COMUNICACIONES
SECRETARÍA DE INFRAESTRUCTURA, COMUNICACIONES Y TRANSPORTES

COMITÉ DE TRANSPARENCIA

Documento de Seguridad en materia de protección de datos personales en posesión de la Secretaría de Infraestructura, Comunicaciones y Transportes (Versión Pública).

Vigencia: Julio 2024

Contenido

Introducción

De conformidad con lo establecido en el artículo 29 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (en adelante, Ley General) la Secretaría de Infraestructura, Comunicaciones y Transportes (SICT), como sujeto obligado y responsable del tratamiento de datos personales, debe de implementar mecanismos para acreditar el cumplimiento y observancia de los principios de licitud, lealtad, información, consentimiento, finalidad, proporcionalidad, calidad y responsabilidad, de los deberes de confidencialidad y seguridad, así como de las demás obligaciones establecidas en la normatividad aplicable.

El artículo 35 de la Ley General establece la obligación de elaborar un Documento de Seguridad entendido como 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.

En ese sentido, y con la finalidad de dar cumplimiento a dicha obligación, se elaboró el **"Documento de Seguridad en materia de protección de datos personales en posesión de la Secretaría de Infraestructura, Comunicaciones y Transportes"**, el cual comprende el inventario de datos personales y de los sistemas de tratamiento con los que se cuenta, las funciones y obligaciones de las personas servidoras públicas que tratan datos personales, el análisis de riesgos y de brecha, el plan de trabajo, los mecanismos de monitoreo y revisión de las medidas de seguridad así como el programa general de capacitación.

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 Secretaría de Infraestructura, Comunicaciones y Transportes 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 y 17, fracción X, de los Lineamientos de Integración y Funcionamiento del Comité de Transparencia de la Secretaría de Infraestructura, Comunicaciones y Transportes.

Ámbito de aplicación

El Documento de Seguridad es de observancia obligatoria para las Unidades Administrativas Centrales y Centros SICT de la Secretaría de Infraestructura, Comunicaciones y Transportes que traten datos personales.

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 ACT-PUB/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).
- **Lineamientos de Integración y funcionamiento del Comité de Transparencia de la Secretaría de Infraestructura, Comunicaciones y Transportes** (Normateca Interna, abril 2024).
- **Políticas de Gestión de Datos Personales de la Secretaría de Infraestructura, Comunicaciones y Transportes** (Normateca Interna, mayo 2024).
- **Catálogo de Datos Personales e Información Confidencial de la Secretaría de Infraestructura, Comunicaciones y Transportes** (Normateca Interna, enero 2023).

I. Inventario de datos personales y de los sistemas de tratamiento.

De conformidad con lo establecido en el artículo 3, apartado A, del DECRETO por el que se expide el Reglamento Interior de la Secretaría de Infraestructura, Comunicaciones y Transportes (DOF. 29/01/2024), la SICT cuenta con las siguientes unidades administrativas centrales:

Oficina del C. Secretario

- Dirección General de Comunicación Social
- Dirección General Patrimonial y del Derecho de Vía
- Dirección General de Planeación
- Dirección General de Vinculación
- Coordinación de Centros SICT

Subsecretaría de Infraestructura

- Dirección General de Carreteras
- Dirección General de Conservación de Carreteras
- Dirección General de Desarrollo Carretero
- Dirección General de Desarrollo Ferroviario y Multimodal
- Dirección General de Servicios Técnicos

Subsecretaría de Comunicaciones y Transportes

- Dirección General de Autotransporte Federal
- Dirección General de Protección y Medicina Preventiva en el Transporte
- Dirección General de Inclusión Digital y Redes de Telecomunicaciones
- Dirección General de Políticas de Telecomunicaciones y Radiodifusión

Unidad de Administración y Finanzas

- Dirección General de Programación y Presupuesto
- Dirección General de Recursos Humanos y Organización
- Dirección General de Recursos Materiales y Servicios Generales
- Dirección General de Tecnologías de Información y Comunicaciones

Unidad de Asuntos Jurídicos

- Dirección Ejecutiva de Procesos Contenciosos
- Dirección Ejecutiva Normativa
- Dirección Ejecutiva Operativa
- Dirección Ejecutiva de Supervisión y Control Jurídico de Centros SICT
- Dirección Ejecutiva de Coordinación Jurídica entre las Unidades Administrativas con las Entidades del Sector

Del mismo modo, el artículo 3, apartado B, del mismo Reglamento, establece que la SICT cuenta con Oficinas de Representación en las Entidades Federativas, siendo éstas las siguientes:

Aguascalientes	**Baja California**	**Baja California Sur**	**Campeche**
Chiapas	**Chihuahua**	**Coahuila**	**Colima**
Durango	**Estado de México**	**Guanajuato**	**Guerrero**
Hidalgo	**Jalisco**	**Michoacán**	**Morelos**
Nayarit	**Nuevo León**	**Oaxaca**	**Puebla**
Querétaro	**Quintana Roo**	**San Luis Potosí**	**Sinaloa**
Sonora	**Tabasco**	**Tamaulipas**	**Tlaxcala**
Veracruz	**Yucatán**	**Zacatecas**	

I.I. Catálogo de medios a través de los cuales se obtienen datos personales.

De conformidad con lo establecido en los artículos 33, fracción III, de la Ley General y 58, fracción I, de los Lineamientos Generales de Protección de Datos Personales para el Sector Público, el inventario de datos personales debe contener el catálogo de medios físicos y electrónicos a través de los cuales se obtienen los datos personales.

Con base en lo anterior, se precisa que, en la SICT, los datos personales se obtienen a través de los siguientes medios:

a) Directamente del titular.
b) A través de su representante legal.
c) Vía telefónica.
d) Por correo electrónico.
e) Por internet o sistema informático.

I.II. Finalidades del tratamiento.

De conformidad con lo establecido en los artículos 33, fracción III, de la Ley General y 58, fracción II, de los Lineamientos Generales de Protección de Datos Personales para el Sector Público, el inventario de datos personales debe contener las finalidades de cada tratamiento de datos personales que se realice en el sujeto obligado.

Al respecto, se precisa que, en la SICT, se cuenta con Avisos de Privacidad entendidos como los documentos puestos a disposición del titular de forma física, electrónica o en cualquier formato generado por el responsable, a partir del momento en el cual se recaban sus datos personales, con el objeto de informarle los propósitos del tratamiento de los mismos.

Los Avisos de Privacidad que ha aprobado el Comité de Transparencia, y en los cuales se describen las finalidades específicas para cada tratamiento de datos personales que se realiza, son públicos y se encuentran disponibles para su consulta en el micrositio de la Unidad de Transparencia, a través del siguiente enlace electrónico:

https://www.sct.gob.mx/transparencia-sct/proteccion-de-datos-personales/proteccion-de-datos-personales-sict/avisos-de-privacidad-integrales/

I.III. Tipos de datos personales.

De conformidad con lo establecido en los artículos 33, fracción III, de la Ley General y 58, fracción III, de los Lineamientos Generales de Protección de Datos Personales para el Sector Público, el inventario de datos personales debe contener el catálogo de los tipos de datos personales que se tratan, indicando si son, o no, sensibles.

En ese sentido, la Unidad de Transparencia realizó el levantamiento del inventario de datos personales en posesión de la SICT, y se identificaron principalmente los siguientes:

No.	Dato Personal	Descripción
1	CURP	Clave alfanumérica que se integra por datos personales que sólo conciernen al particular titular de ésta, como son su nombre, apellidos, fecha de nacimiento, lugar de nacimiento y sexo. Dichos datos, constituyen información que distingue plenamente a una persona física del resto de los habitantes del país, por lo que se considera como información confidencial.
2	Correo electrónico	Dirección electrónica que se utiliza habitualmente en comunicaciones privadas, que pueden contener en su integración de forma voluntaria o involuntaria información acerca de su titular, como son nombre

		y apellidos, fecha de nacimiento, país de residencia, etc.
3	Domicilio	Dato personal confidencial que se asocia a una persona identificada o identificable, siendo éste el lugar donde la misma reside.
4	Edad	Se refiere a la información natural de tiempo que ha vivido una persona, que por su propia naturaleza incide en la esfera privada de sus titulares, así si el dato corresponde a los años cumplidos por una persona física identificable, o si en el caso a través de su composición por la referencia o data en que ocurrió el nacimiento o meramente el año de registro, se actualiza la necesidad de protección al ser un dato personal.
5	Fecha de nacimiento	Dato personal que hace identificable a una persona, pues la sitúa en una condición de indudable identificación, ya que este dato correlacionado con el nombre permite por sí mismo, acceder a un sin número de datos requeridos en la más variada prestación de servicios de todo tipo, por lo que su uso y conocimiento concierne solo a su titular.
6	Firma	Escritura gráfica o grafo manuscrito que representa al nombre y apellido (s) o, título que una persona escribe de su propia mano, que tiene fines de identificación, jurídicos, representativos y diplomáticos, a través de los cuales es posible identificar o hacer identificable a su titular.
7	Lugar de nacimiento	Municipio, estado o país del cual es originario un individuo, lo que permitiría relacionar a una persona física identificada con su origen geográfico o territorial.
8	Nacionalidad	Atributo de la personalidad que señala al individuo como miembro de un estado es decir es el vínculo legal que relaciona a una persona con su nación de origen.
9	Número de pasaporte	Se considera un dato personal que debe clasificarse como confidencial, ya que publicarlo permitiría a cualquier tercero allegarse de información que haga localizable e identificable a su titular, tomando en consideración que el pasaporte mexicano es prueba de la nacionalidad mexicana.
10	RFC	Clave de carácter fiscal, única e irrepetible, que permite identificar al titular, su edad y fecha de nacimiento. De acuerdo con la legislación tributaria, las personas físicas tramitan su inscripción en el Registro Federal de Contribuyentes con el único propósito de realizar mediante esa clave de

		identificación, operaciones o actividades de naturaleza tributaria.
11	Teléfono	Dato numérico de acceso al servicio de telefonía fija o celular asignado por empresa o compañía que lo proporciona, y que corresponde al uso en forma particular, personal y privada, con independencia de que éste se proporcione para un determinado fin o propósito a terceras personas, incluidas autoridades o prestadores de servicio. Dato personal que debe protegerse y sólo podrá otorgarse mediante el consentimiento de su titular.

Del mismo modo, y con fundamento en lo establecido en el artículo 3, fracción X, de la Ley General se identificaron los siguientes datos personales sensibles:

No.	Dato Personal Sensible	Descripción
1	Grupo sanguíneo o tipo de sangre	De la clasificación de la sangre, se puede obtener información necesaria para conocer el estado de salud, el grupo y tipo de sangre, la huella genética o el perfil de ADN entre otros condicionantes de la salud o sus antecedentes.
2	Datos médicos	Información que permite conocer datos relativos al estado de salud físico o mental de una persona física, así como su historial clínico. Como son: uso de lentes y comorbilidades.
3	Datos biométricos	Información que permite conocer las propiedades físicas, fisiológicas, de comportamiento o rasgos de la personalidad, atribuibles a una sola persona y que son medibles como fotografía, huella dactilar y huella digital.

I.IV. Catálogo de formatos de almacenamiento.

De conformidad con lo establecido en los artículos 33, fracción III, de la Ley General y 58, fracción IV, de los Lineamientos Generales de Protección de Datos Personales para el Sector Público, el inventario de datos personales debe contener el catálogo de formatos de almacenamiento, así como la descripción general de la ubicación física y/o electrónica de los datos personales.

Al respecto, se precisa que en la SICT los datos personales son resguardados en medio físico conocido como archivo de trámite, bajo las medidas de seguridad físicas y administrativas implementadas por las unidades responsables, o bien, en medio electrónico a través de los sistemas de tratamiento de datos personales, considerando las medidas de seguridad técnicas, físicas y administrativas correspondientes.

I.V. Personas servidoras públicas con acceso a los sistemas de tratamiento.

De conformidad con lo establecido en los artículos 33, fracción III, de la Ley General y 58, fracción V, de los Lineamientos Generales de Protección de Datos Personales para el Sector Público, el inventario de datos personales debe contener la lista de personas servidoras públicas que tienen acceso a los sistemas de tratamiento.

Al respecto, se precisa que, en la SICT, se encuentran debidamente identificadas las personas servidoras públicas que tienen acceso a los datos personales que se tratan con base en sus facultades y atribuciones, así como para las finalidades descritas en los Avisos de Privacidad.

II. Funciones y obligaciones de quienes tratan datos personales.

De conformidad con lo establecido en los artículos 33, fracción II, de la Ley General y 57 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público, en la SICT existen obligaciones definidas para las personas servidoras públicas que tratan datos personales.

De manera enunciativa más no limitativa, se enlistan las siguientes:

1. Observar los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad, entendidos de la siguiente manera:

   Licitud: El tratamiento de datos personales por parte del responsable deberá sujetarse a las facultades o atribuciones que la normatividad aplicable le confiera.

   Finalidad: Todo tratamiento de datos personales que efectúe el responsable deberá estar justificado por finalidades concretas, licitas, explícitas y legítimas, relacionadas con las atribuciones que la normatividad aplicable les confiera.

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

   Consentimiento: Cuando no se actualicen alguna de las causales de excepción previstas en el artículo 22 de la Ley General, deberá contar con el consentimiento previo del titular.

   Calidad: El responsable deberá adoptar 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 estos.

   Proporcionalidad: El responsable solo deberá tratar los datos responsables que resulten adecuados, relevantes y estrictamente necesarios para la finalidad que justifica su tratamiento.

   Información: El responsable deberá informar al titular a través del aviso de privacidad, la existencia y características principales del tratamiento al que serán sometidos sus datos personales, a fin de que pueda tomar decisiones informadas al respecto.

   Responsabilidad: El responsable deberá implementar los mecanismos previos en el artículo 30 de la Ley General para acreditar el cumplimiento de los principios,

deberes y obligaciones establecidos en la Ley y rendir cuentas sobre el tratamiento de datos personales.

2. Cumplir con los deberes de seguridad y confidencialidad, entendidos de la siguiente manera:

   Seguridad: se refiere a la obligación de establecer y mantener medidas de seguridad tanto técnicas, físicas y administrativas, que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado.

   Confidencialidad: toda persona tiene derecho a que sus datos personales sean tratados con confidencialidad, es decir, a que éstos no se difundan o compartan con terceros, salvo que exista consentimiento para ello o alguna obligación normativa requiera su difusión.

3. El tratamiento de datos personales deberá sujetarse a las facultades o atribuciones que la normatividad aplicable le confiera.

4. Todo tratamiento de datos personales que se efectúe deberá estar justificado por finalidades concretas, lícitas, explícitas y legítimas, relacionadas con las atribuciones que la normatividad aplicable les confiera.

5. Sólo deberán tratar los datos personales que resulten adecuados, relevantes y estrictamente necesarios para la finalidad que justifica su tratamiento.

6. Conocer el Aviso de Privacidad, integral y simplificado, del tratamiento de datos personales en el que participa.

7. 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.

8. En todo momento, se deberá de privilegiar la protección de los datos personales del titular.

9. Conocer la normatividad en materia de protección de datos personales.

10. Acreditar los cursos de capacitación en la materia a los que sean convocados por la Unidad de Transparencia.

Cabe precisar que las funciones específicas de cada persona servidora pública dependen del proceso que se trate, del nivel de responsabilidad de su encargo y del rol en el que participen dentro del tratamiento. En ese sentido, éstas se encuentran definidas en la legislación y normatividad que rige el actuar de la Secretaría de Infraestructura, Comunicaciones y Transportes.

III. Análisis de Riesgo, Análisis de Brecha y Plan de Trabajo.

De conformidad con lo establecido en los artículos 35, fracciones III, IV y V, de la Ley General y 60, 61 y 62 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público, parte integrante del Documento de Seguridad son el análisis de riesgo, el análisis de brecha y el plan de trabajo.

El artículo 35, fracciones III, IV y V, de la Ley General establece lo siguiente:

> ***Artículo 35.*** *De manera particular, el responsable deberá elaborar un documento de seguridad que contenga, al menos, lo siguiente:*
>
> *...*
>
> *III. El análisis de riesgos;*
>
> *IV. El análisis de brecha;*
>
> *V. El plan de trabajo;*
>
> *...*

Asimismo, los artículos 60, 61 y 62 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público, establecen lo siguiente:

> ***Artículo 60****. Para dar cumplimiento al artículo 33, fracción IV, de la Ley General, el responsable deberá realizar un* ***análisis de riesgos*** *de los datos personales tratados considerando lo siguiente:*
>
> *I. Los requerimientos regulatorios, códigos de conducta o mejores prácticas de un sector específico;*
> *II. El valor de los datos personales de acuerdo a su clasificación previamente definida y su ciclo de vida;*
> *III. El valor y exposición de los activos involucrados en el tratamiento de los datos personales;*
> *IV. Las consecuencias negativas para los titulares que pudieran derivar de una vulneración de seguridad ocurrida, y*
> *V. Los factores previstos en el artículo 32 de la Ley General.*
>
> ***Artículo 61****. Con relación al artículo 33, fracción V, de la Ley General, para la realización del* ***análisis de brecha*** *el responsable deberá considerar lo siguiente:*
>
> *I. Las medidas de seguridad existentes y efectivas;*
> *II. Las medidas de seguridad faltantes, y*
> *III. La existencia de nuevas medidas de seguridad que pudieran reemplazar a uno o más controles implementados actualmente.*
>
> ***Artículo 62****. De conformidad con lo dispuesto en el artículo 33, fracción VI, de la Ley General, el responsable deberá elaborar un* ***plan de trabajo*** *que defina las acciones a implementar de acuerdo con el resultado del análisis de riesgos y del análisis de brecha, priorizando las medidas de seguridad más relevantes e inmediatas a establecer.*

Lo anterior, considerando los recursos designados; el personal interno y externo en su organización y las fechas compromiso para la implementación de las medidas de seguridad nuevas o faltantes.

Por su parte, el artículo 33, fracciones IV, V y VI, de la Ley General establece lo siguiente:

***Artículo 33**. Para establecer y mantener las medidas de seguridad para la protección de los datos personales, el responsable deberá realizar, al menos, las siguientes actividades interrelacionadas:*

IV. Realizar un análisis de riesgo de los datos personales, considerando las amenazas y vulnerabilidades existentes para los datos personales y los recursos involucrados en su tratamiento, como pueden ser, de manera enunciativa más no limitativa, hardware, software, personal del responsable, entre otros;

V. Realizar un análisis de brecha, comparando las medidas de seguridad existentes contra las faltantes en la organización del responsable; y

VI. Elaborar un plan de trabajo para la implementación de las medidas de seguridad faltantes, así como las medidas para el cumplimiento cotidiano de las políticas de gestión y tratamiento de los datos personales.

Con base en dichas obligaciones, se integró este apartado como un acercamiento certero para evaluar las medidas de seguridad necesarias para proteger los datos personales en la Secretaría de Infraestructura, Comunicaciones y Transportes.

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

De conformidad con lo establecido en el artículo 3, fracción XX, de la Ley General, las medidas de seguridad se definen como el conjunto de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permiten proteger a los datos personales contra daños, pérdidas, alteración, destrucción, uso, acceso o tratamiento no autorizado, así como para garantizar su confidencialidad, integridad y disponibilidad.

En ese sentido, la SICT, como responsable, debe establecer y mantener medidas de seguridad de carácter administrativo, físico y técnico para la protección de los datos personales en su posesión, de conformidad con lo previsto en los artículos 31, 32 y 33 de la Ley General.

Se entenderán como medidas administrativas, técnicas y físicas las siguientes:

- **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.

- **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. De manera enunciativa más no limitativa, se deben considerar las siguientes actividades:

  a) Prevenir que el acceso a las bases de datos o a la información, así como a los recursos, sea por usuarios identificados y autorizados;

  b) Generar un esquema de privilegios para que el usuario lleve a cabo las actividades que requiere con motivo de sus funciones;

  c) Revisar la configuración de seguridad en la adquisición, operación, desarrollo y mantenimiento del software y hardware, y

  d) Gestionar las comunicaciones, operaciones y medios de almacenamiento de los recursos informáticos en el tratamiento de datos personales.

- **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. De manera enunciativa más no limitativa, se deben considerar las siguientes actividades:
  a) Prevenir el acceso no autorizado al perímetro de la organización, sus instalaciones físicas, áreas críticas, recursos e información;

  b) Prevenir el daño o interferencia a las instalaciones físicas, áreas críticas de la organización, recursos e información;

  c) Proteger los recursos móviles, portátiles y cualquier soporte físico o electrónico que pueda salir de la organización, y

  d) Proveer a los equipos que contienen o almacenan datos personales de un mantenimiento eficaz, que asegure su disponibilidad e integridad.

Ahora bien, de conformidad con lo establecido en el artículo 33, fracción VII, de la Ley General y 63 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público, se

deberán monitorear y revisar de manera periódica las medidas de seguridad implementadas, así como las amenazas y vulneraciones a las que están sujetos los datos personales.

Para cumplir con dicha actividad, en la Secretaría de Infraestructura, Comunicaciones y Transportes se monitorean continuamente los siguientes elementos:

I. Los nuevos activos que se incluyan en la gestión de riesgos;

II. Las modificaciones necesarias a los activos, como podría ser el cambio o migración tecnológica, entre otras;

III. Las nuevas amenazas que podrían estar activas dentro y fuera de la Secretaría y que no han sido valoradas;

IV. La posibilidad de que vulnerabilidades nuevas o incrementadas sean explotadas por las amenazas correspondientes;

V. Las vulnerabilidades identificadas para determinar aquéllas expuestas a amenazas nuevas o pasadas que vuelvan a surgir;

VI. El cambio en el impacto o consecuencias de amenazas valoradas, vulnerabilidades y riesgos en conjunto, que resulten en un nivel inaceptable de riesgo, y

VII. Los incidentes y vulneraciones de seguridad ocurridas.

Aunado a lo anterior, el responsable debe contar con un programa de auditoría, interno y/o externo, para monitorear y revisar la eficacia del sistema de gestión.

Cabe precisar que el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) realiza auditorías voluntarias en materia de protección de datos personales, para evaluar algún procedimiento o tratamiento de datos personales de los sujetos obligados con el objeto de conocer la adaptación, adecuación y eficiencia de los controles, medidas y mecanismos implementados para cumplir con las disposiciones previstas en la Ley General.

V. Programa General de Capacitación.

De conformidad con lo establecido en los artículos 33, fracción VIII, y 64 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público de la Ley General, es necesario diseñar y aplicar diferentes niveles de capacitación del personal, dependiendo de los roles y responsabilidades respecto del tratamiento de los datos personales.

Para este fin, en la SICT se debe tomar en cuenta lo siguiente:

I. Los requerimientos y actualizaciones del sistema de gestión;

II. La legislación vigente en materia de protección de datos personales y las mejores prácticas relacionadas con el tratamiento de éstos;

III. Las consecuencias del incumplimiento de los requerimientos legales o requisitos organizacionales, y

IV. Las herramientas tecnológicas relacionadas o utilizadas para el tratamiento de los datos personales y para la implementación de las medidas de seguridad.

Con base en lo anterior, anualmente, se integra y aprueba un Programa de Capacitación en Transparencia, Acceso a la Información, Protección de Datos Personales y Temas Relacionados, con la finalidad de fortalecer el conocimiento en la materia de las personas servidoras públicas que integran a este sujeto obligado.

CONTROL DE CAMBIOS DEL DOCUMENTO

Fecha de autorización del cambio	Código y número de revisión	Tipo de cambio	Nombre del documento	Descripción del cambio
		Emisión.	Documento de Seguridad en materia de protección de datos personales en posesión de la Secretaría de Infraestructura, Comunicaciones y Transportes (Versión Pública).	Se emite el documento en cumplimiento de lo establecido en el artículo 35 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.