INSTITUTO FEDERAL DE TELECOMUNICACIONES

PROGRAMA DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DEL INSTITUTO FEDERAL DE TELECOMUNICACIONES

2023- 2024

Tabla de contenido

APROBACIÓN

El Acuerdo mediante el cual el Comité de Transparencia del Instituto Federal de Telecomunicaciones aprobó el "Programa de Protección de Datos Personales del Instituto Federal de Telecomunicaciones 2023-2024", se emitió en cumplimiento a los artículos 16, párrafo segundo, de la Constitución Política de los Estados Unidos Mexicanos; 30, fracciones II, IV, V, VII, VIII, 33 y 84, fracciones I y V, de la LGPDPPSO; 47, 49, 51, 52 y 63 de los Lineamientos de Datos Personales; 89, fracción XVI y 90, fracción IV, del Estatuto Orgánico del IFT; Al respecto, el presente Programa fue aprobado por el Comité en su Décima Sesión Ordinaria, celebrada el 13 de abril de 2023, mediante Acuerdo número 10/SO/08/23.

El Programa de Protección de Datos Personales del Instituto Federal de Telecomunicaciones 2023-2024 fue refrendado por el Comité de Transparencia el día 25 de enero de 2024, en el marco de su Tercera Sesión Ordinaria de 2024, mediante Acuerdo 03/SO/22/24, a fin de que el presente documento sea considerado en la evaluación vinculante del ejercicio 2023, que realizará el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.

I. Glosario de términos comunes

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

Bases de datos: Conjunto ordenado de datos personales 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.

Cómputo en la nube: Modelo de provisión externa de servicios de cómputo bajo demanda, que implica el suministro de infraestructura, plataforma o programa informático, distribuido de modo flexible, mediante procedimientos virtuales, en recursos compartidos dinámicamente.

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

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 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.

DGTIC: Dirección General de Tecnologías de la Información y Comunicaciones.

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.

INAI: Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.

Instituto o IFT: Instituto Federal de Telecomunicaciones, en su calidad de responsable del tratamiento de los datos personales que se encuentran en su posesión.

LGPDPPSO: 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.

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

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.

Persona titular: La persona física a quien corresponden los datos personales.

Programa: Programa de Protección de Datos Personales del Instituto Federal de Telecomunicaciones.

Sistema de Gestión: El Sistema de Gestión de Seguridad de Datos Personales que, de conformidad con el artículo 34 de la LGPDPPSO, es un conjunto de

elementos y actividades interrelacionadas para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el tratamiento y seguridad de los datos personales, así como el cumplimiento de los principios, deberes y obligaciones previstos en dicha ley y las demás disposiciones que resulten aplicables en la materia.

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.

II. Presentación

El Programa se elabora con fundamento en los artículos 30, fracciones I y II de la LGPDPPSO, y 47 de los Lineamientos Generales, que establecen que entre las acciones que deberán realizar los responsables del tratamiento de datos personales para cumplir con el principio de responsabilidad, está la elaboración de políticas y **programas de protección de datos personales**, obligatorios y exigibles al interior de la organización del responsable, así como destinar los recursos necesarios para la implementación de dichos programas y políticas.

El Programa sienta las bases para el establecimiento de un Sistema de Gestión que permite proveer los elementos y actividades de dirección, operación y control de los procesos de la organización, para proteger de manera sistemática y continua los datos personales que estén en su posesión.

El Sistema de Gestión desarrolla las siguientes cuatro fases: (1) Planificar, (2) Hacer, (3) Verificar y (4) Actuar, identificado con las siglas PHVA, de acuerdo con lo descrito en la tabla siguiente:

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

Asimismo, cabe señalar que el Sistema de Gestión es el mismo que ha sugerido el INAI en los *Parámetros de Autorregulación en materia de*

Protección de Datos Personales[1], en las *Recomendaciones en materia de Seguridad de Datos Personales*[2], publicadas en el Diario Oficial de la Federación el 30 de octubre de 2013, y en la *Guía para implementar un Sistema de Gestión de Seguridad de Datos Personales*[3] que, si bien no aplican a los sujetos obligados del sector público, mantiene congruencia con la postura técnica del INAI en el tema.

III. Objetivos del Programa

1. Proveer el marco de trabajo necesario para la protección de los datos personales en posesión del IFT durante el periodo 2023 - 2024;

2. Permitir el seguimiento al cumplimiento de las obligaciones que establece la LGPDPPSO y los Lineamientos Generales, así como la normatividad que derive de los mismos;

3. Establecer los elementos y actividades de dirección, operación y control de los procesos que impliquen el tratamiento de datos personales, a efecto de protegerlos de manera sistemática y continua, y

4. Promover la adopción de mejores prácticas en la protección de datos personales, de manera preferente una vez que el programa se haya implementado de manera integral en el IFT, o bien, cuando se estime pertinente la implementación de buenas prácticas en tratamientos de datos personales específicos.

IV. Responsabilidades del Comité de Transparencia dentro del Programa

Con fundamento en lo dispuesto por los artículos 83 y 84, fracción I de la LGPDPPSO y 47, segundo párrafo, así como 48 de los Lineamientos Generales, que señalan que el Comité de Transparencia (Comité), es la autoridad máxima en materia de protección de datos personales y que tiene entre sus funciones la de coordinar, supervisar y realizar las acciones necesarias para garantizar el derecho a la protección de los datos personales en la organización del responsable, dicho órgano colegiado tendrá las siguientes funciones con relación a este Programa:

---

[1] Disponible en: http://www.dof.gob.mx/nota_detalle.php?codigo=5346597&fecha=29/05/2014
[2] Disponible en: http://dof.gob.mx/nota_detalle.php?codigo=5320179&fecha=30/10/2013
[3] Disponible en: https://home.inai.org.mx/wp-content/documentos/DocumentosSectorPrivado/Gu%C3%ADa_Implementaci%C3%B3n_SGSDP(Junio2015).pdf

I. Aprobar, coordinar y supervisar el Programa, en conjunto con las Áreas que estime necesario involucrar o consultar;

II. Proponer cambios y mejoras al Programa, a partir de la experiencia de su implementación;

III. Dar a conocer el Programa al interior del IFT;

IV. Coordinar la implementación del Programa en el IFT;

V. Asesorar a las Áreas del IFT en la implementación de este Programa, con el apoyo de la Unidad de Transparencia y la DGTIC;

VI. Presentar un informe anual al Comisionado Presidente en el que se describan las acciones realizadas para cumplir con lo dispuesto por este Programa;

VII. Supervisar la correcta implementación del Programa;

VIII. Aprobar, coordinar y supervisar el programa anual de capacitación, en conjunto con las áreas técnicas que estime necesario involucrar o consultar, y

IX. Las demás que de manera expresa señale el propio Programa.

El informe al que refiere la fracción VI anterior, deberá presentarse en las primeras dos semanas del mes de marzo de cada año y referirá al año inmediato anterior. Algunos de los elementos que pueden incluirse en el informe son:

- Estadística e información general sobre el cumplimiento de las obligaciones señaladas en el Programa por parte de Áreas del Instituto;

- Acciones realizadas por el Comité y la Unidad de Transparencia para cumplir con los objetivos que establece el Programa, y

- En su caso, los resultados de las revisiones y/o auditorias que se realicen en la materia.

Adicionalmente, con fundamento en el artículo 90, fracción IV, del Estatuto Orgánico del Instituto Federal de Telecomunicaciones (Estatuto), al Comité le corresponde, entre otras, la atribución de:

> *"**IV.** Aprobar, coordinar y supervisar, de conformidad con la normatividad aplicable, las políticas y programas de protección de datos personales obligatorios y exigibles al interior del Instituto, y"*

Las atribuciones anteriores se refieren sin perjuicio de las expresamente conferidas para el Comité, en términos del artículo 84 de la LGPDPPSO.

V. Responsabilidades de la Unidad de Transparencia dentro del Programa

Por su parte, en términos del artículo 89, fracción XVI, del Estatuto, a la Unidad de Transparencia le compete, entre otras, la atribución siguiente:

> (…)
>
> ***XVI.** Elaborar y proponer al Comité de Transparencia las políticas y programas de protección de datos personales obligatorios y exigibles al interior del Instituto, así como fungir dentro del mismo como órgano de consulta en la materia, y*
>
> (…)

Adicionalmente, la Unidad de Transparencia apoyará al Comité, para asesorar a las Áreas del IFT en la implementación de este Programa, con el apoyo de la DGTIC en lo que resulte aplicable.

Las atribuciones anteriores se refieren sin perjuicio de las expresamente conferidas para la Unidad de Transparencia, en términos del artículo 85 de la LGPDPPSO.

VI. Alcance del Programa

El Programa será aplicable a todas las Áreas del IFT que realicen tratamiento de datos personales en ejercicio de sus atribuciones, y a todos los tratamientos de datos personales que éstas efectúen en ejercicio de sus atribuciones. Las Áreas que forman parte del IFT, que deberán observar el Programa son las siguientes:

1. Secretaría Técnica del Pleno;
2. Coordinación Ejecutiva;
3. Unidad de Política Regulatoria;

4. Unidad de Espectro Radioeléctrico;

5. Unidad de Concesiones y Servicios;

6. Unidad de Medios y Contenidos Audiovisuales;

7. Unidad de Cumplimiento;

8. Unidad de Competencia Económica;

9. Unidad de Asuntos Jurídicos;

10. Unidad de Administración (UADM);

11. Autoridad Investigadora;

12. Centro de Estudios;

13. Coordinación General de Asuntos Internacionales;

14. Coordinación General de Política del Usuario;

15. Coordinación General de Planeación Estratégica;

16. Coordinación General de Mejora Regulatoria;

17. Coordinación General de Vinculación Institucional;

18. Coordinación General de Comunicación Social, y

19. Órgano Interno de Control.

VII. Gestión de los Datos Personales

El tratamiento de datos personales que realicen las Áreas del IFT deberá cumplir con los principios, deberes y obligaciones que prevé la LGPDPPSO, con independencia del formato, plataforma o infraestructura tecnológica en que se encuentren, la forma, lugar o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento, organización o tecnología empleada para su tratamiento, para lo cual este Programa establecerá el marco de trabajo mínimo que se deberá seguir para alcanzar dicho objetivo.

El Programa es obligatorio y exigible para todas las personas servidoras públicas del Instituto, personas prestadoras de servicios por honorarios, personas prestadoras de servicio social y/o prácticas profesionales, y personas físicas o morales que actúen como prestadoras de servicios del Instituto, sea que se trate de encargados o no, en lo referente a la protección de datos personales, en el tramo de responsabilidad que les corresponda de conformidad con las funciones y obligaciones previstas en el Estatuto, en los Manuales de Organización Específicos de cada una de las Unidades Administrativas del Instituto, Contratos, Convenios y/o cualquier otro instrumento jurídico que resulte aplicable para delimitar y acreditar la existencia, alcance y contenido de sus obligaciones, en materia de protección de datos personales.

En caso de que el encargado o encargados del IFT no se encuentren establecidos en territorio mexicano, las Áreas del Instituto deberán verificar que el encargado cuenta con medidas suficientes para garantizar el cumplimiento de los principios, deberes y/o derechos de protección de datos personales, de manera adecuada, conforme, equiparable o superior al nivel previsto en la LGPDPPSO, los Lineamientos Generales y demás normativa derivada y aplicable.

El Programa es complementario a la **"Política Interna de Gestión y Tratamiento de Datos Personales del Instituto Federal de Telecomunicaciones"**, aprobada por el Comité en su Vigésima Novena Sesión Extraordinaria de fecha 16 de diciembre de 2022, y al **"Documento de Seguridad"**, cuya última actualización fue aprobada por el Comité en la Décima Primera Sesión Extraordinaria, de fecha 25 de abril de 2022, mediante el Acuerdo 11/SE/03/22.[4]

Para ello, se identificarán las obligaciones que se deberán cumplir en todos los tratamientos de datos personales que realicen las Áreas del Instituto, de acuerdo con lo que establece la LGPDPPSO y los Lineamientos Generales, y según el Ciclo de vida de los datos personales. Asimismo, el presente documento prevé mejores prácticas para la protección de datos personales, en aquellos tratamientos que así lo permitan y según el nivel de madurez que exista.

En la elaboración del Programa, se consideran como Líneas Estratégicas las siguientes:

[4] La Política y la versión publicable del Documento de Seguridad se encuentran disponibles en el Apartado Virtual de Protección de Datos Personales del IFT, ingresando al vínculo electrónico siguiente:
https://www.ift.org.mx/proteccion_de_datos_personales/informacion_relevante/variable-y-formato-21-deber-de-seguridad

A. Identificación y categorización de datos personales.

B. Documentación de roles y responsabilidades en el tratamiento de datos personales.

C. Identificación de riesgos y fortalecimiento de medidas y controles de seguridad existentes.

D. Respuesta a incidentes de seguridad.

E. Sensibilización y capacitación.

F. Monitoreo y revisión.

A continuación, se da cuenta de cada una de las líneas estratégicas, con sus respectivas obligaciones y recomendaciones.

A. Identificación y categorización de datos personales

La identificación de los datos personales que se encuentran en posesión del IFT es la base para su protección y resguardo. El "Inventario de datos personales en posesión del Instituto Federal de Telecomunicaciones" (Inventario), fue aprobado por el Comité de Transparencia, en la Décima Séptima Sesión Extraordinaria, de fecha 28 de junio de 2019, como un anexo al Documento de Seguridad del IFT, en términos de lo dispuesto por el artículo 35, fracción I, de la LGPDPPSO. El Inventario reúne y da cuenta de los datos personales, sistemas de tratamiento y demás elementos requeridos por los artículos 33, fracción III, 35, fracción I, de la LGPDPPSO y 58 de los Lineamientos Generales.

Para el periodo que comprendía el ciclo **2021-2022** se programó la actualización integral del Inventario y la documentación del Ciclo de vida de los datos asociados, las cuales se llevaron a cabo durante el año 2021. La actualización de los Inventarios y la documentación de los Ciclos de vida, se tuvo por presentada ante el Comité de Transparencia el 02 de julio de 2021, en la Décima Segunda Sesión Extraordinaria, mediante el Acuerdo 12/SE/16/21.

Respecto al periodo que comprende el ciclo **2023-2024**, se tiene igualmente programada la actualización de los Inventarios y el Ciclo de Vida de los datos personales que se encuentran en posesión de las Áreas del IFT. Para tal efecto, se proponen las actividades siguientes:

Actividades para su cumplimiento	Áreas responsables del cumplimiento
• Verificar y actualizar las facultades o atribuciones para efectuar el tratamiento de los datos personales, en términos de lo dispuesto por el artículo 17 de la LGPDPPSO.[5] • Actualizar el catálogo de los medios físicos y/o electrónicos a través de los cuales se obtienen los datos personales; • Verificar y actualizar las finalidades de cada tratamiento de datos personales; • Determinar la procedencia del consentimiento como base jurídica para efectuar el tratamiento de los datos, o bien, alguna de las excepciones a su obtención, de conformidad con lo establecido en los artículos 22 y 70 de la LGPDPPSO. • Actualizar el catálogo de los tipos de datos personales que se traten, indicando si son sensibles o no; • Actualizar el catálogo de los formatos o soportes de almacenamiento, así como la descripción general de la ubicación física y/o electrónica de los datos personales; • Actualizar y validar la lista de personas servidoras públicas que tienen acceso a los sistemas de tratamiento; • Actualizar el nombre completo o denominación o razón social del encargado y el instrumento jurídico que	Todas las Áreas del Instituto que realicen tratamiento de datos personales.

[5] **Artículo 17.** El tratamiento de datos personales por parte del responsable deberá sujetarse a las facultades o atribuciones que la normatividad aplicable le confiera.

formaliza la prestación de los servicios que brinda al IFT, en su carácter de responsable; • Validar y actualizar la información relativa a los destinatarios o terceros receptores de las transferencias que se efectúen, así como las finalidades que justifican éstas, y • Revisar y actualizar cada uno de los elementos del Ciclo de vida de los datos personales en posesión de las Áreas del IFT, de manera enunciativa, los relativos a la obtención, registro, almacenamiento, organización, uso, utilización, aprovechamiento, manejo, acceso, elaboración, posesión, conservación, comunicación, difusión, divulgación, transferencia, disposición, destrucción, supresión y eliminación; así como las personas o Áreas intervinientes, y si el tratamiento se lleva a cabo a través de medios automatizados (electrónicos o digitales) o no automatizados (manuales).	

Medios que facilitan la acreditación del cumplimiento
• Ciclo de vida de los datos personales. • Mapeo de procesos de tratamiento de datos personales. • Inventario de datos personales.

Nota: En este apartado se incluyen de manera enunciativa (no exhaustiva) algunas de las categorías de datos que comúnmente son considerados personales, las cuales podrían encontrarse en posesión de las Áreas del IFT. La referencia a las categorías no tiene como finalidad pronunciarse respecto a su carácter confidencial o público, siendo únicamente una guía útil para determinar cuándo se está en presencia de datos personales, concernientes a personas físicas identificadas o identificables.

Datos personales:

- **Datos de identificación.** Información concerniente a una persona física que permite diferenciarla de otras en una colectividad, tales como: nombre; estado civil; firma autógrafa y electrónica; Registro Federal de Contribuyentes (RFC); Clave Única de Registro de Población (CURP); número de cartilla militar; lugar y fecha de nacimiento; nacionalidad; fotografía; edad, entre otros.

- **Datos de contacto.** Información que permite mantener o entrar en contacto con su titular, tal como: domicilio; correo electrónico; teléfono fijo; teléfono celular, entre otra.

- **Datos laborales.** Información concerniente a una persona física relativa a su empleo, cargo o comisión; desempeño laboral y experiencia profesional, generada a partir de procesos de reclutamiento, selección, contratación, nombramiento, evaluación y capacitación, tales como: puesto, domicilio de trabajo, correo electrónico institucional, teléfono institucional; referencias laborales; fecha de ingreso y salida del empleo, entre otros.

- **Datos sobre características físicas.** Información sobre una persona física relativa a su fisonomía, anatomía, rasgos o particularidades específicas, como: color de la piel, del iris o del cabello; señas particulares; estatura; peso; complexión; cicatrices, tipo de sangre, entre otras.

- **Datos académicos.** Información concerniente a una persona física que describe su preparación, aptitudes, desarrollo y orientación profesional o técnica, avalada por instituciones educativas, como lo son: trayectoria educativa; títulos; cédula profesional; certificados; reconocimientos; entre otros.

- **Datos patrimoniales o financieros.** Información concerniente a una persona física relativa a sus bienes, derechos, cargas u obligaciones susceptibles de valoración económica, como pueden ser: bienes muebles e inmuebles; información fiscal; historial crediticio; ingresos y egresos; cuentas bancarias; seguros; afores; fianzas, número de tarjeta de crédito, número de seguridad, entre otros.

- **Datos biométricos.** Información sobre una persona física relativa a imagen del iris, huella dactilar, palma de la mano u otros análogos.

Datos personales sensibles:

- **Datos ideológicos.** Información sobre las posturas ideológicas, religiosas, filosóficas o morales de una persona.

- **Datos sobre opiniones políticas.** Opinión de una persona con relación a un hecho político o sobre su postura política en general.

- **Datos sobre afiliación sindical.** Pertenencia de una persona a un sindicato y la información que de ello derive.

- **Datos de salud.** Información concerniente a una persona física relacionada con la valoración, preservación, cuidado, mejoramiento y recuperación de su estado de salud físico o mental, presente, pasado o futuro, así como información genética.

- **Datos sobre vida sexual.** Información de una persona física relacionada con su comportamiento, preferencias, prácticas o hábitos sexuales, entre otros.

Datos de origen étnico o racial. Información concerniente a una persona física relativa a su pertenencia a un pueblo, etnia o región que la distingue por sus condiciones e identidades sociales, culturales y económicas, así como por sus costumbres, tradiciones, creencias.

B. Roles y Responsabilidades en el tratamiento de datos personales

1. Principios del tratamiento

El tratamiento de los datos personales que se encuentren en posesión de las Áreas del IFT, deberá realizarse observando los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad, así como los deberes de seguridad y confidencialidad, conforme al ciclo de vida siguiente:

Fase	Principios y deberes	Tipo de tratamiento
Obtención	Licitud Información Consentimiento Proporcionalidad Seguridad Confidencialidad	• Registro • Organización • Conservación • Elaboración • Utilización • Comunicación • Difusión

Fase	Principios y deberes	Tipo de tratamiento
Uso	Calidad Finalidad Lealtad Seguridad Confidencialidad	• Almacenamiento • Posesión • Acceso • Manejo • Aprovechamiento • Divulgación • Transferencia • Disposición
Eliminación	Calidad Seguridad	

a) Principio de Licitud

En términos de lo dispuesto en los artículos 17 de la LGPDPPSO y 8 de los Lineamientos Generales, las personas servidoras públicas del IFT deberán llevar a cabo el tratamiento de los datos personales conforme a las disposiciones de la LGPDPPSO, los Lineamientos Generales, la legislación mexicana especifica o sectorial que resulte aplicable y, en su caso, el derecho internacional, respetando en todo momento los derechos y libertades de los titulares. Para el cumplimiento del principio de licitud, se considera adecuado tener en cuenta las acciones siguientes:

Actividades para su cumplimiento	Áreas responsables del cumplimiento
• Identificar y conocer los principios y deberes del tratamiento de datos personales, así como los derechos de las personas titulares, contenidos en la normativa mexicana en materia de protección de datos personales. • Identificar y conocer la normativa expresa o específica que regule el tratamiento de datos personales en los trámites, procesos o procedimientos realizados por las Áreas del IFT. • Llevar a cabo el tratamiento de datos personales con estricto apego a la legislación sectorial que, en lo particular, regule de manera directa o indirecta, la actividad en la que se tratan los datos personales.	Todas las Áreas del Instituto que lleven a cabo tratamiento de datos personales.

• Identificar si existen disposiciones de derecho internacional que regulen un determinado tratamiento de datos personales (por ejemplo, Convenios o Tratados Internacionales suscritos y ratificados por México).	

Medios que facilitan la acreditación del cumplimiento
Marco normativo aplicable al tratamiento de datos personales respectivo.

Comprobación:

	Sí	No
1. Están identificadas las disposiciones normativas (ley, acuerdos o tratados internacionales, reglamentos, lineamientos, entre otros, con sus respectivos artículos), que facultan al Área para tratar los datos personales para cada una de las finalidades que lleva a cabo, y aquél que regula el tratamiento respectivo.	☐	☐
2. Las disposiciones normativas son expresas o específicas para habilitar el tratamiento de los datos personales que corresponda.	☐	☐

b) Principio de Lealtad

Con fundamento en los artículos 19 de la LGPDPPSO y 11 de los Lineamientos Generales, las personas servidoras públicas del IFT no deberán obtener ni tratar los datos personales a través de medios **engañosos** o **fraudulentos**. De acuerdo con el artículo 11, fracción I, de los Lineamientos Generales, se entiende por medios engañosos y fraudulentos aquéllos que se utilicen para tratar los datos personales con **dolo**, **mala fe** o **negligencia**.

Asimismo, en el tratamiento de los datos personales, las personas servidoras públicas deberán privilegiar los **intereses** y la **expectativa razonable de privacidad de los titulares**.

En términos del artículo 11, fracción II, de los Lineamientos Generales, se entenderá que el sujeto obligado privilegia los **intereses** de la persona titular cuando el tratamiento de datos personales no da lugar a discriminación, trato injusto o arbitrario en contra de la persona titular.

Por su parte, de conformidad con el artículo 11, fracción III, de los Lineamientos Generales, se entiende por **expectativa razonable de privacidad**, la confianza que la persona titular ha depositado en el sujeto obligado respecto a que sus datos personales serán tratados conforme a lo señalado en el Aviso de Privacidad y en cumplimiento a las disposiciones previstas en la LGPDPPSO y los Lineamientos Generales.

Para el cumplimiento del principio de lealtad, se considera adecuado llevar a cabo las acciones siguientes:

Actividades para su cumplimiento	Áreas responsables del cumplimiento
• Verificar que los datos personales no se obtengan con dolo, mala fe o negligencia. • Verificar los tratamientos que se llevan a cabo, a fin de confirmar que los mismos no den lugar a discriminación, trato injusto o arbitrario en contra de la persona titular. • Tratar los datos personales conforme a lo señalado en el Aviso de Privacidad y las disposiciones jurídicas que resulten aplicables al tratamiento correspondiente.	Todas las Áreas del Instituto que lleven a cabo tratamiento de datos personales.

Medios que facilitan la acreditación del cumplimiento
• Avisos de Privacidad actualizados. • Documentación que se genere durante el tratamiento, que permita acreditar que los datos personales se utilizaron conforme a lo dispuesto en la legislación aplicable y según lo señalado en el Aviso de Privacidad. • En su caso, resultado de las auditorías o procedimientos de revisión efectuados.

Comprobación:

	Sí	No
1. Se ha verificado que en todos los tratamientos que realiza el IFT no se obtienen los datos personales con dolo, mala fe o negligencia.	☐	☐

2. Los Avisos de Privacidad cuentan con todos los elementos informativos que establece la LGPDPPSO.	☐	☐
3. En los Avisos de Privacidad se incluyen todas las finalidades del tratamiento.	☐	☐
4. Los datos personales solo se utilizan para las finalidades previstas en el Aviso de Privacidad.	☐	☐
5. Se ha verificado que todos los tratamientos que realiza el IFT no dan lugar a discriminación o trato injusto o arbitrario en contra de la persona titular.	☐	☐

c) Principio de Información

De conformidad con lo dispuesto en los artículos 3, fracción II, 26, 27 y 28 de la LGPDPPSO, y 26 a 45 de los Lineamientos Generales, el personal del IFT deberá Informar al titular, a través del Aviso de Privacidad, la existencia y características principales del tratamiento al que serán sometidos sus datos personales, por regla general, de manera previa al tratamiento de los mismos, a fin de que pueda tomar decisiones informadas al respecto.

Cuando resulte imposible dar a conocer al titular el Aviso de Privacidad simplificado de manera directa, o ello exija esfuerzos desproporcionados, de acuerdo con los *Criterios Generales para la instrumentación de medidas compensatorias en el sector público del orden federal, estatal y municipal*,[6] deberán instrumentarse las **medidas compensatorias** correspondientes.

En la elaboración y actualización de los Avisos de Privacidad correspondientes a los procesos a cargo de las Áreas del IFT, según corresponda, deberán emplearse los formatos (modelos), de Avisos de Privacidad en sus modalidades "Integral" y "Simplificado", aprobados por el Comité el 21 de noviembre de 2019, en la Décimo Novena Sesión Ordinaria, los cuales se anexan para pronta referencia en la parte final del Programa.

Medios que facilitan la acreditación del cumplimiento
• Avisos de Privacidad en sus dos modalidades: simplificado e integral. • Avisos de Privacidad ubicados en sitios de fácil acceso, redactados en forma clara y con un lenguaje sencillo, que hagan posible su consulta práctica por parte de la persona titular. • Procedimientos para la puesta a disposición de los Avisos de Privacidad.

[6] Disponibles en el vínculo electrónico: http://www.dof.gob.mx/nota_detalle.php?codigo=5511114&fecha=23/01/2018

- En caso de la instrumentación de medidas compensatorias, autorización del INAI y evidencia de la difusión del Aviso de Privacidad correspondiente a través del medio de comunicación masiva utilizado para la medida compensatoria implementada.

Comprobación:

	Sí	No
1. Se tienen identificados todos los Avisos de Privacidad que se requieren según los tratamientos que realizan las Áreas del IFT.	☐	☐
2. Los Avisos de Privacidad están redactados en sus dos modalidades: simplificado e integral.	☐	☐
3. Los Avisos de Privacidad contienen todos los elementos informativos que exige la LGPDPPSO y los Lineamientos Generales.	☐	☐
4. Los Avisos de Privacidad están redactados de manera clara y sencilla, según las características y conforme a los formatos aprobados por el Comité.	☐	☐
5. Los Avisos de Privacidad se ponen a disposición de las personas titulares en el momento en que señala la norma (por regla general, de manera previa al tratamiento de los datos personales).	☐	☐
6. Los Avisos de Privacidad simplificados e integrales se difunden en el Apartado Virtual de Protección de Datos Personales[7] del IFT y están disponibles de manera impresa en las instalaciones del Área correspondiente.	☐	☐
7. Los Avisos de Privacidad están colocados en un lugar visible y de fácil consulta por parte de los titulares.	☐	☐
8. Los Avisos de Privacidad integrales están publicados en los sitios que señalan los correspondientes Avisos de Privacidad simplificados.	☐	☐

[7] Los Avisos de Privacidad del IFT se encuentran publicados en la sección siguiente: https://www.ift.org.mx/proteccion_de_datos_personales/avisos_de_privacidad

9. Los mecanismos que se ofrecen para que la persona titular pueda manifestar su negativa para el tratamiento de sus datos personales, para las finalidades y transferencias que requieran su consentimiento, permiten que dicha manifestación pueda ocurrir previo al tratamiento.	☐	☐
10. En caso de requerirse, se puso a disposición de los titulares el nuevo Aviso de Privacidad.	☐	☐
11. Los Avisos de Privacidad se actualizan de manera periódica (idealmente cada 6 meses y, cuando menos, una vez por año).	☐	☐

Para el caso de la instrumentación de medidas compensatorias:

	Sí	No
1. Se tienen identificados los casos en los que se requiere la implementación de medidas compensatorias.	☐	☐
2. Se han implementado las medidas compensatorias en esos casos.	☐	☐
3. Se ha revisado que en dichos casos haya sido imposible dar a conocer el Aviso de Privacidad de manera directa a la persona titular o ello exija esfuerzos desproporcionados.	☐	☐
4. Se ha evaluado si se requiere o no la autorización expresa del INAI.	☐	☐
5. Se ha revisado que se cumple con los requisitos de los Criterios Generales para la instrumentación de medidas compensatorias en el sector público del orden federal, estatal y municipal.[8]	☐	☐

d) Principio del Consentimiento

En términos de los artículos 7, 20, 21 y 22 de la LGPDPPSO, así como 12 al 20 y 53 de los Lineamientos Generales, las personas servidoras públicas del IFT deberán obtener el consentimiento de la persona titular de manera previa

[8] Disponibles en el vínculo electrónico: https://dof.gob.mx/nota_detalle.php?codigo=5511114&fecha=23/01/2018

al tratamiento de sus datos personales, salvo que se actualice alguna de las excepciones previstas en el artículo 22 de la LGPDPPSO.

Conforme a lo dispuesto por el artículo 20 de la LGPDPPSO, cuando resulte procedente la obtención del consentimiento, éste deberá obtenerse de manera:

- **Libre:** Sin que medie error, mala fe, violencia o dolo que puedan afectar la manifestación de voluntad de la persona titular.

- **Específica:** El consentimiento deberá obtenerse para finalidades concretas, lícitas, explícitas y legítimas que justifiquen el tratamiento.

- **Informada:** Que la persona titular tenga conocimiento del Aviso de Privacidad previo al tratamiento a que serán sometidos sus datos personales.

Actividades para su cumplimiento	Áreas responsables del cumplimiento
• Identificar si el consentimiento de la persona titular es la base jurídica que habilita el tratamiento de datos personales, o bien, si el tratamiento de los datos tiene como fundamento alguna de las excepciones establecidas en los artículos 22 y/o 70 de la LGPDPPSO. • No tratar datos personales sensibles, salvo que se cuente con el consentimiento expreso de la persona titular o se actualice alguna de las excepciones establecidas en los artículos 22 y/o 70 de la LGPDPPSO. • En función del tipo de datos personales recabados, el consentimiento deberá ser tácito o expreso, siguiendo las reglas establecidas en el artículo 21 de la LGPDPPPSO. • Cuando los datos personales se recaben **directamente** de la persona titular, y se requiera el consentimiento, éste deberá	Todas las Áreas del Instituto que lleven a cabo tratamiento de datos personales.

solicitarse previo a la obtención de los datos personales y después de la puesta a disposición del Aviso de Privacidad. Se entenderá que el responsable obtiene los datos personales directamente de la persona titular cuando es ésta quien los proporciona o la persona que lo representa, personalmente o por algún medio que permita su entrega directa como podrían ser medios electrónicos, ópticos, sonoros, visuales, vía telefónica, Internet o cualquier otra tecnología y/o medio. • Cuando los datos personales **se obtengan de manera indirecta** de la persona titular, y no se actualice alguna de las excepciones para la obtención del consentimiento, los datos personales no podrán ser tratados hasta que se cuente con la manifestación libre, específica e informada de la persona titular, mediante la que autorice el tratamiento de sus datos personales de manera tácita o expresa, según corresponda. • De conformidad con el segundo y tercer párrafos del artículo 15 de los Lineamientos Generales, la persona titular tendrá un plazo de cinco días, contados a partir del día siguiente de recibir el Aviso de Privacidad por parte del responsable, para que, en su caso, manifieste su negativa al tratamiento de sus datos personales a través de los medios establecidos por el responsable. En caso de que la persona titular no manifieste su negativa en el plazo antes señalado, se entenderá que ha otorgado su consentimiento tácito para el	

tratamiento de sus datos personales, salvo prueba en contrario. • Atender las solicitudes de revocación del consentimiento, mismas que podrán ser presentadas por la persona titular en cualquier momento del tratamiento sin que se le atribuyan efectos retroactivos, a través del ejercicio de los derechos de oposición y cancelación. El consentimiento únicamente podrá ser revocado cuando éste constituya la base jurídica sobre la cual se efectúa el tratamiento de los datos personales.	

Medios que facilitan la acreditación del cumplimiento
• Procedimiento implementado por el Área para la solicitud del consentimiento. • Procedimiento implementado por el Área para la puesta a disposición de los Avisos de Privacidad. • Texto de solicitud de consentimiento (por ejemplo, Carta para obtener el consentimiento). • En su caso, el consentimiento expreso otorgado por las personas titulares (prueba de su obtención).

Comprobación:

	Sí	No
1. Se ha corroborado que el consentimiento es, en efecto, la base jurídica del tratamiento de los datos personales (excluyendo, por ejemplo, un tratamiento obligatorio en ejercicio de atribuciones jurídicas o por mandato de ley).	☐	☐
2. Se han identificado las finalidades para las cuales se requiere el consentimiento.	☐	☐
3. Se ha definido el tipo de consentimiento que se requiere (expreso o tácito), según el tipo de datos personales que se tratan y tomando en cuenta las disposiciones normativas que regulan el tratamiento.	☐	☐

4. Se han habilitado los mecanismos para solicitar el consentimiento expreso, en su caso.	☐	☐
5. El consentimiento se requiere después de que se da a conocer el Aviso de Privacidad.	☐	☐
6. Se encuentra documentada la puesta a disposición del Aviso de Privacidad y la obtención del consentimiento expreso, en su caso.	☐	☐
7. Las solicitudes de consentimiento se encuentran redactadas de forma tal que éste sea libre, específico e informado, y de que las solicitudes sean concisas e inteligibles, estén en un lenguaje claro y sencillo acorde con el perfil de la persona titular, y se distingan de asuntos ajenos a la protección de datos personales, cuando ello sea necesario.	☐	☐
8. Cuando los datos personales se recaban directamente de la persona titular, el consentimiento se solicita previo a la obtención de los datos personales y después de la puesta a disposición del Aviso de Privacidad.	☐	☐
9. Cuando los datos personales se recaban de manera indirecta, (i) se envía el Aviso de Privacidad correspondiente a los titulares; (ii) se les informa sobre los 5 días hábiles que tienen para manifestar su negativa, y (iii) en caso de que se requiera el consentimiento expreso, éste se solicita y los datos personales se tratan solo si se cuenta con el consentimiento de la persona titular.	☐	☐
10. El procedimiento interno para la atención de los derechos ARCO contempla lo relativo a la revocación del consentimiento.	☐	☐

Comprobación respecto a la obtención del consentimiento para el tratamiento de datos personales sensibles:

	Sí	No
1. El tratamiento de los datos personales sensibles está debidamente justificado por las atribuciones del Área del IFT y la necesidad de su tratamiento.	☐	☐

2. Se tienen identificados los casos en los que se requiere el consentimiento expreso y por escrito de las personas titulares, o bien, las excepciones a su obtención.	☐	☐
3. Se obtiene el consentimiento expreso y por escrito de la persona titular.	☐	☐
4. Se ha verificado que el tratamiento no tenga como consecuencia discriminación para las personas titulares.	☐	☐

e) Principio de Proporcionalidad

De conformidad con lo dispuesto en los artículos 25 de la LGPDPPSO, así como 24 y 25 de los Lineamientos Generales, los datos personales deberán tratarse solo cuando resulten adecuados, relevantes y sean estrictamente necesarios para la finalidad que justifica su tratamiento.

Se entenderá que los datos personales son 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 a las Áreas del Instituto por la normatividad que le resulte aplicable.

El personal del IFT deberá realizar esfuerzos razonables para limitar la cantidad de los datos personales tratados, así como la temporalidad de su tratamiento, al mínimo necesario, con relación a las finalidades que motivaron su obtención y posterior tratamiento.

Para el cumplimiento del principio de proporcionalidad, se recomienda llevar a cabo las acciones siguientes:

Actividades para su cumplimiento	Áreas responsables del cumplimiento
• Identificar las finalidades de los procesos del tratamiento, derivadas de las atribuciones conferidas por la normatividad que resulte aplicable. • Identificar qué datos personales se requieren para el cumplimiento de cada una de las finalidades. • Recabar y tratar únicamente los datos personales que resulten estrictamente	Todas las Áreas del Instituto que recaben y lleven a cabo tratamiento de datos personales.

necesarios para el cumplimiento de las finalidades correspondientes. • Requerir el mínimo posible de datos personales (cantidad estrictamente necesaria de información) para el cumplimiento de las finalidades para las cuales se tratan, así como limitar al máximo la temporalidad del tratamiento de los datos (periodo de tratamiento). • En caso de contratación con terceros, revisar las Políticas de Privacidad y/o los Avisos de Privacidad aplicables, con el objeto de validar la previsión del cumplimiento de este principio.	

Medios que facilitan la acreditación del cumplimiento
• Inventario y Ciclo de vida de los datos personales. • Avisos de Privacidad que establezcan los datos estrictamente necesarios que serán objeto de tratamiento. • Normatividad que establezca, en su caso, los datos personales que deberán solicitarse para el tratamiento específico.

Comprobación:

	Sí	No
1. Se tienen identificados los datos personales que se requieren para cada una de las finalidades.	☐	☐
2. Los datos personales que se solicitan (cantidad) son los mínimos necesarios para cumplir con las finalidades.	☐	☐
3. El periodo de tratamiento (temporalidad) de los datos personales se limita al mínimo indispensable.	☐	☐

f) Principio de Finalidad

En términos de lo dispuesto por los artículos 18 de la LGPDPPSO, y 9 y 10 de los Lineamientos Generales, el tratamiento de los datos personales que efectúen las Áreas del IFT deberá llevarse a cabo conforme a finalidades concretas, lícitas, explícitas y legítimas, relacionadas con las atribuciones que la normatividad aplicable les confiera. En el cumplimiento del principio de finalidad, las Áreas del IFT deberán llevar a cabo las recomendaciones siguientes:

Actividades para su cumplimiento	Áreas responsables del cumplimiento
• Identificar el marco normativo (ley, reglamento, lineamientos, entre otros, con sus respectivos artículos), que otorga las atribuciones a las Áreas del Instituto para tratar los datos personales. • Verificar que la finalidad del tratamiento sea compatible con las atribuciones expresas conferidas a las Áreas del Instituto. • Identificar las finalidades de cada tratamiento que se realice, y verificar que las mismas correspondan a finalidades específicas o determinadas, que sean acordes a las atribuciones o facultades de las personas servidoras públicas del Instituto, en función del Área de que se trate. • Verificar que en los Avisos de Privacidad se informen todas las finalidades para las cuales se recaban y tratan los datos personales, y que éstas se describan de manera clara. • Llevar a cabo el tratamiento de los datos personales solo para los fines informados en el Aviso de Privacidad.	Todas las Áreas del Instituto que recaben y lleven a cabo tratamiento de datos personales.

• Identificar si existen finalidades que requieran del consentimiento de la persona titular y solicitarlo según las reglas establecidas en la LGPDPPSO y los Lineamientos Generales.	

Medios que facilitan la acreditación del cumplimiento
• Marco normativo que establezca las facultades o atribuciones a partir de las cuales se deriven finalidades del tratamiento (concretas, lícitas, explícitas y legítimas). • Avisos de privacidad que contengan las finalidades del tratamiento. • Inventario de tratamientos de datos personales y su Ciclo de vida. • Documentos que se generen conforme a las atribuciones correspondientes, en los que se señalen de manera expresa las finalidades del tratamiento conforme a atribuciones legalmente conferidas a las Áreas del Instituto.

Comprobación:

	Sí	No
1. Se tienen identificadas cada una de las finalidades de todos los tratamientos que realiza el Área del IFT.	☐	☐
2. Estas finalidades atienden a fines específicos o determinados, los cuales son acordes a las atribuciones o facultades expresas del IFT y el Área de que se trate, de tal forma que sean consideradas lícitas y legítimas.	☐	☐
3. Estas finalidades son informadas en los Avisos de Privacidad de manera clara y completa.	☐	☐
4. Se han identificado las finalidades que requieren el consentimiento y el mismo se ha solicitado, o bien, se ha determinado alguna de las excepciones para la obtención del consentimiento.	☐	☐
6. Se identifican de manera periódica nuevas finalidades del tratamiento de los datos, de tal manera que se informen sin dilación en el Aviso o Aviso de Privacidad correspondiente (actualización del Aviso de Privacidad por adición o cambio de finalidad).	☐	☐

7. En su caso, se ha verificado que existen atribuciones legales para llevar a cabo estas finalidades adicionales.	☐	☐
8. Se ha solicitado el consentimiento de los titulares para las finalidades adicionales, en caso de requerirse, o se ha identificado que se actualiza alguno de los supuestos previstos en los artículo 22 y/o 70 de la LGPDPPSO.	☐	☐
9. Se han definido e implementado las medidas que se requieran para cumplir con las obligaciones que establece la LGPDPPSO y los Lineamientos Generales, con relación a las finalidades adicionales.	☐	☐

g) Principio de Calidad

Exactitud, actualización y pertinencia de los datos personales

Según lo dispuesto por los artículos 23 y 24 de la LGPDPPSO, y 21, 22 y 23 de los Lineamientos Generales, los datos personales en posesión del Instituto deberán ser pertinentes, correctos y actualizados para los fines para los cuales fueron recabados.

Conservación de los datos personales

En términos del artículo 23, último párrafo, de la LGPDPPSO, el plazo de conservación de los datos personales no debe exceder el tiempo estrictamente necesario para llevar a cabo las finalidades que justificaron el tratamiento, ni aquél que se requiera para cumplir especialmente con:

- Las disposiciones legales establecidas en la Ley General de Archivos;
- Las disposiciones aplicables en la materia de que se trate, que establezcan condiciones generales o específicas para un determinado tratamiento de datos personales;
- Los aspectos administrativos, contables, fiscales, jurídicos e históricos de la información, y
- El periodo de bloqueo de los datos personales.

En particular, el artículo 24 la LGPDPPSO establece que se deben documentar los procedimientos para la conservación y, en su caso, bloqueo y supresión de los datos personales respecto de cada tratamiento que se efectúe por las Áreas del IFT.

Conclusión del plazo de conservación

Una vez concluido el plazo de conservación, y siempre que no exista disposición legal o reglamentaria que establezca lo contrario, deberá procederse a la supresión de los datos personales. El plazo de conservación debe incluir un periodo de bloqueo, ya que los datos personales deben ser bloqueados antes de que sean eliminados o suprimidos. En cuanto a los datos personales sensibles, las Áreas del Instituto deberán realizar esfuerzos razonables para limitar el periodo de conservación al mínimo indispensable.

Bloqueo de los datos personales

El bloqueo se define como la acción que tiene por objeto impedir el tratamiento de los datos personales para cualquier finalidad, con excepción de su almacenamiento y acceso para determinar posibles responsabilidades en relación con el tratamiento de los datos personales, hasta el plazo de prescripción correspondiente. Las personas servidoras públicas del IFT están obligadas a:

- Bloquear los datos personales antes de suprimirlos, y durante el periodo de bloqueo solo tratarlos para su almacenamiento y acceso en caso de que se requiera determinar posibles responsabilidades en relación con el tratamiento de los datos personales.

Supresión de los datos personales

En la cancelación, eliminación o supresión de los datos personales, las personas servidoras públicas del Instituto deberán emplear como referencia la *Guía de Borrado Seguro de Datos Personales*, emitida por el INAI, la cual se encuentra disponible en su portal de Internet,[9] de conformidad con las disposiciones previstas en la Ley General de Archivos, y las disposiciones específicas que se establezcan en el IFT por el Área Coordinadora de Archivos.

Para el cumplimiento del principio de calidad, podrán tenerse en cuenta las acciones siguientes:

[9] Disponible en el vínculo electrónico:
http://inicio.inai.org.mx/DocumentosdeInteres/Guia_Borrado_Seguro_DP.pdf

Actividades para su cumplimiento	Áreas responsables del cumplimiento
• Establecer los plazos de conservación de los datos personales, para cada uno de los tratamientos, lo cual deberá ser congruente con los plazos de conservación establecidos en los instrumentos de clasificación archivística.	Todas las Áreas que realicen tratamiento de datos personales con el apoyo del Área Coordinadora de Archivos del Instituto, la Unidad de Transparencia, la DGTIC y el Comité de Transparencia.
• Establecer políticas, procedimientos, métodos y técnicas orientadas a la supresión definitiva de los datos personales, considerando los atributos de irreversibilidad; seguridad y confidencialidad.	

Medios que facilitan la acreditación del cumplimiento
• Bases de datos en formato físico o electrónico con información correcta y actualizada. • Existencia de controles o registros en donde consten las actualizaciones realizadas, en aquellos casos en que las mismas hayan resultado procedentes. • Documento que contenga el establecimiento o identificación de los plazos de conservación de los datos personales.

Comprobación:

	Sí	No
1. Se cuenta con medidas para mantener actualizados, corregir o completar los datos personales que están en posesión del IFT.	☐	☐
2. Se tienen establecidos los plazos de conservación de los datos personales por cada tratamiento.	☐	☐

3. Los plazos de conservación son congruentes con los establecidos en los instrumentos de archivo.	☐	☐
4. Se cuenta con procedimientos para la conservación y supresión de los datos personales y éstos se encuentran documentados.	☐	☐

h) Principio de Responsabilidad

Con fundamento en los artículos 29 y 30 de la LGPDPPSO y 46 al 54 de los Lineamientos Generales, las Áreas del Instituto deberán velar por el cumplimiento de todos los principios del tratamiento, adoptar las medidas necesarias para su aplicación, y demostrar ante los titulares y el INAI, según corresponda, que cumplen con sus obligaciones en materia de protección de datos personales. Para el cumplimiento del principio de responsabilidad, se tiene en cuenta especialmente las siguientes acciones:

Actividades para su cumplimiento	Áreas responsables del cumplimiento
• Mantener actualizadas las políticas y programas de datos personales y seguridad de la información para determinar las modificaciones que se requieran. • Revisar y fortalecer el sistema de supervisión y vigilancia interna y/o externa, incluyendo auditorías, para comprobar el cumplimiento de las políticas de protección de datos personales. • Incluir cursos y temas, inclusive adicionales al programa de capacitación y actualización del personal del Instituto sobre las obligaciones y demás deberes en materia de protección de datos personales.	Comité de Transparencia, de manera conjunta y coordinada con las Áreas del Instituto que tengan incidencia en la implementación de las acciones, mecanismos o controles específicos.

Medios que facilitan la acreditación del cumplimiento
• Políticas y/o programas de protección de datos personales, y de seguridad de la información, actualizados.

- Acciones de supervisión y vigilancia (incluyendo las efectuadas por el Grupo de Trabajo de Protección de Datos Personales).
- Programa de capacitación para servidores públicos del Instituto.

Comprobación:

	Sí	No
1. El presupuesto del IFT contempla los recursos necesarios para la instrumentación de Políticas y Programas de protección de datos personales.	☐	☐
2. Las Áreas conocen y aplican lo dispuesto en la Política o Programa de protección de datos personales al interior del IFT.	☐	☐
3. Se tiene y aplica un programa de capacitación y actualización de las personas servidoras públicas del IFT en materia de protección de datos personales según lo establecido en este Programa.	☐	☐
4. Se tiene y aplica un procedimiento y programa de supervisión y vigilancia y/o externa para comprobar el cumplimiento de este programa, incluyendo las medidas de seguridad, cada dos años o antes si es necesario.	☐	☐
5. Se tiene y aplica un procedimiento para atender dudas y quejas de los titulares.	☐	☐
6. Las políticas públicas, programas, servicios, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología, que implique el tratamiento de datos personales, se diseñan, desarrollan e implementan tomando en cuenta la privacidad por diseño y por defecto.	☐	☐
7. Se genera evidencia para acreditar el cumplimiento de los principios, deberes y obligaciones que establece la LGPDPPSO, los Lineamientos Generales y demás disposiciones que resulten aplicables.	☐	☐

2. Deberes

a) Seguridad

Con fundamento en el artículo 31 de la LGPDPPSO, el deber de seguridad consiste en la implementación de medidas de seguridad físicas, técnicas y administrativas necesarias para proteger los datos personales contra daño, pérdida, alteración, destrucción, o su uso, acceso o tratamiento no automatizado, así como para garantizar su confidencialidad, integridad y disponibilidad.

Comprobación:

	Sí	No
1. Se han definido y se establecen y mantienen las medidas de seguridad administrativas, técnicas y físicas necesarias para la protección de los datos personales.	☐	☐
2. Se tienen en cuenta estándares y mejores prácticas en la implementación, monitoreo y mejora continua de las medidas de seguridad administrativas, técnicas y físicas.	☐	☐
3. Se ha revisado el marco normativo que regula en lo particular el tratamiento de datos personales en cuestión, a fin de identificar si éste contempla medidas de seguridad específicas o adicionales a las previstas en la LGPDPPSO y los Lineamientos Generales, y se ha definido la procedencia de su implementación.	☐	☐
4. El Área del IFT toma en cuenta el contexto en el que ocurren los tratamientos y el ciclo de vida de los datos personales, así como el nivel de riesgo y/o las consecuencias potencialmente negativas que podrían impactar en las personas titulares.	☐	☐
5. Se han definido las funciones, obligaciones y cadena de mando de cada servidor público que trata datos personales, por unidad administrativa.	☐	☐
6. Se ha comunicado a cada servidor público sus funciones, obligaciones y cadena de mando con relación al tratamiento de datos personales que efectúa.	☐	☐
7. Se ha elaborado el inventario de datos personales con los siguientes elementos:	☐	☐

• El catálogo de medios físicos y electrónicos a través de los cuales se obtienen los datos personales; • Las finalidades de cada tratamiento de datos personales; • El catálogo de los tipos de datos personales que se traten, indicando si son sensibles o no; • El catálogo de formatos de almacenamiento, así como la descripción general de la ubicación física y/o electrónica de los datos personales; • La lista de servidores públicos que tienen acceso a los sistemas de tratamiento; • En su caso, el nombre completo o denominación o razón social del encargado y el instrumento jurídico que formaliza la prestación de los servicios que brinda al responsable, y • En su caso, los destinatarios o terceros receptores de las transferencias que se efectúen, así como las finalidades que las justifican.		
8. En el inventario de datos personales se tomó en cuenta el ciclo de vida de los datos personales, conforme a lo siguiente: • La obtención de los datos personales; • El almacenamiento de los datos personales; • El uso de los datos personales conforme a su acceso, manejo, aprovechamiento, monitoreo y procesamiento, incluyendo los sistemas físicos y/o electrónicos utilizados para tal fin; • La divulgación de los datos personales considerando las remisiones y transferencias que, en su caso, se efectúen; • El bloqueo de los datos personales, en su caso, y • La cancelación, supresión o destrucción de los datos personales.	☐	☐
9. Se ha realizado el análisis de riesgo, considerando lo siguiente: • Los requerimientos regulatorios, códigos de conducta o mejores prácticas de un sector específico; • El valor de los datos personales de acuerdo a su clasificación previamente definida y su ciclo de vida;	☐	☐

• El valor y exposición de los activos involucrados en el tratamiento de los datos personales; • Las consecuencias negativas para los titulares que pudieran derivar de una vulneración de seguridad ocurrida; • El riesgo inherente a los datos personales tratados, contemplando el ciclo de vida de los datos personales, las amenazas y vulnerabilidades existentes para los datos personales y los recursos o activos involucrados en su tratamiento, como pueden ser, de manera enunciativa más no limitativa, hardware, software, personal o cualquier otro recurso humano o material, entre otros; • La sensibilidad de los datos personales tratados; • El desarrollo tecnológico; • Las transferencias de datos personales que se realicen; • El número de titulares; • Las vulneraciones previas ocurridas en los sistemas de tratamiento, y • El riesgo por el valor potencial cuantitativo o cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada para su posesión.		
10. Se ha realizado el análisis de brecha, tomando en cuenta lo siguiente: • Las medidas de seguridad existentes y efectivas; • Las medidas de seguridad faltantes, y • La existencia de nuevas medidas de seguridad que pudieran remplazar a uno o más controles implementados actualmente.	☐	☐
11. Se ha elaborado el 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, a partir del análisis de riesgo y brecha realizado, y priorizando las medidas de seguridad más relevantes e inmediatas a establecer.	☐	☐
12. Se monitorea y revisa de manera periódica las medidas de seguridad implementadas, así como las amenazas y	☐	☐

vulneraciones a las que están sujetos los datos personales, tomando en cuenta lo siguiente: • Los nuevos activos que se incluyan en la gestión de riesgos; • Las modificaciones necesarias a los activos, como podría ser el cambio o migración tecnológica, entre otras; • Las nuevas amenazas que podrían estar activas dentro y fuera de su organización y que no han sido valoradas; • La posibilidad de que vulnerabilidades nuevas o incrementadas sean explotadas por las amenazas correspondientes; • Las vulnerabilidades identificadas para determinar aquéllas expuestas a amenazas nuevas o pasadas que vuelvan a surgir; • El cambio en el impacto o consecuencias de amenazas valoradas, vulnerabilidades y riesgos en conjunto, que resulten en un nivel inaceptable de riesgo, y • Los incidentes y vulneraciones de seguridad ocurridas.		
13. Se cuenta con un programa de capacitación para los servidores públicos y externos involucrados en el tratamiento de datos personales, y se implementa.	☐	☐
14. Se ha implementado un Sistema de Gestión.	☐	☐
15. Se cuenta con el Documento de Seguridad con la información que establece el artículo 35 de la LGPDPPSO.	☐	☐
16. En el Documento de Seguridad se establece un procedimiento para su actualización, en caso de que ocurra alguno de los supuestos del artículo 36 de la LGPDPPSO.	☐	☐

Medios que facilitan la acreditación del cumplimiento
• Documento de Seguridad del IFT. • Evidencia generada en la implementación de los controles de seguridad. • Marco normativo que regula en lo particular el tratamiento en cuestión.

- Documentación que se genere con motivo de la planeación, implementación, evaluación y mejora de las Políticas y Programas de protección de datos.
- Documento en el que se establezcan las funciones, obligaciones y cadena de mando de cada persona servidora pública.
- Documento mediante el cual se haya comunicado la información antes señalada.
- Constancias de acciones de capacitación dirigidas al personal del Instituto.
- Inventario de datos personales
- Análisis de riesgos documentado.
- Análisis de brecha documentado.
- Plan de trabajo elaborado.
- Plan de monitoreo periódico.
- Documentación que se genere a partir de la implementación del plan.
- Programa de capacitación.

b) Confidencialidad

De conformidad con lo dispuesto en el artículo 42 de la LGPDPPSO, las personas servidoras públicas del IFT que intervengan en cualquier fase del tratamiento de los datos personales, deberán guardar confidencialidad respecto a los datos personales a los que tengan acceso, obligación que subsistirá aún después de finalizar sus relaciones con el Instituto, y sin menoscabo de lo establecido en las disposiciones de acceso a la información pública.

Comprobación:

	Sí	No
1. Los controles para la seguridad de los datos personales incluyen medidas para la confidencialidad de los datos personales.		
2. Se implementan los controles para la confidencialidad de los datos personales.		
3. Los contratos celebrados por el IFT contienen cláusulas de confidencialidad.		
4. Los contratos con encargados contienen cláusulas de confidencialidad, cuando así es requerido por el área		

	Sí	No
requirente y administradora del contrato respectivo o ésta notifique que existe la posibilidad de tratar datos personales con motivo de la contratación efectuada.		

3. Encargados

En cumplimiento a lo dispuesto en los artículos 59 y 61 de la LGPDPPSO, y 108 a 110 de los Lineamientos Generales, las Áreas del IFT que contraten los servicios de proveedores externos que actúen con carácter de encargados, deberán elaborar y suscribir contratos u otros instrumentos jurídicos que permitan acreditar la existencia, alcance y contenido de la relación jurídica con el Instituto, en su carácter de responsable del tratamiento; debiendo informar sobre dicha circunstancia a la Unidad de Administración, a través de su Dirección General de Adquisiciones, Recursos Materiales y Servicios Generales.

En los contratos, sus anexos u otros instrumentos jurídicos que las Áreas del Instituto celebren con terceros que actúen con carácter de encargados, deberán incluirse, cuando menos, las siguientes obligaciones para el encargado:

- Realizar el tratamiento de los datos personales conforme a las instrucciones conferidas por el Instituto.

- Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por el Instituto.

- Implementar medidas de seguridad físicas, técnicas y administrativas para garantizar la confidencialidad, integridad y seguridad de los datos personales.

- Informar al Instituto cuando ocurra una vulneración a los datos personales que se encuentran en su posesión.

- Guardar confidencialidad respecto de los datos personales tratados.

- Suprimir o devolver los datos personales objeto de tratamiento una vez cumplida la relación jurídica con el responsable, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales por parte del encargado.

- Abstenerse de transferir los datos personales salvo en el caso de que el Instituto así lo determine, o la comunicación derive de una subcontratación, o por mandato expreso de una autoridad competente.

- Cumplir con las obligaciones previstas en la LGPDPPSO y los Lineamientos Generales de Protección de Datos Personales para el Sector Púbico, y demás normatividad aplicable.

- Generar, actualizar y conservar la documentación necesaria que les permita acreditar el cumplimiento de sus obligaciones.

Medios que facilitan la acreditación del cumplimiento
• Cláusulas tipo. • Contratos, sus anexos u otros instrumentos jurídicos.

Comprobación:

	Sí	No
1. Las relaciones con los encargados se formalizan mediante contratos o instrumentos jurídicos.	☐	☐
2. Estos contratos o instrumentos jurídicos establecen cláusulas con las obligaciones mínimas establecidas en la LGPDPPSO para los encargados.	☐	☐
3. En caso de ser necesario, el contrato original establece una cláusula mediante la cual se autoriza subcontrataciones y/o que establezca que todas las subcontrataciones deberán ser autorizadas por el responsable.	☐	☐
4. En aquellos casos que el responsable autorice las subcontrataciones, éstas son específicas y se encuentran contenidas en un contrato o instrumento jurídico que establezca las cláusulas aplicables al encargado.	☐	☐
5. Se informa al encargado la obligación de incluir en el contrato o instrumento jurídico mediante el cual se formalice, en su caso, la subcontratación, las obligaciones antes señaladas para el tercero subcontratado.	☐	☐

4. Contratación de proveedores de servicios de cómputo en la nube

En términos de los artículos 63 y 64 de la LGPDPPSO, y 111 de los Lineamientos Generales, en la contratación de proveedores de servicios de cómputo en la nube y similares, el área requirente en coordinación con el área técnica del Instituto tendrán la obligación de establecer mecanismos en los procedimientos de contratación aplicables, que les permitan cerciorarse que dichos proveedores cuentan con políticas de protección de datos personales adecuados, conformes, equiparables o superiores al nivel de protección establecido en la LGPDPPSO, los Lineamientos Generales y demás disposiciones que resulten aplicables en la materia.

Comprobación:

	Sí	No
1. En caso de que, en la contratación de este tipo de servicios, el responsable tenga la posibilidad de convenir con el proveedor las condiciones y términos que impliquen un tratamiento de los datos personales, en el contrato, sus anexos o instrumento jurídico que suscriban con éstos, se deberán revisar las cláusulas contractuales previo a la celebración del contrato respectivo, con objeto de determinar si las mismas cumplen con los requisitos de la LGPDPPSO, los Lineamientos Generales y demás normatividad que resulte aplicable.	☐	☐
2. En caso de que el responsable se adhiera a los servicios de cómputo en la nube y otras materias semejantes, mediante condiciones, cláusulas, términos, condiciones y políticas generales de contratación previamente estipuladas por el proveedor de los servicios, el área requirente y el área técnica del Instituto, deberán verificar que se cumpla con lo dispuesto en los artículos 63 y 64 de la LGPDPPSO, en lo aplicable.	☐	☐
3. Los contratos de servicios de cómputo en la nube vigentes cumplen con los requisitos de la LGPDPPSO, o bien, para el caso de contrataciones efectuadas con base en la legislación del país en donde se encuentre el establecimiento principal de los proveedores y fabricantes de los servicios; éstas son acordes con los principios y deberes de la LGPDPPSO.	☐	☐

5. Transferencias de datos personales

De conformidad con lo dispuesto por los artículos 66, 67, 68, 69 y 70 de la LGPDPPSO y 113 a 118 de los Lineamientos Generales, las transferencias nacionales e internacionales de datos personales que realicen las Áreas del IFT deberán formalizarse mediante la suscripción de cláusulas contractuales, convenios de colaboración o cualquier otro instrumento jurídico, que permita demostrar el alcance del tratamiento de los datos personales, así como las obligaciones y responsabilidades asumidas por las partes, excepto en los supuestos siguientes:

- Cuando la transferencia sea nacional y se realice entre el sujeto obligado y otros responsables en virtud del cumplimiento de una disposición legal o en el ejercicio de atribuciones expresamente conferidas a éstos, o

- Cuando la transferencia sea internacional y se encuentre prevista en una ley o tratado suscrito y ratificado por México, o bien, se realice a petición de una autoridad extranjera u organismo internacional competente en su carácter de receptor, siempre y cuando las facultades entre el sujeto obligado y el responsable receptor sean homólogas, o bien, las finalidades que motivan la transferencia sean análogas o compatibles respecto de aquéllas que dieron origen al tratamiento que realiza el sujeto obligado.

Actividades para su cumplimiento	Áreas responsables del cumplimiento
• Identificar las transferencias que requieran la suscripción de cláusulas contractuales, convenios de colaboración u otro instrumento jurídico, que permita demostrar el alcance del tratamiento de los datos personales, así como las obligaciones y responsabilidades asumidas por las partes. • Elaborar y suscribir las cláusulas contractuales, convenios de colaboración u otro instrumento jurídico, cuando se requiera. • Realizar transferencias de datos fuera del territorio nacional únicamente cuando el	Áreas del Instituto que lleven a cabo transferencias de datos personales.

tercero receptor se obligue a proteger los datos personales conforme a los principios y deberes que establece la LGPDPPSO y las disposiciones que resulten aplicables en la materia. • Comunicar el Aviso de Privacidad respectivo al tercero receptor en las transferencias nacionales e internacionales que se lleven a cabo.	

Comprobación:

	Sí	No
1. Se tienen identificadas las transferencias que requieren la suscripción de cláusulas contractuales, convenios de colaboración u otro instrumento jurídico, que permita demostrar el alcance del tratamiento de los datos personales, así como las obligaciones y responsabilidades asumidas por las partes.	☐	☐
2. Se han elaborado y suscrito las cláusulas contractuales, convenios de colaboración u otro instrumento jurídico respectivos.	☐	☐
3. Se solicita al tercero receptor internacional que manifieste por escrito que se obliga a proteger los datos personales conforme a los principios y deberes que establece la LGPDPPSO y las disposiciones que resulten aplicables en la materia.	☐	☐
4. Se comunica al tercero receptor el Aviso de Privacidad correspondiente y, en su caso, sus modificaciones.	☐	☐
5. Se han identificado las transferencias que requieren el consentimiento y todas ellas son informadas en el Aviso de Privacidad.	☐	☐
6. Se solicita el consentimiento de las personas titulares, en su caso.	☐	☐
7. Se han establecido medios adecuados para solicitar el consentimiento expreso: que permitan obtenerlo de manera	☐	☐

previa a la transferencia, que sean de fácil acceso y con la mayor cobertura posible, y que consideren el perfil de los titulares y la forma en cómo se mantiene contacto cotidiano o común con ellos.		
8. Sólo se tratan los datos personales para las finalidades para las cuales fueron transferidos.	☐	☐
9. Se aplican controles de seguridad para la transferencia de los datos personales.	☐	☐

6. Evaluaciones de Impacto en la Protección de Datos Personales

En términos de lo dispuesto por los artículos 74, 75, 77, 78 y 79 de la LGPDPPSO y 120 de los Lineamientos Generales, cuando el personal del Instituto pretenda poner en operación o modificar políticas públicas, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que a su juicio y de conformidad con este ordenamiento impliquen el tratamiento intensivo o relevante de datos personales, deberá realizar una Evaluación de impacto en la protección de datos personales (Evaluación de Impacto), y presentarla ante el INAI.

La Evaluación de Impacto deberá elaborarse teniendo en cuenta las *Disposiciones administrativas de carácter general para la elaboración, presentación y valoración de evaluaciones de impacto en la protección de datos personales,*[10] aprobadas por el Sistema Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales.

Actividades para su cumplimiento	Áreas responsables del cumplimiento
• Identificar los tratamientos de datos personales que puedan ser considerados intensivos o relevantes, en términos del artículo 75 de la LGPDPPSO y las *Disposiciones administrativas de carácter general para la elaboración, presentación y valoración de evaluaciones de impacto en la protección de datos personales.*	Todas las Áreas del Instituto que identifiquen un tratamiento de datos personales intensivos o relevantes.

[10] Disponibles en el vínculo electrónico: https://dof.gob.mx/nota_detalle.php?codigo=5511113&fecha=23/01/2018

• Atender el plazo para presentar la Evaluación de Impacto ante el INAI (30 días anteriores a la fecha en que se pretenda poner en operación o modificar políticas públicas, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento intensivo o relevante de datos personales).	

Comprobación:

	Sí	No
1. Se ha identificado la necesidad de poner en operación o modificar políticas públicas, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que impliquen el tratamiento intensivo o relevante de datos personales.	☐	☐
2. Se ha identificado si el tratamiento emplea nuevas tecnologías que, por su naturaleza, alcance, contexto o fines, entrañe un riesgo alto para los datos personales, así como para los derechos y libertades de las personas titulares.	☐	☐
3. Se han observado los requisitos establecidos en las *Disposiciones administrativas de carácter general para la elaboración, presentación y valoración de evaluaciones de impacto en la protección de datos personales.*	☐	☐
4. Las evaluaciones de impacto se presentan en tiempo y forma.	☐	☐
5. Se atienden las observaciones del INAI.	☐	☐

7. Portabilidad de Datos Personales

La portabilidad de los datos personales confiere a los titulares la prerrogativa de obtener y reutilizar sus datos personales, para fines propios y en diferentes servicios. En este sentido, el derecho a la portabilidad busca facilitar la capacidad para obtener, copiar o transmitir fácilmente datos personales de un sistema de tratamiento automatizado a otro sistema en un formato electrónico estructurado y comúnmente utilizado.

Para ser objeto de portabilidad, los datos personales deben tratarse por el IFT por vía electrónica, en un formato estructurado y comúnmente utilizado, y ser proporcionados al titular en un formato de similar naturaleza, que le permita seguir utilizándolos.

Ahora bien, teniendo en cuenta que los Lineamientos de Portabilidad no establecen de manera específica los tipos o categorías de formatos que tienen la calidad de estructurados y comúnmente utilizados, refiriendo únicamente y de manera general las características que estos deben reunir para considerarse como tales, el Instituto implementó y determinó que, para garantizar el ejercicio del derecho a la portabilidad de datos personales, serían considerados como formatos electrónicos estructurados y comúnmente utilizados, los siguientes:

a) Formato Excel (*.xlsx);

b) Formato de Texto (*.txt);

c) Formato de Archivo de texto (*.csv), y

d) Formato de Lenguaje de marcas de hipertexto (*.html).

Los formatos anteriores son, por ende, los formatos electrónicos estructurados y comúnmente utilizados por el Instituto, en los cuales deben encontrarse los datos personales para ser objeto de portabilidad, con el objeto de proporcionarse en el mismo formato al titular de los datos, en respuesta y atención a una solicitud de portabilidad de datos personales.

El 26 de septiembre de 2019, en la Décimo Sexta Sesión Ordinaria de 2019, el Comité aprobó los siguientes mecanismos específicos para garantizar este derecho:

a) La "*Guía para ejercer el derecho a la portabilidad de los datos personales en posesión del Instituto Federal de Telecomunicaciones*";

b) El "*Formato para el ejercicio del derecho a la portabilidad de los datos personales en posesión del Instituto Federal de Telecomunicaciones*", y

c) El "*Procedimiento interno para garantizar los derechos de acceso, rectificación, cancelación, oposición y portabilidad de datos personales ejercidos ante el Instituto Federal de Telecomunicaciones*" (Procedimiento Interno).

Los documentos referidos en los incisos a y b, se encuentran disponibles en el Apartado Virtual de Protección de Datos Personales del IFT, en la ruta: https://www.ift.org.mx/sites/default/files/OPNT/LGPDPPSO/4_Portabilidad/Criterio_4_1_2.zip.

Respecto al Procedimiento Interno, referido en el inciso c, se encuentra disponible en la subcarpeta de Datos Personales, ubicada en la carpeta de la Unidad de Transparencia, disponible accediendo a la red interna del IFT, mediante el vínculo electrónico que se indica a continuación:

http://www.conexion.ift.org.mx/intranet/index.php/equipo/unidad-de-transparencia

Comprobación:

	Sí	No
Se atienden las solicitudes del ejercicio del derecho de portabilidad según los criterios y parámetros establecidos por la LGPDPPSO y los Lineamientos que establecen los parámetros, modalidades y procedimientos para la portabilidad de datos personales.	☐	☐

C. Identificación de riesgos y fortalecimiento de medidas y controles de seguridad existentes.

Un riesgo de seguridad se define como el potencial de que cierta amenaza pueda explotar las vulnerabilidades de un activo o grupo de activos en perjuicio de la organización. Durante el Sistema de Gestión de Seguridad de Datos Personales, se deben identificar los riesgos relacionados a los datos personales, así como al resto de activos que interactúan directamente con ellos, y de ese modo determinar los controles de seguridad que pueden mitigar los incidentes.

Como parte de las acciones para la seguridad de los datos personales, y con fundamento en el artículo 35 de la LGPDPPSO, el Instituto elaboró el Documento de Seguridad del IFT que describe y da cuenta de manera general sobre las medidas de seguridad adoptadas, para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que se encuentran en su posesión.

El Documento de Seguridad incorpora, en términos generales, los elementos requeridos para el diseño de un Sistema de Gestión. No obstante, durante el periodo 2023-2024 se propone llevar a cabo acciones para mejorar el enfoque del Sistema de Gestión, de conformidad con algunos estándares

internacionales (por ejemplo, la Norma ISO/IEC 27701:2019) y las Guías emitidas por el INAI.

D. Respuesta a incidentes o vulneraciones de seguridad.

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:

Clasificación de vulneraciones de seguridad	Incide en
• Pérdida o destrucción no autorizada	Disponibilidad
• Robo, extravío o copia no autorizada	Confidencialidad y Disponibilidad
• Uso, acceso o tratamiento no autorizado	Confidencialidad
• Daño, alteración o modificación no autorizada	Integridad

La gestión y notificación de vulneraciones de seguridad se llevará a cabo conforme a lo previsto en los numerales XXI y XXII de la *Política Interna de Gestión y Tratamiento de Datos Personales del Instituto Federal de Telecomunicaciones*. Durante el periodo 2023-2024, se definirán acciones adicionales para identificar y responder a vulneraciones de seguridad, en cualquier fase del tratamiento de los datos personales.

Lo anterior, con el objeto de dar cabal cumplimiento a lo previsto en el artículo 40 de la LGPDPPSO, que establece la obligación a cargo del IFT de informar sin dilación alguna a la persona titular, y según corresponda, al INAI las vulneraciones **que afecten de forma significativa (énfasis añadido),** los derechos patrimoniales o morales, en un plazo máximo de **72 horas**, a partir de que se confirme que ocurrió la vulneración y que se haya empezado a tomar las acciones encaminadas a detonar un proceso de mitigación de la afectación. El plazo de 72 horas comenzará a correr el mismo día natural en que el responsable confirme la vulneración de seguridad.

Afectación de derechos morales	Afectación de derechos patrimoniales
Se entenderá que se afectan los derechos morales de la persona titular cuando la vulneración esté relacionada, de manera enunciativa más no limitativa, con sus sentimientos, afectos, creencias,	Se entenderá que se afectan los derechos patrimoniales de la persona titular cuando la vulneración esté relacionada, de manera enunciativa más no limitativa, con sus bienes muebles e

Afectación de derechos morales	Afectación de derechos patrimoniales
decoro, honor, reputación, vida privada, configuración y aspecto físicos, consideración que de sí mismo tienen los demás, o cuando se menoscabe ilegítimamente la libertad o la integridad física o psíquica de éste.	inmuebles, información fiscal, historial crediticio, ingresos y egresos, cuentas bancarias, seguros, afores, fianzas, servicios contratados o las cantidades o porcentajes relacionados con la situación económica de la persona titular.

El procedimiento para llevar a cabo la notificación de vulneraciones de seguridad, comprenderá las acciones siguientes:

- Diseñar un formato de notificación de las vulneraciones de seguridad ocurridas, donde se incluya la descripción de la información siguiente:

  - La naturaleza del incidente o vulneración ocurrida;
  - Los datos personales comprometidos;
  - Las recomendaciones al titular acerca de las medidas que éste pueda adoptar para proteger sus intereses;
  - Las acciones correctivas realizadas de forma inmediata;
  - Los medios donde puede obtener más información al respecto;
  - La descripción de las circunstancias generales en torno a la vulneración ocurrida, que ayuden al titular a entender el impacto del incidente, y
  - Cualquier otra información y documentación que considere conveniente para apoyar a los titulares.

- Actualizar la bitácora o registro de las vulneraciones a la seguridad en la que se describan éstas, la fecha en la que ocurrieron, el motivo de éstas y las acciones correctivas implementadas de forma inmediata y definitiva.

E. Sensibilización y capacitación

Con fundamento en el artículo 30 de la LGPDPPSO, fracción III, el IFT ha implementado un programa de capacitación y actualización del personal sobre las obligaciones y demás deberes en materia de protección de datos

personales. Este programa forma parte de los mecanismos para cumplir con el principio de "responsabilidad", que a su vez es necesario para garantizar y facilitar el cumplimiento de los demás principios y deberes en el tratamiento de datos personales, previstos en el artículo 16 de la LGPDPPSO.

A su vez, en términos del artículo 35, fracción VII, de la LGPDPPSO, el programa general de capacitación forma parte del Documento de Seguridad del IFT y constituye, de manera específica, una medida de seguridad administrativa, en términos de lo dispuesto por el artículo 3°, fracción XXI, de este ordenamiento.

En este sentido, el Programa General asume como una premisa central que la promoción, difusión y fomento de una cultura de protección de datos personales, es un factor determinante para orientar y garantizar el cumplimiento adecuado de algunos de los objetivos establecidos en el artículo 2° de la LGPDPPSO.

En términos del artículo 84, fracción VII, de la LGPDPPSO, corresponde al Comité de Transparencia del IFT establecer programas de capacitación y actualización para las personas servidoras públicas en materia de protección de datos personales. En ese sentido, a continuación, se incluyen las acciones de capacitación previstas para el personal del IFT en materia de protección de datos personales, aprobadas por el Comité de Transparencia:

No.	Acción de capacitación	Tipo de Acción	Proveedor	Modalidad
1	Introducción a la Ley Federal de Transparencia y Acceso a la Información Pública.	Curso	INAI	Presencial a distancia
2	Introducción a la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.	Curso	INAI	Presencial a distancia
3	Introducción a la Ley General de Archivos.	Curso	INAI	Presencial a distancia
4	Ética Pública.	Curso	INAI	Presencial a distancia
5	Clasificación de la Información y Prueba de Daño.	Curso	INAI	Presencial a distancia

No.	Acción de capacitación	Tipo de Acción	Proveedor	Modalidad
6	Fundamentos del Documento de Seguridad en Materia de Protección de Datos Personales.	Curso	INAI	Presencial a distancia
7	Procedimiento de Impugnación y Criterios del Pleno.	Curso	INAI	Presencial a distancia
8	Transparencia Proactiva.	Curso	INAI	Presencial a distancia
9	Políticas de Acceso a la Información.	Curso	INAI	Presencial a distancia
10	Obligaciones de Transparencia y Carga de Información en el Sistema de Portales de Obligaciones de Transparencia (SIPOT).	Curso	INAI	Presencial a distancia
11	Esquemas de Mejores Prácticas en Materia de Protección de Datos Personales en el Sector Público.	Curso	INAI	Presencial a distancia
12	Auditorías Voluntarias en Materia de Protección de Datos Personales en el Sector Público.	Curso	INAI	Presencial a distancia
13	Interpretación y Argumentación Jurídica.	Curso	INAI	Presencial a distancia

1	Ciberseguridad - Web 3.0 y Protección de Datos Personales.	Curso de temas especializados	INAI	Presencial a distancia

No.	Acción de capacitación	Tipo de Acción	Proveedor	Modalidad
2	Seguridad de Datos Personales y Uso Responsable de Tecnologías.	Curso de temas especializados	INAI	Presencial a distancia
3	Inteligencia Artificial y sus Implicaciones en la Protección de Datos Personales.	Curso de temas especializados	INAI	Presencial a distancia
4	Protección de Datos Personales en el Tratamiento de Datos Biométricos y Sensibles.	Curso de temas especializados	INAI	Presencial a distancia
5	Retos Tecnológicos de la Portabilidad.	Curso de temas especializados	INAI	Presencial a distancia
6	Comunicación de Datos Personales y el Flujo Transfronterizo de los mismos.	Curso de temas especializados	INAI	Presencial a distancia
7	Seguridad de Datos Personales y uso responsable de tecnologías en los sectores público y privado.	Curso de temas especializados	INAI	Presencial a distancia

	Sí	No
1. Se cuenta con un programa anual de capacitación y actualización de las personas servidoras públicas del IFT y encargados de la protección de los datos personales, a corto, mediano y largo plazo, que toma en cuenta los roles y responsabilidades asignadas para el tratamiento y seguridad de los datos personales y el perfil de puestos.	☐	☐

F. Monitoreo y revisión

Con el fin de monitorear y supervisar de manera permanente el cumplimiento de los principios y deberes en el tratamiento de datos, así

como las medidas de seguridad administrativas, físicas y técnicas en el IFT, y de conformidad con lo previsto en el artículo 35, fracciones V y VI, de la LGPDPPSO, y los apartados X y XI del Documento de Seguridad del IFT, se creó el "Grupo de Trabajo de Protección de Datos Personales en Posesión del Instituto Federal de Telecomunicaciones" (Grupo de Trabajo).

El Grupo cuenta con la participación de los Integrantes del Comité, el personal especializado en temas de protección de datos personales, archivo, control interno y administración de riesgos, seguridad de la información, las personas que fungen como "Subenlaces de Transparencia y Protección de Datos Personales", así como de las personas servidoras públicas involucradas directamente en el tratamiento de los datos personales en las distintas Áreas del Instituto.

El Grupo de Trabajo tiene como objetivos:

- Analizar la situación actual del cumplimiento de los principios y deberes establecidos en la LGPDPPSO y los Lineamientos Generales;

- Monitorear el funcionamiento de las medidas de seguridad administrativas, físicas y técnicas, implementadas para proteger la confidencialidad, integridad y disponibilidad de los datos personales en posesión del Instituto;

- Proponer medidas de seguridad administrativas, físicas y técnicas adicionales que puedan incluirse en las políticas de seguridad de la información o en un programa de protección de datos personales institucional;

- Identificar posibles riesgos y amenazas que requieran la adopción de estrategias organizacionales para mitigarlas, con el objetivo de disminuir el impacto en los activos de información en posesión del Instituto;

- Identificar y diseñar soluciones prácticas a problemas, complicaciones y/o contrariedades, entre otras, que dificulten la aplicación y/o cumplimiento de la normatividad en la materia, a efecto de adoptar o estandarizar criterios de control interno para cumplir con los principios de protección de datos personales;

- Detectar y solicitar a las instancias correspondientes capacitación en temas específicos del derecho a la protección de datos personales en atención a las necesidades que se identifiquen al interior del Instituto;

- Aplicar herramientas y metodologías especializadas de control interno y administración de riesgos que promuevan una cultura institucional de protección de datos personales;

- Fungir como un foro para el intercambio de información, apreciaciones o propuestas respecto al cumplimiento de los objetivos previstos en la LGPDPPSO, los Lineamientos Generales y demás normativa aplicable, la Política de Datos Personales, el Documento de Seguridad del IFT, y cualquier instrumento relativo y derivado de dichos ordenamientos;

- Llevar a cabo reuniones de trabajo, cuando las circunstancias específicas así lo ameriten, conforme a la convocatoria, calendario y dinámica acordados previamente por el Comité, y remitidas por la Secretaría del Grupo de Trabajo, las cuales tendrán como objeto planear, diseñar, elaborar, instituir, coordinar y supervisar, en tiempo real, las acciones y los procedimientos para garantizar el derecho a la protección de los datos personales en posesión del IFT, de conformidad con las disposiciones previstas en la LGPDPPSO, los Lineamientos Generales y demás normativa aplicable, la Política de Datos Personales, el Documento de Seguridad del IFT, y cualquier instrumento relativo y derivado de dichos ordenamientos, y

- Coadyuvar con las Unidades Administrativas del Instituto, que así lo requieran, en cuanto a la posible adopción de las medidas de seguridad que correspondan, con base en los insumos recabados y proporcionados por las Áreas.

De conformidad con la regla NOVENA de las "Reglas del Grupo de Trabajo de Protección de Datos Personales en Posesión del Instituto Federal de Telecomunicaciones", se prevén 4 reuniones anuales, distribuidas trimestralmente en los meses de febrero, mayo, agosto y noviembre. Para pronta referencia, se adjunta el calendario de las próximas reuniones, en el periodo que comprende el presente documento:

Reuniones Ordinarias del Grupo de Trabajo de Protección de Datos Personales en Posesión del Instituto Federal de Telecomunicaciones (2023)				
	Febrero 2023	Mayo 2023	Agosto 2023	Noviembre 2023
Primera Reunión 2023				
Segunda Reunión 2023				
Tercera Reunión 2023				
Cuarta Reunión 2023				

Reuniones Ordinarias del Grupo de Trabajo de Protección de Datos Personales en Posesión del Instituto Federal de Telecomunicaciones (2024)				
	Febrero 2024	Mayo 2024	Agosto 2024	Noviembre 2024
Primera Reunión 2024				
Segunda Reunión 2024				
Tercera Reunión 2024				
Cuarta Reunión 2024				

G. Sanciones

Cualquier incumplimiento a este Programa será informado a la Dirección General de Gestión de Talento, para que ésta en ejercicio de sus atribuciones, determine e imponga, en su caso, las medidas disciplinarias laborales que correspondan, con independencia de las sanciones establecidas en la LGPDPPSO, Ley General de Transparencia y Acceso a la Información Pública y Ley General de Responsabilidades Administrativas. Los procedimientos administrativos correspondientes derivados de la violación a las disposiciones referidas son independientes de las del orden civil, penal o de cualquier otro tipo que se puedan derivar de los mismos hechos.

VIII. Documentos relevantes

Denominación del documento	Hipervínculo para consulta
Apartado de protección de datos personales del IFT	https://www.ift.org.mx/proteccion_de_datos_personales
Avisos de Privacidad de datos personales que el IFT recaba a través de sus Áreas	https://www.ift.org.mx/proteccion_de_datos_personales/avisos_de_privacidad
Acuerdo del Comité de Transparencia mediante el cual se aprueban los formatos de los Avisos de Privacidad del Instituto Federal de Telecomunicaciones	https://www.ift.org.mx/sites/default/files/OPNT/LGPDPPSO/6_CT_UT/Formatos_AP.pdf
Política Interna de Gestión y Tratamiento de Datos Personales del Instituto Federal de Telecomunicaciones	https://www.ift.org.mx/sites/default/files/OPNT/LGPDPPSO/1_M_cumplimiento/Política_Interna_Gestión_Tratamiento_DP.pdf
Documento de Seguridad, Inventario y Ciclo de Vida de Datos Personales en Posesión del IFT, así como la matriz de riesgos en procesos o sistemas	https://www.ift.org.mx/sites/default/files/OPNT/LGPDPPSO/2_Seguridad/Documento_Seguridad.pdf

manuales o no automatizados	
Manifiesto de resguardo electrónico de bases de datos por la Dirección General de Tecnologías de la Información y Comunicaciones	https://www.ift.org.mx/sites/default/files/OPNT/LGPDPPSO/2_Seguridad/Manifiesto_2022.pdf
Informes anuales referidos en el Documento de Seguridad para la Protección de Datos Personales en Posesión del IFT	https://www.ift.org.mx/sites/default/files/OPNT/LGPDPPSO/1_M_cumplimiento/Informe_DS_2020.pdf (Ejercicio 2020) https://www.ift.org.mx/sites/default/files/OPNT/LGPDPPSO/1_M_cumplimiento/Informe_DS_2021.pdf (Ejercicio 2021) https://www.ift.org.mx/sites/default/files/OPNT/LGPDPPSO/1_M_cumplimiento/Informe_DS_2022.pdf (Ejercicio 2022)
Informes anuales referidos en el Programa de Protección de Datos Personales (2021-2022)	https://www.ift.org.mx/sites/default/files/OPNT/LGPDPPSO/1_M_cumplimiento/Informe_Programa_2021.pdf (Ejercicio 2021) https://www.ift.org.mx/sites/default/files/OPNT/LGPDPPSO/1_M_cumplimiento/Informe_Programa_2022.pdf (Ejercicio 2022)
Metodología de Administración de Riegos del Instituto Federal de Telecomunicaciones	https://www.ift.org.mx/sites/default/files/OPNT/LGPDPPSO/1_M_cumplimiento/Metodologia_Admon_Riesgos.pdf
Mecanismos de monitoreo y revisión de las medidas de seguridad implementadas	https://www.ift.org.mx/sites/default/files/OPNT/LGPDPPSO/1_M_cumplimiento/M_monitoreo_revision.pdf
Programa General de Capacitación contenido en el Documento de Seguridad para la Protección de Datos Personales en Posesión del Instituto Federal de Telecomunicaciones	https://www.ift.org.mx/sites/default/files/OPNT/LGPDPPSO/1_M_cumplimiento/Programa_general_capacitacion.pdf
Programa Anual de Capacitación Institucional 2023	https://www.ift.org.mx/sites/default/files/OPNT/LGPDPPSO/1_M_cumplimiento/PAC_2023.pdf
Programa de Capacitación en Transparencia, Acceso a la Información, Protección de Datos Personales y Temas	https://www.ift.org.mx/sites/default/files/OPNT/LGPDPPSO/1_M_cumplimiento/ PCTAIPDPTR_2023.pdf

relacionados – 2023 (Comité de Transparencia – IFT)	
Normas de Control Interno del Instituto Federal de Telecomunicaciones	https://www.ift.org.mx/sites/default/files/OPNT/LGPDPPSO/1_M_cumplimiento/Normas_Control Interno.pdf
Informe relativo a los análisis de riesgos y de brecha identificados en los procesos y/o sistemas de tratamiento manual o no automatizado de datos personales en posesión del Instituto Federal de Telecomunicaciones	https://www.ift.org.mx/sites/default/files/OPNT/LGPDPPSO/1_M_cumplimiento/Informe_Riesgos_dp.pdf
Carta de confidencialidad que se suscribe al ingresar a trabajar al IFT	https://www.ift.org.mx/sites/default/files/OPNT/LGPDPPSO/2_Conf_com/Carta_Confidencialidad.pdf
Cláusula dirigida a asegurar la confidencialidad por parte de los proveedores del IFT	https://www.ift.org.mx/sites/default/files/OPNT/LGPDPPSO/2_Conf_com/Clausula_tipo_DGRMSG_contratos.pdf
Instrumentos jurídicos mediante los cuales se formaliza la contratación o adhesión a servicios, aplicaciones e infraestructura en el cómputo en la nube y otras materias	https://www.ift.org.mx/sites/default/files/OPNT/LGPDPPSO/2_Conf_com/Anexo_1_Seguridad_nube_publica.pdf (Características de la nube contratada) https://www.ift.org.mx/sites/default/files/OPNT/LGPDPPSO/2_Conf_com/Numeral_4_Computo_en_la_nube.pdf (Análisis artículo 64 de la LGPDPPSO)
Obligaciones a las que se comprometen los proveedores del IFT respecto del tratamiento y protección de datos personales a los que tengan acceso	https://www.ift.org.mx/sites/default/files/OPNT/LGPDPPSO/2_Conf_com/Anexo_9_IFT_SANHSO.pdf
Reglas de Operación del Grupo de Trabajo de Protección de Datos Personales del Instituto Federal de Telecomunicaciones	https://www.ift.org.mx/sites/default/files/OPNT/LGPDPPSO/1_M_cumplimiento/Reglas_grupo_pdp.pdf

Procedimiento para recibir y responder dudas, quejas y/o sugerencias de los titulares en materia de protección de datos personales	https://www.ift.org.mx/sites/default/files/OPNT/LGPDPPSO/1_M_cumplimiento/Procedimiento_dudas_quejas.pdf
Procedimiento interno para garantizar el ejercicio de los derechos de acceso, rectificación, cancelación, oposición y portabilidad de datos personales ejercidos ante el Instituto Federal de Telecomunicaciones	https://www.ift.org.mx/sites/default/files/OPNT/LGPDPPSO/6_CT_UT/Procedimiento_ARCOP.pdf
Guía para el ejercicio del derecho a la portabilidad de los datos personales en posesión del Instituto Federal de Telecomunicaciones	https://www.ift.org.mx/sites/default/files/OPNT/LGPDPPSO/3_M_ARCO/Guia_portabilidad.pdf
Formato para el ejercicio del derecho a la portabilidad de los datos personales en posesión del Instituto Federal de Telecomunicaciones	https://www.ift.org.mx/sites/default/files/OPNT/LGPDPPSO/3_M_ARCO/Formato_portabilidad.pdf
Encuesta de evaluación de calidad sobre la gestión de las solicitudes para el ejercicio de los derechos ARCO y/o Portabilidad	https://www.ift.org.mx/sites/default/files/OPNT/LGPDPPSO/6_CT_UT/Encuesta_ARCO.pdf