciones establecidas en la Ley General y demas disposiciones aplicables, lo que permitira garantizar una adecuada y correcta protección de los datos personales y el ejercicio de los derechos ARCO (Acceso, Rectificación, Cancelación y Oposición) y la Portabilidad al tratamiento de datos personales por parte de sus titulares.

De conformidad a lo establecido en el numeral 3.6, inciso (e) del Manual de Organización de la Agencia Espacial Mexicana, la Dirección de Administración es la persona encargada de fungir como Titular de la Unidad de Transparencia. Asimismo, de conformidad a lo establecido en el numeral 3.6.6, inciso (f), la Gerencia de Transparencia y Acceso a la Información Pública funge como Oficial de Protección de Datos Personales, será responsable de auxialiar y orientar al titular que lo requiera con relación al ejercicio del derecho a la protección de datos personales, así como asesorar a las áreas del sujeto oligado en materia de protección de datos personales así como hacer las gestiones necesarias para el manejo, mantenimiento, seguridad y protección de los sistemas de datos personales en posesión del responsable.

Asimismo, en los artículos 30, fracciones I, II, IV y VII de la Ley General y 47 de los Lineamientos Generales, se establece que, entre las acciones que deberán realizar los responsables del tratamiento de datos personales para cumplir con el principio de responsabilidad y programas de protección de datos personales, obligatorios y exigibles al interior de la organización del responsable, en este caso la AEM, así como destinar los recursos necesarios para la implementación de dichos programas y políticas.

Asimismo, el artículo 33 de la Ley General, establece en la fracción I, la obligación de los responsables de contar con políticas internas para el tratamiento y protección de los datos personales.

Lo señalado en el párrafo anterior, se establece con fundamento en el artículo 34 de la Ley General que a la letra dispone lo siguiente:

*“Artículo 34. Las acciones relacionadas con las medidas de seguridad para el tratamiento de los datos personales deberán estar documentadas y contenidas en un sistema de gestión.*

*Se entenderá por sistema de gestión al conjunto de elementos y actividades interrelacionadas para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el tratamiento y seguridad de los datos personales, de conformidad con lo previsto en la presente Ley y las demás disposiciones que le resulten aplicables en la materia.”*

Para concluir, se precisa que la presente Guía lnterna de Protecciónn de Datos Personales de la Agencia Espacial Mexicana fue aprobada por el Comite de Transparencia, autoridad máxima en materia de protección de datos personales de conformidad a los artículos 83 y 84, fracción I, y 87 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados; 43 de la Ley General de Transparencia y Acceso a la lnformación Pública; 64 de la Ley Federal de Transparencia y Acceso a la lnformación Pública y 47 de los Lineamientos Generales de Protección de Datos Personales para el Sector Publico.

1. **FINALIDAD**

El objetivo del presente documento, es establecer una Guía Interna de Protección de Datos Personales que operan al interior de la AEM, esta guía establece las reglas y principios relacionados con el tratamiento de datos personales en la AEM. El propósito es que el Organismo, use los datos de forma coherente y conforme los principios de la Ley General, los Lineamientos Generales y demás normativa aplicable, contar con mejores prácticas, elementos y actividades de dirección, operación y control de todos los procesos en los que las Unidades Administrativas de la AEM, en el ejercicio de sus facultades, competencias y funciones, lleven a cabo el tratamiento de datos personales, o en su caso, cuando los datos personales sean tratados por parte de un encargado a solicitud de la Unidad Administrativa responsable, así como al momenta de realizar transferencias, nacionales o internacionales, de datos personales o remisiones.

Los tratamientos de datos personales que realicen las unidades administrativas deberán cumplir con los principios, deberes y obligaciones que prevé la normativa.

1. **MARCO NORMATIVO**

* Constitución Política de los Estados Unidos Mexicanos, artículos 6 apartado A y 16 párrafo segundo.
* Ley Órganica de la Administración Pública Federal
* Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados
* Ley General de Transparencia y Acceso a la Información Pública
* Ley Federal de Transparencia y Acceso a la Información Pública
* Lineamientos Generales de Protección de Datos Personales para el Sector Público
* Lineamientos que establecen los parámetros, modalidades y procedimientos para la portabilidad de datos personales
* Ley que crea la Agencia Espacial Mexicana
* Manual de Organización de la Agencia Espacial Mexicana
* Estatuto Orgánico de la Agencia Espacial Mexicana

1. **ÁMBITO DE APLICACIÓN**

Esta guía es aplicable a todos los tratamientos de datos personales que el Organismo, en el ejercicio de sus atribuciones realice.

El cumplimiento de esta Guía de Protección de Datos Personales es obligatorio para todo el personal de la AEM, sea que el tratamiento se lleve a cabo en la oficina central o en cualquiera de los Centros Regionales de Desarrollo Espacial de la AEM.

1. **VIGENCIA**

Esta Guía, tendrá una vigencia hasta en tanto no se reformen la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y Lineamientos Generales de Protección de Datos Personales para el Sector Público o en su caso; se emitan nuevas disposiciones que obliguen al Organismo a realizar tratamientos de datos personales en forma distinta.

1. **EJERCICIO DE LOS DERECHOS ARCO**

Se refieren al acceso, rectificación, cancelación u oposición de los datos personales que, en su caso, obran en posesión de la persona servidora pública responsable adscrita a la Agencia Espacial Mexicana (AEM).

Tales derechos, son independientes entre sí, por lo que sus titulares pueden ejercer cualquiera de ellos en un mismo momento. Es importante destacar que la protección de datos personales es un derecho personal, por lo que su ejercicio solo corresponde a la persona titular o, en su caso, a quien acredite su representación.

Dependiendo del derecho que desee ejercer, deberá incluir la siguiente información en la solicitud:

**ACCESO[[4]](#footnote-4)**: La modalidad en la que prefiere que se reproduzcan los datos personales a los que se pretende acceder (consulta directa, copia simple, copia certificada, documento electrónico, disco compacto DVD - CD).

**RECTIFICACIÓN[[5]](#footnote-5)**: Descripción de la modificación que solicita que se realice a los datos personales, y en su caso, aportar los documentos que sustenten la solicitud.

**CANCELACIÓN[[6]](#footnote-6)**: Las causas que motivan la petición de que se eliminen los datos de lo archivos, registros o bases de datos del responsable del tratamiento.

**OPOSICIÓN[[7]](#footnote-7)**: las causas o la situación que lo llevan a solicitar que finalice el tratamiento de sus datos personales, así como el daño o perjuicio que le causaría que dicho tratamiento continúe; o bien, deberá indicar las finalidades específicas respecto de las cuales desea ejercer este derecho.

1. **AVISO DE PRIVACIDAD**

El responsable deberá informar a los titulares, a través del aviso de privacidad, la existencia y las caracteristicas principales del tratamiento al que serán sometidos sus datos personales.

Por regla general, todo responsable está obligado a cumplir con el principio de información y poner a disposición del titular el aviso de privacidad de conformidad con lo dispuesto en los artículos 3, fracción 11, 26, 27 y 28 de la Ley General y los presentes Lineamientos generales, con independencia de que no se requiera el consentimiento del titular para el tratamiento de sus datos personales.

Los avisos de privacidad de la AEM se podran consultar en el siguiente hipervínculo, <https://aem.gob.mx/transparencia-aem/proteccion-de-datos-personales/>

1. **PRINCIPIOS DE PROTECCIÓN DE DATOS PERSONALES**

La AEM, se sujeta al tratamiento de los datos personales conforme a las atribuciones o facultades que la normatividad le confiere en su carácter de sujeto obligado; así como, en estricto apego y cumplimiento a lo dispuesto por la Ley General, los Lineamientos Generales, y, en su caso, el derecho internacional, respetando los derechos y libertades de los titulares.

Con la conformación de esta guía se busca el cumplimiento en la Entidad de todos los principios que establece el artículo 16 de la Ley General, el cual a la letra ordena lo siguiente:

*“Artículo 16. El responsable deberá observar los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad en el tratamiento de datos personales.”*

Cada Unidad Administrativa designará un servidor público vinculado al tratamiento de datos personales, quién será el encargado de apoyar al Titular de la Unidad Administrativa de su adscripción para realizar lo establecido en las presente Guía y tendrá las siguientes funciones:

1. Adoptar las medidas de seguridad físicas, administrativas o técnicas, para la protección de los sistemas de tratamiento de datos personales bajo su responsabilidad, sea en soporte físico o electrónico, de forma que se evite su alteración, pérdida o acceso no autorizado;
2. Llevar una relación actualizada de las personas que tengan acceso al o los sistemas de datos personales que se encuentran en soporte físico o electrónico;
3. Coadyuvar en la aplicación y vigilancia del cumplimiento de las medidas de seguridad para la conservación y resguardo de los datos personales en el Organismo.
4. Recibir la capacitación especializada en materia de protección de datos personales
5. Coadyuvar con el Comité de Transparencia, la Persona Oficial de Protección de Datos Personales o en los requerimientos que realice el INAI con motivo de un revisión o verificación del cumplimiento de la Ley General.

En todo tratamiento de datos personales el responsable deberá observar los iguientes principios rectores de la protección de datos personales:

1. Licitud;
2. Finalidad;
3. Lealtad;
4. Consentimiento;
5. Calidad;
6. Proporcionalidad;
7. Información; y
8. Responsabilidad
9. **Licitud[[8]](#footnote-8)**

Es obligación de la AEM, tratar y recabar datos personales de manera lícita, conforme a las disposiciones establecidas por la Ley General y Lineamientos Generales.

Los datos personales tienen que ser tratados por el responsable de manera lícita, lo que supone que el responsable debe sujetarse a las facultades o atribuciones que la normatividad aplicable le otorga.

El tratamiento de datos personales es una actividad que depende de las atribuciones o facultades que previamente le otorga la ley a los Sujetos Obligados, en consecuencia, no deben tratarse datos personales si no se tienen facultades previamente otorgadas.

La Entidad a través de sus Unidades Administrativas tiene las siguientes obligaciones en torno al principio de licitud:

1. Tratar siempre los datos personales de conformidad con las atribuciones o facultades conferidas por la normatividad, actuando con apego a la legislación mexicana, por lo que el responsable sólo podrá hacer con los datos personales aquello que esté legalmente permitido, como cualquier acto de autoridad.
2. El tratamiento se debe realizar tomando en consideración los derechos de los titulares.
3. **FINALIDAD[[9]](#footnote-9)**

Se entiende por finalidad del tratamiento, el propósito, motivo o razón por el cual se tratan los datos personales. El Organismo debe limitarse al tratamiento de los datos personales únicamente para el cumplimiento de las finalidades previstas en el aviso de privacidad.

Los datos personales obtenidos por la AEM, serán utilizados para uno o más propósitos específicos y lícitos.

Los datos personales sólo pueden ser tratados para cumplir con la finalidad o finalidades que hayan sido informadas al titular en el aviso de privacidad y, en su caso, consentidas por éste.

Las finalidades deben ser concretas, explícitas, lícitas y legítimas:

* **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 confusión en el titular.
* **Explícitas:** Tienen lugar 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 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.

Derivado del cumplimiento al principio de finalidad, la Entidad tiene las siguientes obligaciones:

1. Tratar los datos personales únicamente para la finalidad o finalidades que hayan sido informadas al titular en el aviso de privacidad y, en su caso, consentidas por éste.
2. Informar en el aviso de privacidad todas las finalidades para las cuales se tratarán los datos personales, y redactarlas de forma tal que sean específicas.
3. Identificar y distinguir en el aviso de privacidad entre las finalidades primarias que dan origen al tratamiento, de aquellas que son secundarias a las que lo originaron, pero se consideran compatibles y/o análogas.
4. Ofrecer al titular de los datos personales un mecanismo para que pueda manifestar su negativa al tratamiento de sus datos personales, para todas o algunas de las finalidades secundarias;
5. Cuando el aviso de privacidad se dé a conocer a través de un medio indirecto, como el correo postal, informar al titular que tiene cinco días hábiles para manifestar su negativa para el tratamiento de su información;
6. No tratar los datos personales para finalidades distintas que no resulten compatibles o análogas con aquéllas para las que se hubiese recabado de origen los datos personales y que hayan sido previstas en el aviso de privacidad, al menos que lo permita una ley o reglamento, o se obtenga el consentimiento del titular de los datos.
7. **LEALTAD[[10]](#footnote-10)**

La AEM, no obtendrá datos personales a través de medios fraudulentos y respetará la expectativa razonable de privacidad del titular.

De acuerdo con este principio la obtención de los datos personales no podrá hacerse a través de medios engañosos, ni fraudulentos, lo que implica que:

* No se recaben datos personales con dolo, mala fe o negligencia;
* No tratar los datos de tal manera que genere discriminación o un trato injusto contra los titulares.
* No se vulnere la confianza del titular con relación a que sus datos personales serán tratados conforme a lo acordado; y
* Se informen todas las finalidades del tratamiento en el aviso de privacidad.

La AEM tiene las siguientes obligaciones en torno al principio de lealtad:

1. No hacer uso de medios engañosos o fraudulentos para la obtención de los datos personales.
2. Respetar en todo momento la expectativa razonable de privacidad del titular.
3. **Consentimiento[[11]](#footnote-11)**

Es obligación de la AEM, sujetar el tratamiento de datos personales al consentimiento del titular, salvo las excepciones previstas por la Ley General.

El responsable deberá contar con el consentimiento del titular para el tratamiento de sus datos personales. La solicitud del consentimiento deberá ser conforme a las finalidades concretas que se informen en el aviso de privacidad, es decir, el consentimiento se deberá solicitar solo para las finalidades específicas.

El consentimiento debe ser informado, por lo que previo a su obtención, es necesario que el titular conozca el aviso de privacidad.

Se llevarán a cabo las siguientes actividades para respetar el consentimiento de la persona titular:

1. La AEM obtendrá el consentimiento de la persona titular para el tratamiento de los datos personales, cuando no se actualice alguno de los supuestos de excepción del artículo 22 de la Ley General;
2. Solicitará el consentimiento conforme a las finalidades específicas e informadas en el aviso de privacidad;
3. Determinará el tipo de consentimiento que se requiere: tácito o expreso y por escrito;
4. Solicitará el consentimiento expreso y por escrito para los datos personales sensibles, cuando sea procedente;
5. Por regla general se solicitará el consentimiento previo a la obtención de los datos personales.
6. Implementará medios sencillos y gratuitos para la obtención del consentimiento, de acuerdo con el tipo de consentimiento que se requiera (tácito o expreso);
7. Llevará un control para identificar a los titulares que negaron su consentimiento, así como las finalidades concretas para las cuales no se podrán tratar los datos personales;
8. Esperar el plazo de cinco días hábiles que señala el artículo 15 de los Lineamientos Generales, para utilizar los datos personales, cuando éstos se hayan obtenido de manera indirecta, el aviso de privacidad se haya dado a conocer por un medio que no permita el contacto directo o personal con el titular y se requiera el consentimiento tácito;
9. Documentará la actuación de la AEM para acreditar que se cumplió con el principio de consentimiento, y
10. Solicitará de nuevo el consentimiento cuando se realicen cambios a las finalidades.
11. **CALIDAD[[12]](#footnote-12)**

Cada Unidad Administrativa es responsable del tratamiento de datos personales, por lo que 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.

El principio de calidad implica los siguientes elementos:

1. Procurar que los datos personales tratados sean exactos, correctos, completos y actualizados.

* **Exactos:** Se considera que los datos personales son exactos cuando reflejan la realidad de la situación de su titular, es decir, son verdaderos o fieles. También cuando no presentan errores que pudieran afectar su veracidad.
* **Completos:** Los datos personales están completos cuando no falta ninguno de los que se requieran para las finalidades para las cuales se obtuvieron y son tratados, de forma tal que no se cause un daño o perjuicio al titular.
* **Actualizados:** Los datos personales están actualizados cuando están al día y corresponden a la situación real del titular. De forma análoga, los Lineamientos Generales para la administración pública precisan que este elemento se cumple cuando los datos responden fielmente a la situación actual del titular.
* **Correctos:** Son correctos cuando cumplen con todas las características anteriores. Asimismo, son correctos cuando no presentan errores que pudieran afectar su veracidad.

1. Suprimir los datos personales cuando hayan dejado de ser necesarios para el cumplimiento de las finalidades para las cuales se obtuvieron.

Los plazos de conservación se determinan con base en la legislación en materia de archivos. La AEM, a través de las Unidades Administrativas, debe considerar las disposiciones específicas para la conservación y supresión de la información.

Por lo tanto, debe existir un procedimiento para la supresión de los datos personales y se deben atender a los medios de almacenamiento, ya sean físicos o electrónicos.

1. Utilizar los datos personales únicamente el tiempo necesario y para el cumplimiento de las finalidades establecidas. Al término de las finalidades, los datos personales deben cancelarse previo periodo de bloqueo.

El Organismo tiene las siguientes obligaciones en torno al principio de calidad:

* Adoptar las medidas que considere convenientes para procurar que los datos personales cumplan con las características de ser exactos, completos, actualizados y correctos, a fin de que no se altere la veracidad de la información.
* Conservar los datos personales exclusivamente por el tiempo que sea necesario para llevar a cabo las finalidades que justificaron el tratamiento y para cumplir con aspectos legales, administrativos, contables, fiscales, jurídicos e históricos y el periodo de bloqueo;
* Bloquear los datos personales antes de suprimirlos, y durante el periodo de bloqueo sólo tratarlos para su almacenamiento y acceso, en caso de que se requiera determinar posibles responsabilidades en relación con su tratamiento;
* Suprimir los datos personales, previo bloqueo, cuando haya concluido el plazo de conservación, de conformidad con lo establecido por la Ley General de Archivos;
* Establecer y documentar procedimientos para la conservación, bloqueo y supresión de los datos personales.
* Demostrar que los datos personales se conservan, bloquean y suprimen cumpliendo los plazos previstos para ello, o bien, en atención a una solicitud de ejercicio del derecho de cancelación.

1. **PROPORCIONALIDAD[[13]](#footnote-13)**

Las personas Titulares de las Unidades Administrativas de la AEM recabaran aquellos datos personales que resulten 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 por la normatividad que le resulte aplicable, verificar si los datos personales que se requieran por la persona Titular de la Unidad Administrativa para su tratamiento, no son tratados por otra persona Titular de Unidad Administrativa diversa.

1. **INFORMACIÓN[[14]](#footnote-14)**

La AEM debe Informar a las personas titulares de los datos, la información que se recaba de ellos y con qué fines, a través del aviso de privacidad.

Por medio del principio de información la AEM se encuentra obligada a informar a las personas titulares, las características principales del tratamiento al que será sometida su información personal, para que puedan tomar decisiones informadas y ejercer su derecho a la protección de sus datos, esto se materializa a través del aviso de privacidad.

En torno a este principio, la AEM deberá cumplir de manera puntual con lo siguiente:

1. Poner a disposición de las personas titulares el aviso de privacidad, aunque no se requiera el consentimiento de los titulares para el tratamiento de los datos personales;
2. Poner a disposición del titular el aviso de privacidad en forma previa a la obtención de los datos personales, cuando éstos se obtengan de manera personal y directa del titular;
3. Poner a disposición del titular el aviso de privacidad al primer contacto que se tenga con éste, cuando los datos personales se hayan obtenido de una transferencia consentida, de una que no requiera el consentimiento, o bien de una fuente de acceso público;
4. Poner a disposición del titular el aviso de privacidad previo a iniciar el uso de los datos personales para las nuevas finalidades, cuando el responsable requiera tratar los datos personales para finalidades distintas y no compatibles con aquéllas para las cuales los recabó inicialmente;
5. Redactar el aviso de privacidad de manera que sea claro, comprensible, con una estructura y diseño que facilite su entendimiento, para su elaboración tomará en cuenta el perfil de los titulares y atender lo siguiente: no usar frases inexactas, ambiguas o vagas; incluir textos o formatos que induzcan al titular a elegir una opción en específico; no premarcar casillas en las que se solicite el consentimiento del titular, y no remitir a textos o documentos que no estén disponibles;
6. Ubicar el aviso de privacidad en un lugar visible y que facilite su consulta, con independencia del medio de difusión o reproducción que se utilice;
7. Comunicar el aviso de privacidad a encargados y terceros a los que remita o transfiera datos personales;
8. Demostrar el cumplimiento del principio de información, en caso de que así se requiera;
9. No establecer cobros para la consulta del aviso de privacidad, y
10. Poner a disposición de los titulares un nuevo aviso de privacidad en los siguientes casos:

a) cambie la identidad del responsable;

b) se requiera recabar nuevos datos personales sensibles, patrimoniales o financieros y se requiera el consentimiento del titular;

c) se requiera tratar los datos personales para nuevas finalidades que requieran el consentimiento del titular, y

d) se requiera realizar nuevas transferencias que requieran el consentimiento del titular.

1. **RESPONSABILIDAD[[15]](#footnote-15)**

Las personas Titulares de las Unidades Administrativas de la AEM deberan adoptar políticas e implementar mecanismos para asegurar y acreditar el cumplimiento de los principios, deberes y demas obligaciones establecidas en la Ley General, los Lineamientos Generales; así como establecer aquellos mecanismos necesarios para evidenciar dicho cumplimiento ante las personas titulares y al Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI).

Las personas Titulares de las Unidades Administrativas de la AEM que traten datos personales y el personal involucrado en el tratamiento de datos personales, deberan participar en los programas de capacitaci6n y actualización sobre las obligaciones y demás deberes en materia de protección de datos personales.

1. **DEBERES DE PROTECCIÓN DE DATOS PERSONALES**

La AEM 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.

Las personas Titulares de las Unidades Administrativas de la AEM deberán cumplirán con los siguientes deberes:

1. Deber de confidencialidad
2. Deber de seguridad
3. **DEBER DE CONFIDENCIALIDAD[[16]](#footnote-16)**

Se entiende que se deben 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 secrecia la información, así como evitar que la información sea revelada a persona no aurotizadas y prevenir la divulgación no autorizada de la misma.

Las personas servidoras públicas tiene la obligación de guardar la debida confidencialidad respecto de los datos personales que son tratados en las Unidades Administrativas, para evitar causar un daño a la persona titular. De no ser así, un tercero no autotizado podría tener acceso a determinada información y hacer mas uso de esta.

1. **DEBER DE SEGURIDAD[[17]](#footnote-17)**

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 lleve a cabo, deberán 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, perdida, alteración, acceso o tratamiento no autorizado, así para garantizar la confidencialidad de los datos personales.

Los datos personales, entendidos como cualquier información concerniente a una persona física identificada o identificable, en terminos de la norma aplicable que, de manera enunciativa mas no limitativa se pueden identificar de acuerdo a las siguientes categorías:

**Datos identificativos:** EI nombre, alias, pseudonimo, domicilio, código postal, teléfono particular, sexo, estado civil, teléfono celular, firma, Clave de Registro Federal de Contribuyentes ( Clave Unica de Registro de Población ( Clave de Elector, Matrícula del Servicio Militar Nacional, número de pshcp

porte, lugar y fecha de nacimiento, nacionalidad, edad, fotografía, localidad y sección electoral, y analogos.

**Datos de origen:** Origen, etnia, raza, color de piel, color de ojos, color y tipo de cabello, estatura, complexión, y analogos.

**Datos ideológicos:** Ideologías, creencias, opinión política, afiliación política, opinión pública, afiliación sindical, religión, conviccion filosófica y analogos

**Datos sobre la salud:** EI expediente clínico de cualquier atención médica, historial médico, referencias o descripción de sintomatologias, detección de enfermedades, incapacidades médicas, discapacidades, intervenciones quirurgicas, 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 analogos.

**Datos Laborales:** Número 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.

**Datos patrimoniales:** Bienes muebles e inmuebles de su propiedad, información fiscal, personas físicas y morales privadas, inversiones, seguros, fianzas, servicios contratados, referencias personales, beneficiarios, dependientes económicos, decisiones patrimoniales y análogos.

**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 de cualquier otra rama del Derecho, y analogos.

**Datos académicos:** Trayectoria educativa, avances de créditos, tipos de examenes, promedio, calificaciones, títulos, cedula profesional, certificados, reconocimientos y analogos.

**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.

**Datos electrónicos:** Firma electrónica, dirección e correo electrónico, código QR.

**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 análogo.

Cuando los datos personales hayan dejado de ser necesarios para el cumplimiento de las finalodades previstas en el aviso de privacidad y que motivaron su tratamiento conforme a disposiciones que resulte aplicables, estos deberán ser suprimidos, previo bloqueo en su caso. Una vez que concluya el periodo de conservación, estos no deberán exceder aquellos que sean necesarios para el cumplimiento de las finalidades que justifiquen su tratamiento, y deberán atender a las disposiciones aplicables en la materia de que se tarte y considerar los aspectos administrativos, contables, fiscales. Jurídicos e históricos de los datos personales.

1. **DOCUMENTO DE SEGURIDAD Y EL SISTEMA DE GESTIÓN DE DATOS PERSONALES**

* **Documento de seguridad[[18]](#footnote-18)**

La AEM debera contar con un Documento de Seguridad el cual constituye el instrumento que describe y da cuenta de manera general sobre las medidas de seguridad tecnicas, físicas y administrativas adoptadas por las personas Titulares de las Unidades Administrativas para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que posee, dicho documento debera ser aprobado por el Comite de Transparencia.

El documento de seguridad deberá contener:

1. Inventario de datos personales y sistemas de tratamiento
2. Funciones y obligaciones de quienes traten datos personales
3. Analisis de riesgo
4. Analisis de brecha
5. Plan de Trabajo
6. Mecanismos de monitoreo y revisión de las medidad de seguridad
7. Programa general de capacitación

Las personas Titulares de las Unidades Administrativas, a traves de sus enlaces en materia de datos personales, deberan hacer del conocimiento de la Unidad de Transparencia y a la persona Oficial de Protección de Datos Personales, las modificaciones en el tratamiento de datos personales que realice, que propicie actualizaciones al Documento de Seguridad; por lo que, en todo momenta deberan observar los principios, deberes y obligaciones a los que se refieren la Ley General, los Lineamientos Generales, la presente guía y demas normativa aplicable.

El artículo 36 de la Ley General establece que la persona responsable deberá actualizar el documento de seguridad cuando ocurran los siguientes eventos:

1. Se produzcan modificaciones sustanciales al tratamiento de datos personales que deriven en

un cambio en el nivel de riesgo;

1. Como resultado de un proceso de mejora continua, derivado del monitoreo y revisión del sistema de gestión;
2. Como resultado de un proceso de mejora para mitigar el impacto de una vulneración a la seguridad ocurrida, y
3. Implementación de acciones correctivas y preventivas ante una vulneración de seguridad.

La actualización de los supuestos antes citados, el documento de seguridad podrá actualizarse cada que sea necesatio.

* **Sistema de gestión[[19]](#footnote-19)**

El artículo 65 de los Linemainetos, el responsable deberá implementar un sistema de gestión de seguridad de los datos personales a que se refiere el artículo 34 de la Ley General, el cual permita planificar, establecer, implementar, operar, monitorear, mantener, revisar y mejorar las medidas de seguridad de carácter administrativo, físico y técnico aplicadas a los datos personales; tomando en consideración los estándares nacionales e internacionales en materia de protección de datos personales y seguridad.

* **Auditorías**

El artículo 63 último párrafo de los Lineamientos Generales. 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.

Esta auditoría puede incidir en la actualización de las medidas de seguridad pero también en las fases del propio SGSDP.

* **Otros mecanismos de monitoreo y revisión**

Reuniones con el Trasparencia a efectos de informar y debatir reportes de vulneraciones: establecer reuniones cada 6 meses o anualmente a efectos de evaluar las acciones preventivas y correctivas implementadas y las medidas de seguridad.

El documento de seguridad y el Sistema de Gestión de Datos Personales será implementado de la siguiente forma:

* **Vulneraciones a la seguridad de los datos personales**

Además de las que señalen las leyes respectivas y la normatividad aplicable, se considerarán como vulneraciones de seguridad, en cualquier fase del tratamiento de datos, al menos, las siguientes:

1. La pérdida o destrucción no autorizada;
2. El robo, extravío o copia no autorizada;
3. El uso, acceso o tratamiento no autorizado, o
4. El daño, la alteración o modificación no autorizada.

En caso de que ocurra una vulneración a la seguridad, las personas Titulares de las Unidades Administrativas deberan analizar las causas por las cuales se presentó e implementar en su plan de trabajo las acciones preventivas y correctivas para adecuar las medidas de seguridad y el tratamiento de los datos personales si fuese el caso a efecto de evitar que la vulneración se repita.

* **Plazo para notificar las vulneraciones de seguridad[[20]](#footnote-20)**

De conformidad con lo dispuesto en el articulo 40 de la Ley General, el responsable deberá notificar al titular y al Instituto las vulneraciones de seguridad que de forma significativa afecten los derechos patrimoniales o morales del titular dentro en un plazo máximo de setenta y dos horas, a partir de que confirme la ocurrencia de éstas y el responsable haya empezado a tomar las acciones encaminadas a detonar un proceso de mitigación de la afectación.

El plazo a que se refiere el párrafo anterior, comenzará a correr el mismo día natural en que el responsable confirme la vulneración de seguridad.

* **Notificación de las vulneracines de seguridad al INAI[[21]](#footnote-21)**

En la notificación a que se refiere el articulo anterior, el responsable deberá informar mediante escrito presentado en el domicilio del Instituto, o bien, a través de cualquier otro medio que se habilite para tal efecto, al menos, lo siguiente:

1. La hora y fecha de la identificación de la vulneración;
2. La hora y fecha del inicio de la investigación sobre la vulneración;
3. La naturaleza del incidente o vulneración ocurrida;
4. La descripción detallada de las circunstancias en torno a la vulneración ocurrida;
5. Las categorías y número aproximado de titulares afectados;
6. Los sistemas de tratamiento y datos personales comprometidos;
7. Las acciones correctivas realizadas de forma inmediata;
8. La descripción de las posibles consecuencias de la vulneración de seguridad ocurrida;
9. Las recomendaciones dirigidas al titular;
10. El medio puesto a disposición del titular para que pueda obtener mayor información al respecto;
11. El nombre completo de la o las personas designadas y sus datos de contacto, para que puedan proporcionar mayor información al Instituto, en caso de requerirse, y
12. Cualquier otra información y documentación que considere conveniente hacer del conocimiento del Instituto.

* **Notificación de las vulneracines de seguridad al titular[[22]](#footnote-22)**

En la notificación que realice el responsable al titular sobre las vulneraciones de seguridad a que se refieren los artículos 40 de la Ley General y 66 de los presentes Lineamientos generales deberá informar, al menos, lo siguiente:

1. La naturaleza del incidente o vulneración ocurrida;
2. Los datos personales comprometidos;
3. Las recomendaciones dirigidas al titular sobre las medidas que éste pueda adoptar para

proteger sus intereses;

1. Las acciones correctivas realizadas de forma inmediata;
2. Los medios puestos a disposición del titular para que pueda obtener mayor información al respecto;
3. La descripción de las circunstancias generales en torno a la vulneración ocurrida, que ayuden al titular a entender el impacto del incidente, y
4. Cualquier otra información y documentación que considere conveniente para apoyar a los titulares.
5. **TRANSFERENCIA DE DATOS PERSONALES**

La Ley General define como transferencia en el artículo 3 fracción XXXII, a toda comunicación de datos personales dentro o fuera del territorio mexicano, realizada a persona distinta del titular, del responsable o del encargado.

1. Todas las transferencias sean nacionales e internacionales deben formalizarse mediante la suscripción de un instrumento jurídico, para demostrar el alcance del tratamiento de los datos personales, las obligaciones y responsabilidades contraídas por las partes, salvo en las siguientes excepciones:

a) Cuando la transferencia sea nacional y se realice en virtud del cumplimiento de una disposición legal o en el ejercicio de las atribuciones expresamente conferidas.

b) Cuando la transferencia sea internacional y se encuentre prevista en una ley o tratado suscrito y ratificado por México, o derivado de una petición de la autoridad extranjera u organismo internacional en su carácter de receptor,

c) Cuando las facultades entre el sujeto obligado y el responsable receptor sean homólogas o las transferencias sean análogas respecto de aquéllas que dieron origen al tratamiento.

1. Sólo hacer transferencias fuera del territorio nacional cuando el tercero receptor se obligue a proteger los datos personales conforme a los principios y deberes que establece la Ley General y demás disposiciones aplicables en la materia.
2. Comunicar el aviso de privacidad respectivo al tercero receptor en las transferencias nacionales e internacionales que se realicen.

4. Las Transferencias que se pueden hacer aún sin el consentimiento de la persona titular**[[23]](#footnote-23)**

* Esté prevista en la Ley, convenios o Tratados Internacionales.
* Se realice entre responsables, siempre y cuando los DP se utilicen para el ejercicio de facultades propias, compatibles o análogas
* Sea legalmente exigida para la investigación y persecución de los delitos.
* Sea precisa para el reconocimiento, ejercicio o defensa de un derecho ante autoridad competente, siempre y cuando medie el requerimiento de esta última .
* Sea necesaria para la prevención o el diagnóstico médico, la prestación de asistencia sanitaria, tratamiento médico o la gestión de servicios sanitarios.
* Sea precisa para el mantenimiento o cumplimiento de una relación jurídica entre el Responsable y el Titular.
* Sea necesaria por virtud de un contrato celebrado o por celebrar en interés del Titular, por el Responsable y un tercero.
* En los casos en los que el Responsable no esté obligado a recabar el consentimiento del Titular para el tratamiento y transmisión de sus Datos Personales .
* Sea necesaria por razones de seguridad nacional.

1. **COMITÉ DE TRANSPARENCIA DE LA AEM**

La AEM cuenta con un Comité de Transparencia, que de conformidad con el artículo 83 de la Ley General, es la autoridad máxima en materia de protección de datos personales, tiene las siguientes atribuciones y funciones en materia de protección de datos personales, se encuentra conformado por:

* Titular de la Unidad de Transparencia
* Titular del Órgano Interno de Control
* Titular del Área Coordinadora de Archivos

De acuerdo con lo dispuesto por el artículo 84 de la Ley General, el Comité de Transparencia tenrá las siguientes funciones:

1. *Coordinar, supervisar y realizar las acciones necesarias para garantizar el derecho a la protección de los datos personales en la organización del responsable, de conformidad con las disposiciones previstas en la presente Ley y en aquellas disposiciones que resulten aplicables en la materia;*
2. *Instituir, en su caso, procedimientos internos para asegurar la mayor eficiencia en la gestión de las solicitudes para el ejercicio de los derechos ARCO;*
3. *Confirmar, modificar o revocar las determinaciones en las que se declare la inexistencia de los datos personales, o se niegue por cualquier causa el ejercicio de alguno de los derechos ARCO;*
4. *Establecer y supervisar la aplicación de criterios específicos que resulten necesarios para una mejor observancia de la presente Ley y en aquellas disposiciones que resulten aplicables en la materia;*
5. *Supervisar, en coordinación con las áreas o unidades administrativas competentes, el cumplimiento de las medidas, controles y acciones previstas en el documento de seguridad;*
6. *Dar seguimiento y cumplimiento a las resoluciones emitidas por el Instituto y los organismos garantes, según corresponda;*
7. *Establecer programas de capacitación y actualización para los servidores públicos en materia de protección de datos personales, y*
8. *Dar vista al órgano interno de control o instancia equivalente en aquellos casos en que tenga conocimiento, en el ejercicio de sus atribuciones, de una presunta irregularidad respecto de determinado tratamiento de datos personales; particularmente en casos relacionados con la declaración de inexistencia que realicen los responsables.*
9. **OFICIAL DE DATOS PERSONALES**

La AEM cuenta con una persona Oficial de Protección de Datos, quien tiene, entre otras atribuciones, la de auxiliar y orientar al titular que lo requiera con relación al ejercicio del derecho a la protección de datos personales; asesorar a las Unidades Administrativas de la AEM obligado en materia de protección de datos personales; así como hacer las gestiones necesarias para el manejo, mantenimiento, seguridad y protección de los sistemas de datos personales en posesión del responsable.

La persona oficial de protección de datos personales tendrá las siguientes atribuciones**[[24]](#footnote-24)**:

1. *Asesorar al Comité de Transparencia respecto a los temas que sean sometidos a su consideración en materia de protección de datos personales;*
2. *Proponer al Comité de Transparencia políticas, programas, acciones y demás actividades que correspondan para el cumplimiento de la Ley General y los presentes Lineamientos generales;*
3. *Implementar políticas, programas, acciones y demás actividades que correspondan para el cumplimiento de la Ley General y los presentes Lineamientos generales, previa autorización del Comité de Transparencia;*
4. *Asesorar permanentemente a las áreas adscritas al responsable en materia de protección de datos personales, y*
5. *Las demás que determine el responsable y la normatividad que resulte aplicable.*

El presente documento denominado “Guía de Protección de Datos Personales de la Agencia Espacial Mexicana, fue aprobado por unanimidad por el Comité de Transparencia en su cuarta sesión ordinaria que se llevó a cabo el **05 de octubre de 2023** que consta en el **Acta No. A-CT-ORD-AEM-04/2023**, de conformidad con lo establecido en los artículos 30 fracción II, 83 y 84 fracción I y 87 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y 47 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público.

1. [Artículo](https://www.diputados.gob.mx/LeyesBiblio/pdf/LAEM.pdf) 1 de la Ley que crea la Agencia Espacial Mexicana [↑](#footnote-ref-1)
2. Artículo 1, párrafo quinto de la Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados [↑](#footnote-ref-2)
3. Artículos 29 y 30 de la Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados y 46 y 47 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público [↑](#footnote-ref-3)
4. Art. 44 de la Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados y Art. 92 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público [↑](#footnote-ref-4)
5. Art. 45 de la Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados y Art. 93 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público [↑](#footnote-ref-5)
6. Art. 46 de la Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados y Art. 94 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público [↑](#footnote-ref-6)
7. Art. 47 de la Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados y Art. 95 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público [↑](#footnote-ref-7)
8. Artículo 17 de la Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados y 8 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público [↑](#footnote-ref-8)
9. Artículo 18 de la Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados y 9 y 10 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público [↑](#footnote-ref-9)
10. Artículo 19 de la Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados y 11 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público [↑](#footnote-ref-10)
11. Artículos 20, 21 y 22 de la Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados y 12 a 20 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público [↑](#footnote-ref-11)
12. Artículos 23 y 24 de la Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados y 21,22 y 23 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público [↑](#footnote-ref-12)
13. Artículos 25 de la Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados, 24 y 25 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público [↑](#footnote-ref-13)
14. Artículos 3, fracción II, 26, 27 y 28 de la Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados y 26 a 45 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público [↑](#footnote-ref-14)
15. Artículos 29 y 30 de la Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados y 46 a 54 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público [↑](#footnote-ref-15)
16. Artículo 42 de la Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados y 71 y 72 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público [↑](#footnote-ref-16)
17. Artículos 31 al 36 de la Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados y 55 al 65 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público [↑](#footnote-ref-17)
18. Artículos 3, fracción XIV y 35 de la Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados y 55 al 65 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público [↑](#footnote-ref-18)
19. Artículo 65 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público [↑](#footnote-ref-19)
20. Artículo 66 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público [↑](#footnote-ref-20)
21. Artículo 67 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público [↑](#footnote-ref-21)
22. Artículo 68 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público [↑](#footnote-ref-22)
23. Artículo 70 de la Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados [↑](#footnote-ref-23)
24. Artículo 122 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público [↑](#footnote-ref-24)