AEM
AGENCIA ESPACIAL MEXICANA

Documento de Seguridad

Medidas de seguridad en el tratamiento de Datos Personales en posesión de la Agencia Espacial Mexicana

Diciembre 2024.

2024 Felipe Carrillo PUERTO
BENEMÉRITO DEL PROLETARIADO, REVOLUCIONARIO Y DEFENSOR DEL MAYAB

AEM
AGENCIA ESPACIAL MEXICANA

Documento de Seguridad y Protección de Datos Personales

Índice

Introducción

En 11 de junio de 2002, se promulgó la *Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental*, en la cual se regularon las excepciones para la divulgación de información pública, entre las que se estableció la confidencialidad de los datos personales, entendidos como la información concerniente a una persona física identificada o identificable, incluida la información relativa a su origen étnico o racial, o la referida a las características físicas, morales o emocionales, la vida afectiva y familiar, domicilio, número telefónico, patrimonio, ideología y opiniones políticas, creencias o convicciones religiosas o filosóficas, los estados de salud físicos o mentales, las preferencias sexuales, u otras análogas que afecten su intimidad. Asimismo, establece los parámetros iniciales para la conformación de un sistema protección de los datos personales.

El 30 de septiembre de 2005, el entonces Instituto Federal de Acceso a la Información Pública (IFAI) publicó, en el Diario Oficial de la Federación, los *Lineamientos de protección de datos personales*, cuyo artículo trigésimo tercero establecía que el **Documento de Seguridad** era aquel "elaborado por las dependencias, conjuntamente con sus áreas de tecnología de la información, informática o su equivalente, las medidas administrativas, físicas y técnicas aplicables a los sistemas de datos personales".

En el ámbito constitucional, el 20 de julio de 2007 se publicó una reforma al artículo 6º de *Constitución Política de los Estados Unidos Mexicanos,* en la cual se adiciona un segundo párrafo, con siete fracciones. En su fracción II, dispuso "La

información que se refiere a la vida privada y los datos personales será protegida en los términos y con las excepciones que fijen las leyes.

En el mismo sentido, el uno de junio de 2009 se publicó, en el Diario Oficial de la Federación, el Decreto por el cual se adicionó un párrafo segundo, al artículo 16, en el que se establece el derecho de toda persona a la protección de sus datos personales.

Con estos actos, se reconocen a los datos personales como un derecho humano, el cual, está intrínsecamente relacionado con su titular, por lo que, su uso o tratamiento inadecuado afectan o pueden afectar su bienestar personal, inclusive económico.

El 26 de enero de 2017 se publicó la *Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados*, que regula los principios seguir en la recopilación de datos personales, el ejercicio de los derechos ARCO (ACCESO, RECTIFICACIÓN, CANCELACIÓN y OPOSICIÓN) así como las medidas que los Sujetos Obligados deben adoptar para la debida protección de los mismos.

Dicha ley dispone que los sujetos obligados, que realicen tratamiento de datos personales deben regirse por ocho principios y dos deberes. Los principios son los de **LICITUD, LEALTAD, INFORMACIÓN, CONSENTIMIENTO, FINALIDAD, PROPORCIONALIDAD, CALIDAD Y RESPONSABILIDAD**; mientras que los deberes son CONFIDENCIALIDAD y SEGURIDAD.

Estos principios, deberes y derechos imponen, a los sujetos responsables, una serie de obligaciones que encaminadas a garantizar la protección de los datos personales, con el objeto de respetar el **Derecho a la autodeterminación de los titulares.**

Respecto de la protección que todo sujeto obligado debe adoptar, se encuentra el Documento de Seguridad que, de conformidad con el artículo 3, fracción XIV, dicho documento es el "Instrumento que describe y da cuenta de manera general sobre las medidas de seguridad técnicas, físicas y administrativas adoptadas por 5 el responsable para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que posee".

Objetivo

Contar con un instrumento que describa y de cuenta de manera general sobre las medidas de seguridad técnicas, físicas y administrativas adoptadas por la Agencia Espacial Mexicana para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que posee y protegerlos contra un posible daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado.

Fundamento legal

El Documento de Seguridad se elabora con fundamento en lo establecido en los artículos 35, 83 y 84, fracción I, de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados

Marco normativo

Constitución Política de los Estados Unidos Mexicanos (DOF. 05/02/1917 y sus reformas).

Ley Orgánica de la Administración Pública Federal (DOF. 29/12/1976 y sus reformas).

Ley General de Archivos (DOF. 15/06/2018 y sus reformas).

Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (DOF. 26/01/2017).

Ley General de Transparencia y Acceso a la Información Pública (DOF. 04/05/2015 y sus reformas).

Ley Federal de Procedimiento Administrativo (DOF. 04/08/1994 y sus reformas).

Ley Federal de Transparencia y Acceso a la Información Pública (DOF. 09/05/2016 y sus reformas).

Reglamento Interior de la Secretaría de Infraestructura, Comunicaciones y Transportes (DOF. 29/01/24).

Acuerdo mediante el cual se aprueban los Lineamientos Generales de Protección de Datos Personales para el Sector Público (DOF.26/01/2018).

ACUERDO mediante el cual se establece el Programa de Evaluación Anual 2024, de los sujetos obligados del ámbito público federal, en relación con el desempeño en el cumplimiento de las disposiciones contenidas en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y demás normatividad aplicable en la materia (DOF.17/11/2023).

ACUERDO mediante el cual se aprueba la modificación al diverso ACTPUB/31/10/2023.08, por el cual se establece el Programa de Evaluación Anual 2024, de los sujetos obligados del ámbito público federal, en relación con el desempeño en el cumplimiento de las disposiciones contenidas en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y demás normatividad aplicable en la materia (DOF.29/02/2024).

Glosario

AEM: Agencia Espacial Mexicana.

Amenaza: Circunstancia o condición externa, con la capacidad de causar daño a los activos explotando una o más de sus vulnerabilidades.

Aviso de privacidad: Documento puesto a disposición del Titular de forma física, electrónica o en cualquier otro formato, generado por la AEM a partir del momento en el cual se recaban sus datos personales, con el objeto de informarle los propósitos del tratamiento de los mismos; ya sea en formato integral o simplificado, o en su caso, en formato corto.

Bases de datos: Conjunto ordenado de datos personales referentes a una persona física identificada o identificable, condicionados a criterios determinados, con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización.

Comité de Transparencia (CT): Órgano Colegiado de la AEM, máxima autoridad en materia de datos personales, con la facultad para validar la inexistencia de datos personales o la negativa que se realice en materia de derechos ARCO, mediante resolución.

Confidencialidad: Propiedad de la información para evitar su acceso, divulgación o revelación, no autorizados.

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

Costos: Conceptos de reproducción y/o envió de los datos personales, según la modalidad de entrega que solicite el Titular.

Datos personales: Cualquier información concerniente a una persona física identificada o identificable. Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información.

Datos personales sensibles: Aquellos que se refieran a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve 37 un riesgo grave para éste. De manera enunciativa más no limitativa, se consideran sensibles los datos personales que puedan revelar aspectos como origen racial o étnico, estado de salud presente o futuro, información genética, creencias religiosas, filosóficas y morales, opiniones políticas y preferencia sexual.

Derechos ARCO: Los derechos de Acceso, Rectificación, Cancelación y Oposición al tratamiento de datos personales.

Días: Días hábiles.

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.

Encargado: La persona física o jurídica, pública o privada, ajena a la organización del responsable, que sola o conjuntamente con otras trate datos personales a nombre y por cuenta del responsable.

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.

Incidente de seguridad: Cualquier violación a las medidas de seguridad físicas, técnicas o administrativas de un responsable, que afecte la confidencialidad, la integridad o la disponibilidad de la información.

Institución Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, el Instituto o INAI: Órgano Garante en materia de Protección de Datos Personales en Posesión de los Sujetos Obligados en materia federal.

Ley General: 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.

Medidas de seguridad: Conjunto de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permitan proteger los datos personales.

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

Responsable: Cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos, ya sea en el ámbito federal, estatal y municipal, respecto de los datos personales que obtiene, usa, registra, organiza, conserva, elabora, utiliza, comunica, difunde, almacena, posee, accede, maneja, aprovecha, divulga, transfiere o dispone.

Revelación: Incidente de seguridad en el cual se expone la información a través de Internet o medios masivos de comunicación.

Riesgo: Potencial o probabilidad de que ocurra un escenario donde una amenaza explote una o varias vulnerabilidades existentes en un activo o grupo de activos, y que éste cause un impacto negativo o daño.

Sistema de tratamiento: Conjunto de elementos mutuamente relacionados o que interactúan para realizar la obtención, uso, registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de datos personales, en medios físicos o electrónicos.

Sujetos Obligados: Por Ley, en el ámbito federal, estatal y municipal, cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos.

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

Tercero: La persona física o moral, nacional o extranjera, distinta del titular o del responsable de los datos.

Titular: La persona física a quien corresponden los datos personales.

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

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: las áreas de la AEM que almacenan administran o por razones de sus actividades o funciones pueden obtener, contar, dar tratamiento en la calidad de Responsable o Encargados de las bases de datos personales.

Unidad de Transparencia: Área Administrativa de la AEM, que actúa en su calidad de mandataria respecto de la atención de las solicitudes de Derechos ARCO realizada por los Titulares, y auxiliar en la procuración y el tratamiento de los datos personales realizada por la Agencia Espacial Mexicana.

Vulnerabilidad: Circunstancia o condición propia de un activo, que puede ser explotada por una o más amenazas para causarle daño.

Vulneración de seguridad: Incidente de seguridad que afecta los datos personales en cualquier fase de su tratamiento. De acuerdo con el artículo 63 del Reglamento de la LFPDPPP y 38 de la LGPDPPSO, se consideran al menos las siguientes vulneraciones: (i) La pérdida o destrucción no autorizada; (ii) el robo, extravío o copia no autorizada; (iii) el uso, acceso o tratamiento no autorizado, o (iv) el daño, la alteración o modificación no autorizada.

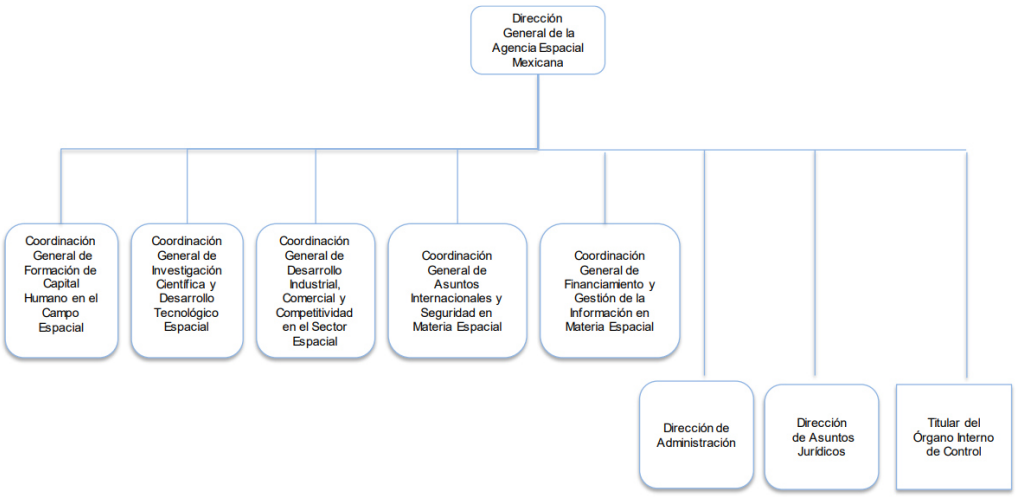
Ámbito de aplicación

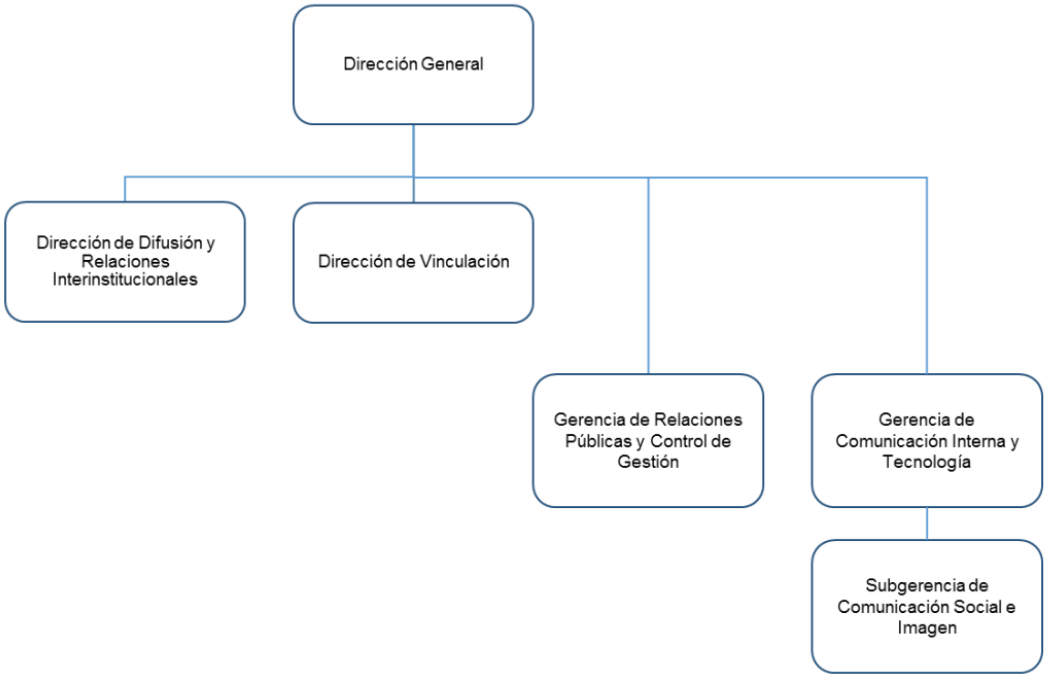
El documento de seguridad es de observancia obligatoria para las Unidades Administrativas de la Agencia Espacial Mexicana que traten datos personales.

Estructura de la Agencia Espacial Mexicana

De conformidad con el Manual de Organización General de la Agencia Espacial Mexicana, publicado en el Diario Oficial de la Federación el 23 de marzo de 2020, la AEM cuenta con las siguientes unidades administrativas:

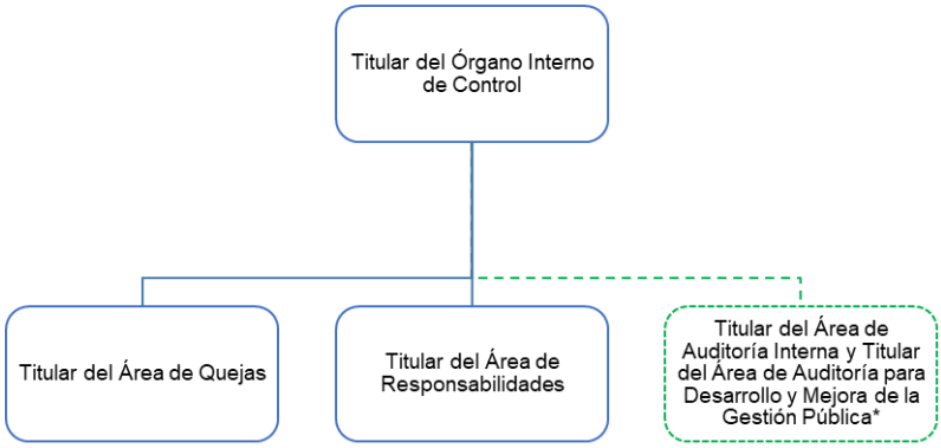
a) Dirección General de la Agencia Espacial Mexicana.




Dirección General
Dirección de Difusión y Relaciones Interinstitucionales
Dirección de Vinculación
Gerencia de Relaciones Públicas y Control de Gestión
Gerencia de Comunicación Interna y Tecnología
Subgerencia de Comunicación Social e Imagen

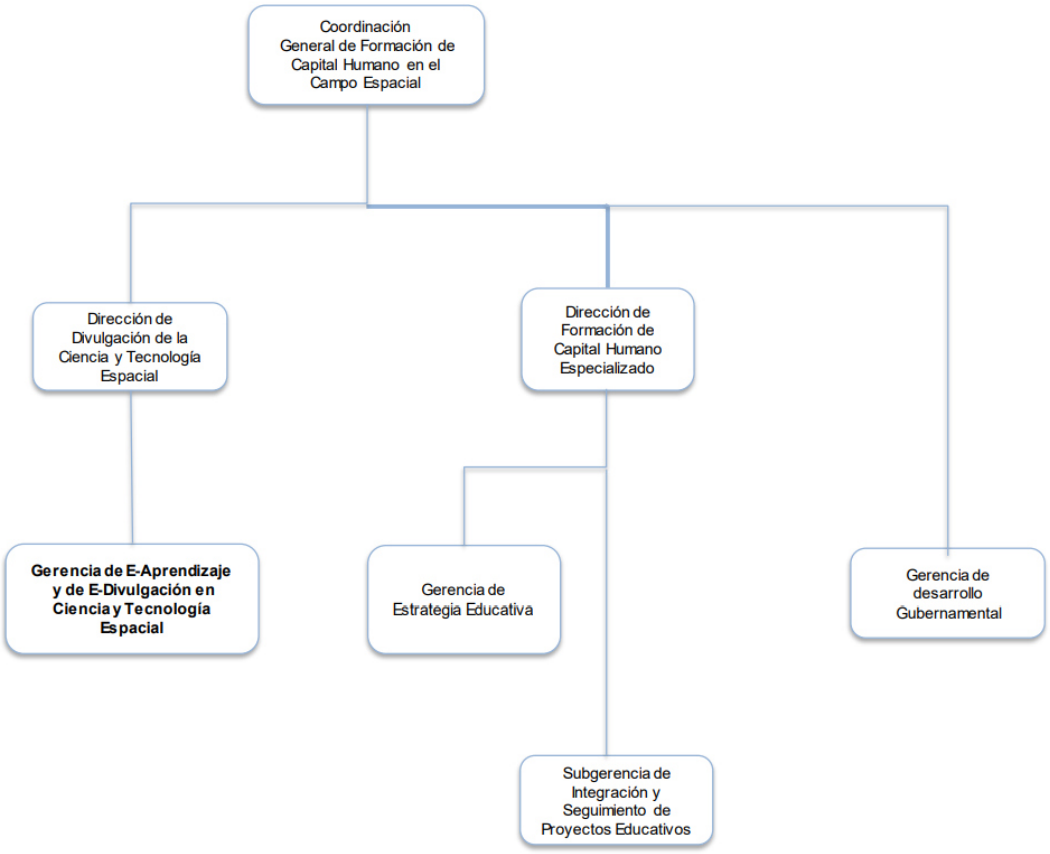

2024
Felipe Carrillo
PUERTO

b) Órgano Interno de Control

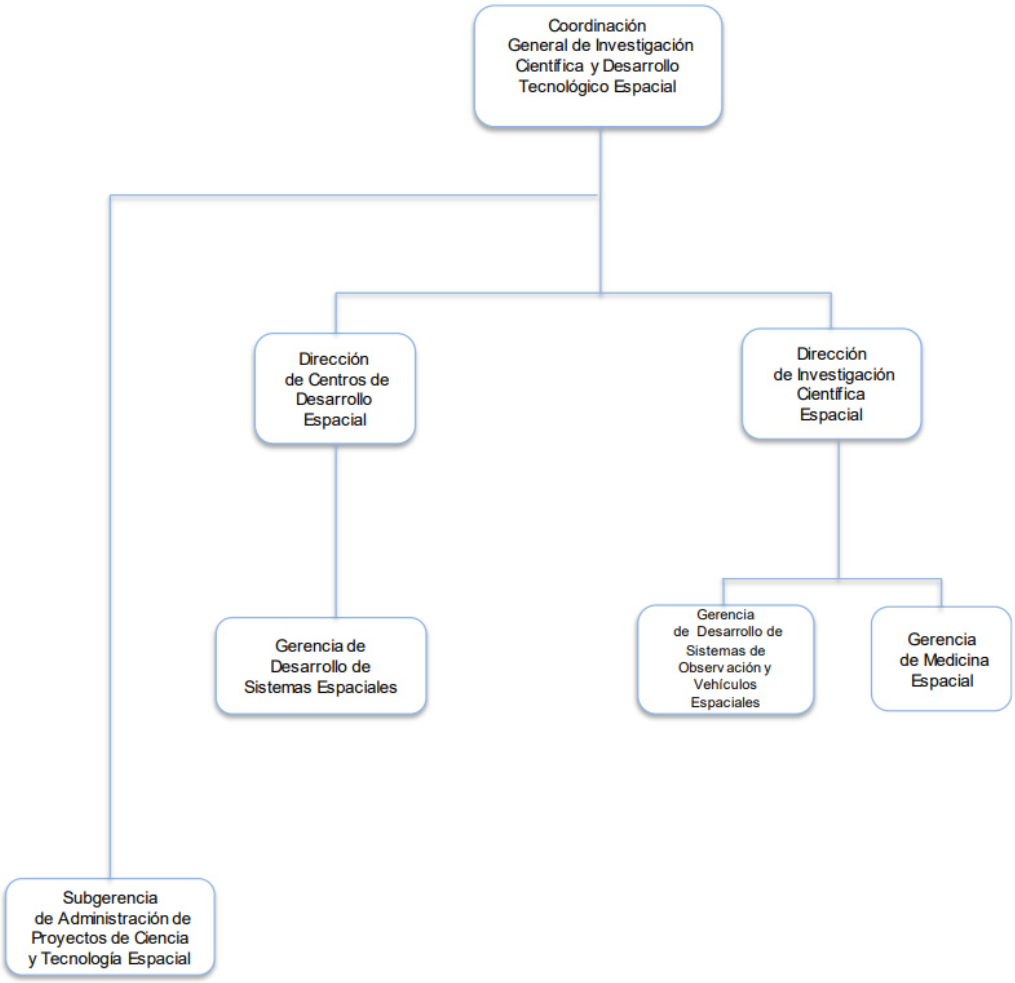


*Área dictaminada sin recursos a la fecha de elaboración de este Manual

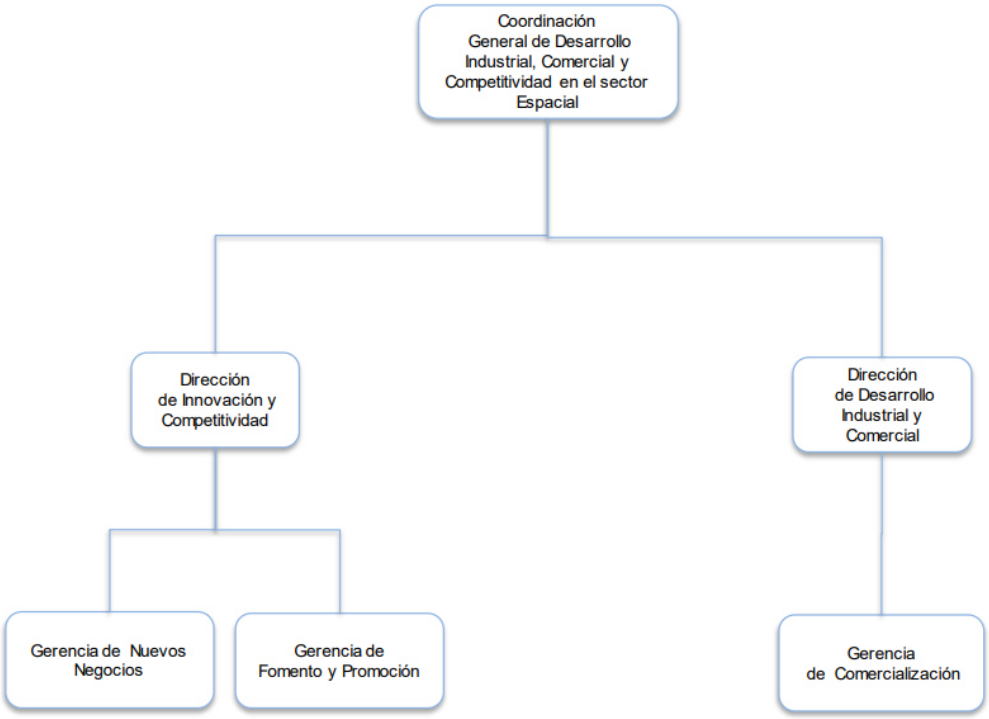
c) Coordinación General de Formación de Capital Humano en el Campo Espacial



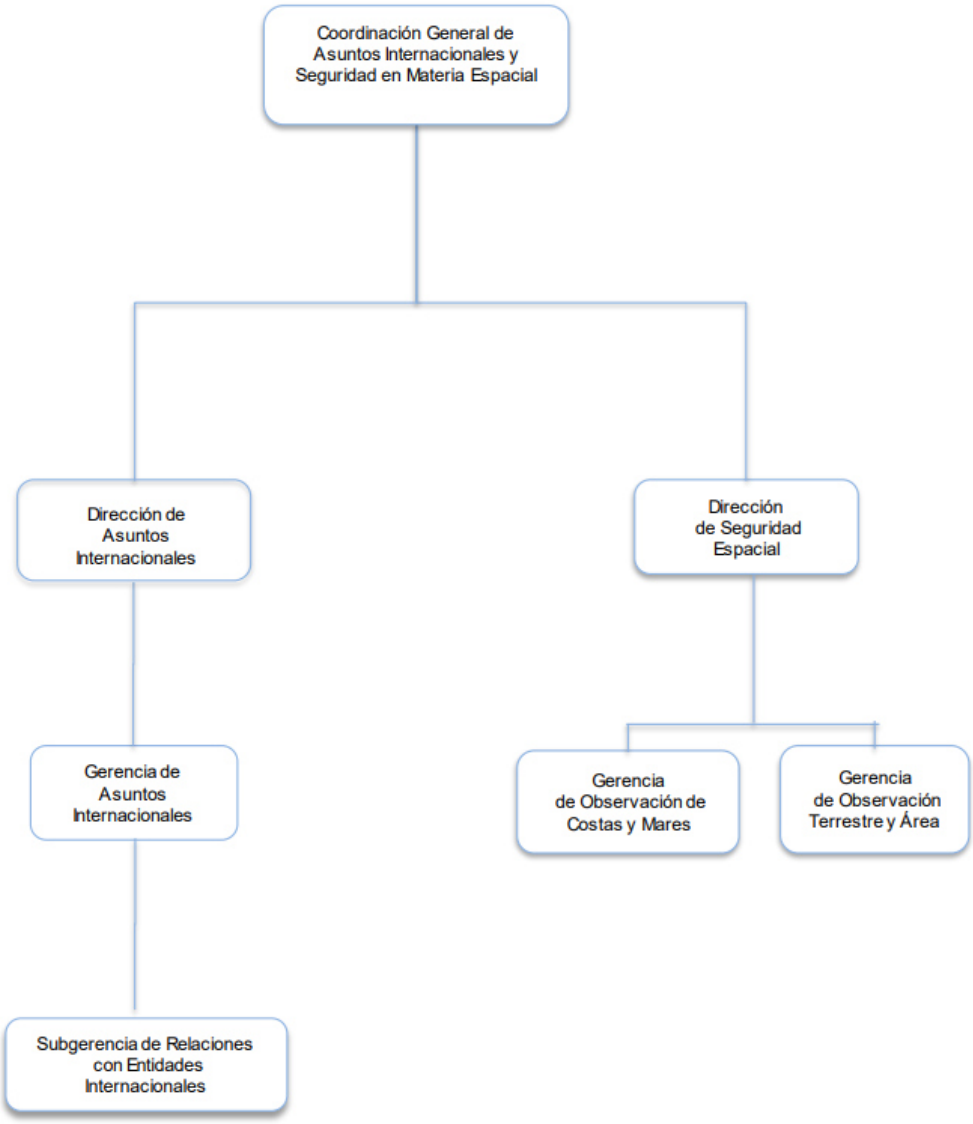
d) Coordinación General de Investigación Científica y Desarrollo Tecnológico Espacial



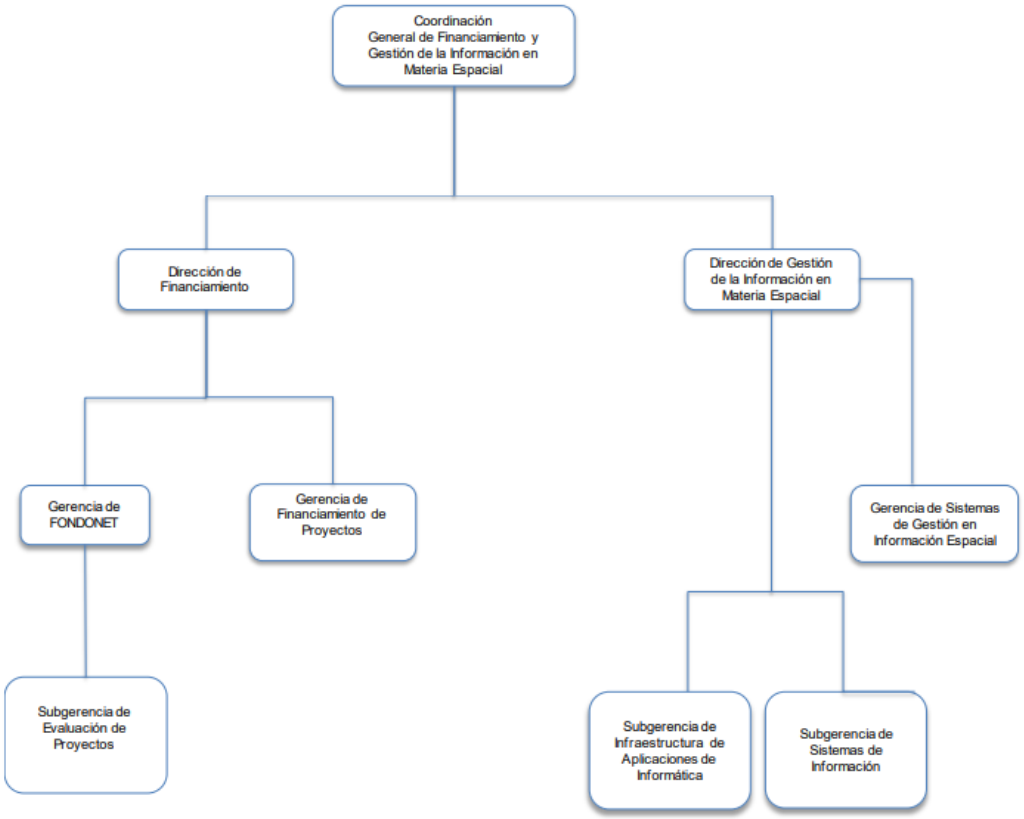
e) Coordinación General de Desarrollo Industrial, Comercial y Competitividad en el Sector Espacial



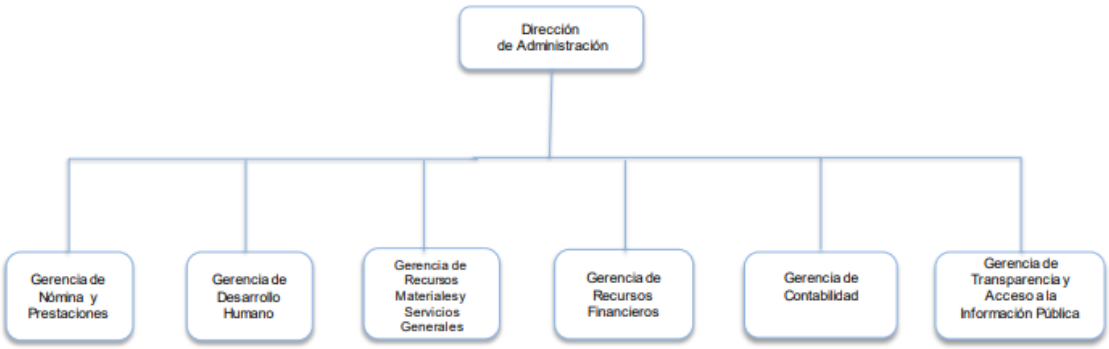
f) Coordinación General de Asuntos Internacionales y Seguridad en Materia Espacial



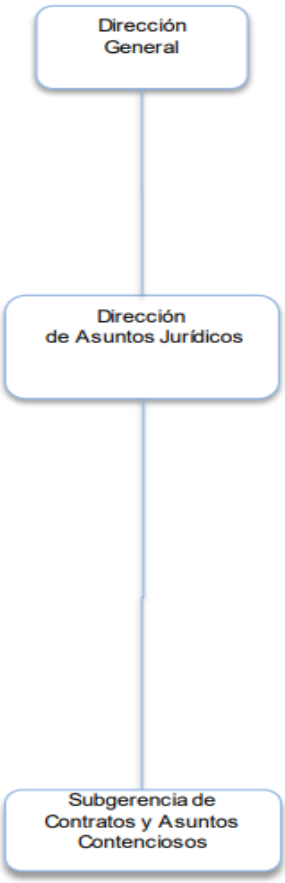
g) Coordinación General de Financiamiento y Gestión de la Información en Materia Espacial



h) Dirección de Administración



i) Dirección de Asuntos Jurídicos



Inventario de datos personales para el Documento de Seguridad

- **Coordinación General de Formación de Capital Humano en el Campo Espacial.**

A) Medios físicos y electrónicos a través de los que se obtienen los datos personales.

- Directamente en el contacto con el ponente.
- Indirectamente cuando otra persona lo refiere.

B) Finalidades de cada tratamiento de datos personales.

- Gestión logística para su participación como ponente.
- Verificar su registro para permitir acceso al evento.
- Evidencia fotográfica y/o en vídeo de la ejecución del evento.
- Emisión y entrega de constancias.

C) Catálogo de tipos de datos personales que se traten.

- Categoría de datos estándar: Identificación, Contacto, Ubicación y Laborales.
- Categoría de datos sensibles: Ninguno.

D) Catálogo de formatos de almacenamiento y la descripción general de ubicación física o electrónica de los datos personales.

- Medios de almacenamiento físico: Ninguno.
- Medios de almacenamiento electrónicos:
- Equipo de cómputo.
- Drive.
- Correo electrónico.
- Equipo celular.

Avenida Insurgentes Sur 1685, interior 301 y 1301, Colonia Guadalupe Inn, Alcaldía Álvaro Obregón, C.P. 01020, Ciudad de México, México.

- **Coordinación General de Financiamiento y Gestión de la Información en Materia Espacial.**

A) Medios físicos y electrónicos a través de los que se obtienen los datos personales.

  - Indirecta.

B) Finalidades de cada tratamiento de datos personales.

  - Seguimiento financiero y contable de los Fideicomisos en los que participa como proveedor.
  - Verificación de la aplicación de los fondos económicos del Fideicomiso.

C) Catálogo de tipos de datos personales que se traten.

  - Categoría de datos estándar: Identificación, Ubicación, Financieros y/o patrimoniales y Datos de situación legal.
  - Categoría de datos sensibles: Ninguno.

D) Catálogo de formatos de almacenamiento y la descripción general de ubicación física o electrónica de los datos personales.

  - Medios de almacenamiento físico: Ninguno.
  - Medios de almacenamiento electrónicos:
    - Equipo de cómputo.
    - Drive.
    - Correo electrónico.

Avenida Insurgentes Sur 1685, interior 301 y 1301, Colonia Guadalupe Inn, Alcaldía Álvaro Obregón, C.P. 01020, Ciudad de México, México.

- **Coordinación General de Investigación Científica y Desarrollo Tecnológico Espacial.**

A) Medios físicos y electrónicos a través de los que se obtienen los datos personales.

- Directamente, al realizar su registro en las bitácoras de uso.
- Directamente, en el registro de su firma en documentos relacionados con el subproceso.

B) Finalidades de cada tratamiento de datos personales.

- Registro del uso de instrumentos o materiales de la AEM.
- Validación del registro del uso del instrumentos o materiales de la AEM en caso de desperfectos de dichos instrumentos o materiales.
- Elaboración y registro de documentos base para la gestión de las Prácticas Profesionales o del Servicio Social de alumnos que le son asignados con tal motivo.
- Elaboración y registro de documentos base para la gestión de Estancias.

C) Catálogo de tipos de datos personales que se traten.

- Categoría de datos estándar: Identificación, Contacto, Ubicación y Laborales.
- Categoría de datos sensibles: Ninguno.

D) Catálogo de formatos de almacenamiento y la descripción general de ubicación física o electrónica de los datos personales.

- Medios de almacenamiento físico:
  - Libreta de registro de uso de instrumentos o materiales de la AEM.
  - Documentos en los que consta el sustento del subproceso.

Centro Regional de Desarrollo Espacial – Zacatecas: Circuito Marie Curie Exterior lote I Interior manzana 1; Colonia la Escondida; C.P. 98160, Zacatecas, Zacatecas conocido como (CREDES - Zacatecas).

Centro Regional de Desarrollo Espacial – Estado de México: Anillo Perimetral S/N Zona Industrial Santa Bárbara Atlacomulco, Estado de México, C.P. 50458. (CREDES – Estado de México).

- Medios de almacenamiento electrónicos:
  - No aplica.

- **Coordinación General de Desarrollo Industrial, Comercial y Competitividad en el Sector Espacial.**

  A) Medios físicos y electrónicos a través de los que se obtienen los datos personales.

  - Indirectamente en la búsqueda en Internet o a través de otros actores.
  - Directamente cuando el actor los entrega a la AEM.

  B) Finalidades de cada tratamiento de datos personales.

  - Envío de invitación para participar en eventos de vinculación.
  - Logística para ejecución del evento.
  - Verificación de identidad para la entrega de gafetes.
  - Evidencia fotográfica y/o en vídeo de la ejecución del evento.
  - Comunicar sus datos de identificación y contacto a otros actores de la industria espacial como parte de las acciones de vinculación.

  C) Catálogo de tipos de datos personales que se traten.

  - Categoría de datos estándar: Identificación, Contacto, Ubicación y Laborales.
  - Categoría de datos sensibles: Ninguno.

  D) Catálogo de formatos de almacenamiento y la descripción general de ubicación física o electrónica de los datos personales.

  - Medios de almacenamiento físico:
    - Listas de entrega de gafetes.

  Avenida Insurgentes Sur 1685, interior 301 y 1301, Colonia Guadalupe Inn, Alcaldía Álvaro Obregón, C.P. 01020, Ciudad de México, México.

  - Medios de almacenamiento electrónicos:
    - Equipo de cómputo.

- Drive.
- Correo electrónico.
- Equipo celular.

Avenida Insurgentes Sur 1685, interior 301 y 1301, Colonia Guadalupe Inn, Alcaldía Álvaro Obregón, C.P. 01020, Ciudad de México, México.

- **Coordinación General de Asuntos Internacionales y Seguridad en Materia Espacial.**

A) Medios físicos y electrónicos a través de los que se obtienen los datos personales.

- Conforme a la indicada por cada área que ejecuta la actividad a reportar.

B) Finalidades de cada tratamiento de datos personales.

- Análisis de actividades para elaboración de informes.

C) Catálogo de tipos de datos personales que se traten.

- Categoría de datos estándar: Identificación, Educativos o académicos y Laborales.
- Categoría de datos sensibles: Ninguno.

D) Catálogo de formatos de almacenamiento y la descripción general de ubicación física o electrónica de los datos personales.

- Medios de almacenamiento físico: No aplica.
- Medios de almacenamiento electrónicos:
  - Equipo de cómputo.
  - Drive.
  - Correo electrónico.
  - Equipo celular.

Avenida Insurgentes Sur 1685, interior 301 y 1301, Colonia Guadalupe Inn, Alcaldía Álvaro Obregón, C.P. 01020, Ciudad de México, México.

- **Dirección de Administración.**

A) Medios físicos y electrónicos a través de los que se obtienen los datos personales.

- Directamente, los entrega el empleado o lo generado durante sus actividades.

B) Finalidades de cada tratamiento de datos personales.

- Conformación de su expediente como empleado.
- Gestión de alta como empleado.
- Conocer su estado de salud y medicamentos que toma.
- Brindar la capacitación que se requiera como empleado y contar con la evidencia de dicha capacitación.
- Control de los movimientos que generen sus nombramientos.
- Control y administración de su expediente como empleado.
- Felicitarlo por su cumpleaños.
- Elaboración de credencial como servidor público adscrito a la AEM.
- Registro, control y administración de nombramientos.
- Registro, control y administración de asistencias.
- Registro, control y administración de vacaciones.
- Registro, control y administración de las capacitaciones a las que asiste.
- Registro, control y administración de renuncias o separaciones.
- Contacto posterior a su baja para comunicarle situaciones relacionadas con el cargo de separación.
- Registro, control y administración de la evaluación del desempeño.
- Registro, control y administración de la estructura organizacional de la institución.
- Asesoría y apoyo para la emisión de su declaración patrimonial.
- Resguardo de su documentación.
- Atender a denuncias o procedimientos judiciales o administrativos.
- Brindar apoyo en emergencias.

C) Catálogo de tipos de datos personales que se traten.

- Categoría de datos estándar: Identificación, Contacto, Ubicación, Identificativos, Académicos o educativos, Laborales, Financieros y/o patrimoniales y Biométricos.
- Categoría de datos sensibles: Estado de Salud, Padecimiento o enfermedad que deba conocer la institución y Situaciones personales (para la justificación de incidencias).

D) Catálogo de formatos de almacenamiento y la descripción general de ubicación física o electrónica de los datos personales.

- Medios de almacenamiento físico:
  - Expediente del empleado – gaveta de almacenamiento.

Avenida Insurgentes Sur 1685, interior 301 y 1301, Colonia Guadalupe Inn, Alcaldía Álvaro Obregón, C.P. 01020, Ciudad de México, México.

- Medios de almacenamiento electrónicos:
  - Equipo de cómputo.
  - Drive.
  - Correo electrónico.
  - Teams.
  - Equipo celular.
  - Expediente digital.

Avenida Insurgentes Sur 1685, interior 301 y 1301, Colonia Guadalupe Inn, Alcaldía Álvaro Obregón, C.P. 01020, Ciudad de México, México.

- **Dirección de Asuntos Jurídicos.**

A) Medios físicos y electrónicos a través de los que se obtienen los datos personales.

- Directamente en la petición formal.
- Indirectamente por la notificación de la demanda.
- Directamente conforme lo obtuvieron las áreas de la AEM.

B) Finalidades de cada tratamiento de datos personales.

- Documentación de las peticiones realizadas con motivo de la ejecución de sus actividades laborales.
- Identificar a las personas involucradas/mencionadas/referidas en los asuntos litigiosos y validar los hechos relacionados para la defensa de la institución.
- Identificar los hechos relacionados con el asunto litigioso de que se trate, a efecto de elaborar y gestionar los documentos correspondientes para la atención del asunto frente a la autoridad que está sustanciando el litigio.
- Gestión para la atención de la sustanciación del asunto litigioso."

C) Catálogo de tipos de datos personales que se traten.

- Categoría de datos estándar: Identificación, Laborales y Datos de situación legal.
- Categoría de datos sensibles: Ninguno.

D) Catálogo de formatos de almacenamiento y la descripción general de ubicación física o electrónica de los datos personales.

- Medios de almacenamiento físico:
  - Gavetas físicas para el resguardo de oficios.
  - Gavetas físicas para el resguardo de expedientes.

Avenida Insurgentes Sur 1685, interior 301 y 1301, Colonia Guadalupe Inn, Alcaldía Álvaro Obregón, C.P. 01020, Ciudad de México, México.

- Medios de almacenamiento electrónicos:
  - Equipo de cómputo.
  - Drive.
  - Correo electrónico.

Avenida Insurgentes Sur 1685, interior 301 y 1301, Colonia Guadalupe Inn, Alcaldía Álvaro Obregón, C.P. 01020, Ciudad de México, México.

Funciones y Obligaciones de las personas que traten datos personales.

1. Funciones sustantivas del personal de la AEM.

Las funciones sustantivas de los servidores públicos que forman parte de la AEM se documentan en la "Descripción y perfil de puestos" de la institución, los que se publican en: Perfiles de Puestos de la Agencia Espacial Mexicana | Agencia Espacial Mexicana | Gobierno | gob.mx

2. Funciones y obligaciones en materia de protección de datos personales del personal de la AEM.

Normatividad en materia de protección de datos personales	Es obligación de todos los servidores públicos de la AEM conoce y aplicar las disposiciones aplicables a la protección de los datos personales en posesión de la institución:
	* Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados en el Diario Oficial de la Federación el día 26 de enero de 2017. * Lineamientos Generales de Protección de Datos Personales para el Sector Público, publicado en el Diario Oficial de la Federación el día 25 de noviembre de 2020. *Adición de un Título Decimo a los Lineamientos Generales de Protección de Datos Personales para el Sector Público, publicado en el Diario Oficial de la Federación el día 23 de enero de 2018.
	* Lineamientos que establecen los parámetros, modalidades y procedimeintos para la portabilidad de datos personales publicados en el Diario Oficial de la Federación el día 12 de febrero de 2019. *Reglas de Operación del Registro de Esquemas de Mejores Prácticas en el Diario Oficial de la Federación, el día 24 de junio de 2020. * Demás disposiciones aplicables en materia de protección de datos personales.

Instrumento de la institución para la protección de los datos personales en posesión de AEM.	Conocer y aplicar los instrumentos que la AEM ha emitido para la protección de los datos personales en su posesión, tales como Avisos de Privacidad, Ciclos de Vida, Inventarios de Datos Personales y Políticas, Procedimientos, Protocolos en materia de protección de datos personales, entre otros
Capacitación en materia de protección de datos personales.	Asistir activamente a las capacitaciones en materia de protección de datos personales que la Institución programe.
	Aprobar las evaluaciones que conforme los conocimientos proporcionados en las capacitaciones en materia de protección de datos personales.

Obligación frente a los Tribunales de datos personales.	Identificar las categorías de Titulares de datos personales de quiénes se realiza tratamiento de la información que lo identifica o lo hace identificable.
	Conocer y aplicar los Archivos de Privacidad que son aplicables a los Titulares de datos personales.
	En caso de que el servidor público sea quién tiene el primer contacto con el Titular de datos personales, poner a disposición el Aviso de Privacidad aplicabl, y en su caso, obtener su consentimiento.
	Realizar el tratamiento de datos personales de los Titulares conforme a los instrumentos que resulten aplicables, tales como Avisos de Privacidad, Politícas de Privacidad, Procedimientos, entre otros.
	Realizar el tratamiento de los datos personales privilegiando la protección de los intereses de los Titulares y su expectativa razonable de privacidad.
Conservación de datos personales	Conocery aplicar los instrumentos que la institución ha emitido para la conservación, bloqueo y supresión de los datos personales en su posesión.
	Realizar la supresión de los datos personales asegurando que el procedimiento adoptado sea seguro y confidencial, amigable con el medio ambiante e irreversibles.

Solicitudes para el ejercicio de Derechos ARCOP (acceso, rectificación, cancelación, oposición y portabilidad)	Hacer del conocimiento inmediato de la Unidad de Transparencia de las solicitudes para el ejercicio de Derechos ARCOP, que le sean presentadas directamente por Titulares de datos personales. En caso de que le sea requerida información para que la AEM atienda solicitudes para el ejercicio de Derechos ARCOP atender oportunamente a dichos requerimientos.
Dudas y quejas en materia de protección de datos personales.	Hacer del conocimiento inmediato de la Unidad de Transparencia de la dudas y quejas en materia de protección de datos personales que le sean presentadas directamente por Titulares de datos personales.

Medidas de seguridad en materia de protección de datos personales	Conocer, adoptar e implimentar las medidas de seguridad físicas, técnicas y administrativas que la AEM ha definido para proteger los datos personales en su posesión.
	En caso de que le sea requerida información para que la AEM evalué e implemente medidas de seguridad, atender oportunamente a dichos requerimientos.
	Hacer del conocimiento inmediato de la Unidad de Transparencia y del área responsable de la Seguridad de la Información y Datos personales de las vulneraciones de seguridad de las que tenga conocimiento.
	En caso de que le sea requerida información para que la AEM evalúe una vulneración en las medidas de seguridad, atender oportunamente a dichos requerimientos.
Comunicación con terceros.	Conocer e identificar las comunicaciones que se realicen con terceros ajenos a la organización, ya sea como remisión subremisión o transferencia de datos personales.
	Cumplir con las obligaciones que la AEM se ha compremetido con terceros ajenos a la organización.

Supervisión y vigilancia.	Atender oportunamete a las acciones de supervisión y vigilancia de cumplimiento de los instrumentos que la institución ha adoptado en materia de protección de datos personales.

3. Análisis de riesgos.

La AEM ha establecido un procedimiento para la Gestión de Riesgos en materia de Seguridad de la Información, el cual contempla los siguientes rubros.

Objetivo de la Gestión de Riesgos	Alcance de la Gestión de Riesgos:	Metodología de la Gestión de Riesgos	Política de Gestión de Riesgos.
•Evaluar los probables escenarios que pudieran impactar sobre los activos e infraestructura donde se soporta la infromación y los datos de AEM, con la finalidad de mitigar sobre la disponibilidad, integridad y confidencialidad de la información;esto a traves de un análisis y definición de acciones y controles que permitan un adecuado tratamiento de los riesgos.	•La evaluación y tratamiento de riesgos se aplican al alcacnce del Sistema de Gestión de Seguridad de Datos personales (SGSDP); es decir, a todos los activos que se utiliza dentro de la dependencia y que pueden tener un impacto a nivel de seguridad de la información y privacidad de datos.	•Se establece la forma de evaluar y tratar los riesgos de Seguridad de la información a través del documento:"Procedimiento de Gestión deRiesgos **(ref. PR-GR-AEM01).**	•El responsable de la Gestión de Riesgos (según la matriz de roles y responsabilidades) deberá realizar el analisis de riesgos y establecer la matriz de gestión de riesgos al menos una vez al año; esto conforme al Procedimiento de Gestión de Riesgos **(ref. PR-GR-AEM01)**

Para el año 2024 la AEM ha realizado su ejercicio de análisis de riesgo y que por su contenido se clasifica como información confidencial.

4. Análisis de brecha.

A través de la **Matriz de Controles de Seguridad y Análisis de Brecha (FO-GRAEM04),** se establecen los controles de seguridad implementados y no implementados. Es decir, se declara la aplicabilidad a través de su estatus de implementación.

Se define que los controles no implementados y que sean alcance del Análisis y Tratamiento de Riesgos deben ser considerados como prioritarios para su implementación.

La declaración de aplicabilidad deberá actualizarse al menos una vez al año para poder verificar que los controles de seguridad con estatus de "no implementados" vayan cambiando al estatus "si implementados". También puede actualizarse la Matriz de Controles de Seguridad cuando la dependencia así lo considere necesario (por ejemplo: cuando hayamos sido ejecutadas acciones de implementación importantes, proyectos o adquisiciones que traigan como resultado la implementación de controles, etc.).

Para el año 2024 la AEM ha realizado su ejercicio de análisis de brecha y que por su contenido se clasifica como información confidencial.

5. Plan de trabajo.

A través e la Matriz de Controles de Seguridad y Análisis de Brecha (**FO-GR-AEM04**), se establecen las acciones, responsables y fechas para la implementación de los controles que tengan el estatus de "no implementados".

Dicha matriz, puede contener otros elementos que sean relevantes como: referencia a proyectos, adquisiciones o justificaciones por la cuales no se han podido implementar.

Para el año 2024 la AEM ha realizado su plan de trabajo y que por su contenido se clasifica como información confidencial.

6. Mecanismos de monitoreo y revisión de las medidas de seguridad.

Revisión Administrativa

- La AEM debe realizar las acciones necesarias para la planeación y ejecución de la evaluación y análisis detallados de los procesos, plítica, actividades y controles que forman parte del SGSPD por lo que debe observar lo dispuesto en el Procedimiento de Revisiones Administrativas **(ref. PR-QP-AEM02).**

Auditorías.

- La AEM debe realizar las acciones necesarias para la planeación y ejecución de las auditorías del SGPDP por lo que se debe observar lo dispuesto en el Procedimiento de Auditorías **(ref. PR-DP-AEM03).**