INSTITUTO FEDERAL DE TELECOMUNICACIONES

POLÍTICA INTERNA DE GESTIÓN Y TRATAMIENTO DE DATOS PERSONALES DEL INSTITUTO FEDERAL DE TELECOMUNICACIONES

APROBACIÓN

El Acuerdo mediante el cual el Comité de Transparencia del Instituto Federal de Telecomunicaciones aprobó la actualización a la "Política Interna de Gestión y Tratamiento de Datos Personales del Instituto Federal de Telecomunicaciones", se emitió en cumplimiento a los artículos 16, párrafo segundo, de la Constitución Política de los Estados Unidos Mexicanos; 30, fracciones II y IV, y 33, fracción I, 84, fracción I de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO), así como el artículo 47, segundo párrafo, de los Lineamientos Generales de Protección de Datos Personales para el Sector Público (Lineamientos de Datos Personales); en su Vigésima Novena Sesión Extraordinaria, celebrada el 16 de diciembre de 2022, mediante Acuerdo número 29/SE/27/22.

La Política Interna de Gestión y Tratamiento de Datos Personales fue refrendada 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.

POLÍTICA INTERNA DE GESTIÓN Y TRATAMIENTO DE DATOS PERSONALES DEL INSTITUTO FEDERAL DE TELECOMUNICACIONES

I. Contenido

Términos y Abreviaturas

ARCOP	Derechos de acceso, rectificación, cancelación y oposición, así como el derecho a la portabilidad de datos personales.
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.
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 Instituto 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 (externa), que sola o conjuntamente con otras trate datos personales a nombre y por cuenta del Instituto, en su carácter de responsable.
Estatuto Orgánico	Estatuto Orgánico del Instituto Federal de Telecomunicaciones.
IFT o Instituto	Instituto Federal de Telecomunicaciones.

INAI	Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.
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.
Lineamientos de Portabilidad	Lineamientos que establecen los parámetros, modalidades y procedimientos para la portabilidad de datos personales.
Política	Documento que describe los requisitos o reglas específicas que deben cumplirse al interior del Instituto Federal de Telecomunicaciones, que presenta una declaración formal, breve y de alto nivel, que abarca las creencias generales de la organización, metas, objetivos y procedimientos aceptables en el tratamiento de los datos personales.
Sistema de Gestión de Seguridad de Datos Personales (SGSDP)	Conjunto de elementos interrelacionados o que interactúan para establecer políticas, objetivos y procesos para lograr estos objetivos. El SGSDP es un proceso continuo que debe operar el Instituto, en su carácter de sujeto obligado y responsable del tratamiento de los datos personales que se encuentran en su posesión.

Titular	La persona física a quien corresponden los datos personales.
Transferencia de datos personales	Toda comunicación de datos personales dentro o fuera del territorio mexicano, realizada a persona distinta de la persona titular de los datos, del Instituto en su carácter de responsable del tratamiento, o de sus encargados.
Vulneraciones de seguridad	De manera enunciativa, la pérdida o destrucción no autorizada de datos personales; el robo, extravío o copia no autorizada de datos personales; el uso, acceso o tratamiento no autorizado de datos personales, o el daño, la alteración o modificación no autorizada de datos personales.

Marco Jurídico Aplicable

1. Constitución Política de los Estados Unidos Mexicanos.

2. Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

3. Lineamientos Generales de Protección de Datos Personales para el Sector Público.

4. Lineamientos que establecen los parámetros, modalidades y procedimientos para la portabilidad de datos personales.

5. Disposiciones administrativas de carácter general para la elaboración, presentación y valoración de evaluaciones de impacto en la protección de datos personales.

Política Interna de Gestión y Tratamiento de Datos Personales del Instituto Federal de Telecomunicaciones

I. Alcance

La Política es aplicable al tratamiento automatizado o no automatizado (manual) de datos personales que sea efectuado por las Unidades Administrativas del Instituto, 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.

La Política es aplicable al tratamiento de datos personales efectuado por personas físicas o morales que actúen como prestadores de servicios del Instituto, sea que se trate de encargados o no, siempre y cuando se encuentren ubicados o establecidos en territorio mexicano.

II. Carácter obligatorio de la Política

La Política es obligatoria 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 Orgánico, 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.

Las personas servidoras públicas, 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, tienen la obligación de conocer el contenido de la Política, así como aplicarla en los tratamientos de datos personales que efectúen, en el tramo de responsabilidad que les corresponda, conforme a sus funciones y atribuciones conferidas por el marco jurídico aplicable.

La Política es complementaria a las disposiciones previstas en la LGPDPPSO, los Lineamientos Generales y demás normativa derivada y aplicable, y será desarrollada en las políticas, programas y procedimientos de protección de datos personales adoptados por el Instituto, que tengan por objeto establecer los elementos y actividades de dirección, operación y control de todos sus procesos que, en el ejercicio de sus funciones y atribuciones, impliquen un tratamiento de datos personales a efecto de proteger éstos de manera sistemática y continúa.

La Política se encontrará disponible como información documentada para consulta de las personas servidoras públicas del Instituto.

III. Objetivos

La Política tiene como objetivos los siguientes:

1. Establecer las directrices generales de alto nivel orientadas a garantizar el derecho a la protección de los datos personales en el Instituto, de conformidad con las disposiciones previstas en la LGPDPPSO, los Lineamientos Generales y demás normativa derivada y aplicable;

2. Promover la capacitación y una cultura de protección de datos personales en el Instituto;

3. Establecer y fortalecer un régimen de responsabilidad proactiva y demostrada en el tratamiento de los datos personales en posesión del Instituto;

4. Instaurar los lineamientos generales de seguridad que permitan establecer, implementar, mantener y mejorar un Sistema de Gestión de Seguridad de Datos Personales, de conformidad con estándares nacionales e internacionales y buenas prácticas en la materia;

5. Prever los mecanismos que permitan al Instituto, medir, reportar y verificar las metas establecidas, y

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

IV. Compromiso

El Instituto asumirá y demostrará liderazgo y compromiso a través de su alta Dirección y el Comité de Transparencia, con respecto del cumplimiento de los principios, deberes y obligaciones establecidos en la LGPDPPSO, los Lineamientos Generales y demás normativa derivada, y llevará a cabo las siguientes acciones:

1. Asegurar que se establecen la Política y los objetivos de protección de datos personales, y que éstos sean compatibles con los objetivos y la dirección estratégica del Instituto;

2. Garantizar la integración de los requisitos del Sistema de Gestión de Seguridad de Datos Personales, en los procesos de tratamiento de datos personales que efectúe el Instituto;

3. Asegurar que los recursos para la instrumentación de programas y políticas de protección de datos personales necesarios estén disponibles de manera oportuna y sean suficientes;

4. Comunicar la importancia de una adecuada gestión de los tratamientos de datos personales;

5. Asegurar que el Sistema de Gestión de Seguridad de Datos Personales consigue los resultados previstos;

6. Promover la mejora continua, y

7. Apoyar los roles pertinentes para demostrar su liderazgo aplicado a sus áreas de responsabilidad.

V. Valores

Son valores que rigen el tratamiento de datos personales en el Instituto, los siguientes:

1. Legalidad[1];
2. Honradez[2];
3. Lealtad[3];
4. Transparencia[4];
5. Expectativa razonable de privacidad[5], y

[1] Las personas servidoras públicas hacen sólo aquello que las normas expresamente les confieren y en todo momento someten su actuación a las facultades que las leyes, reglamentos y demás disposiciones jurídicas atribuyen a su empleo, cargo o comisión, por lo que conocen y cumplen las disposiciones que regulan el ejercicio de sus funciones, facultades y atribuciones.
[2] Las personas servidoras públicas se conducen con rectitud sin utilizar su empleo, cargo o comisión para obtener o pretender obtener algún beneficio, provecho o ventaja personal o a favor de terceros, ni buscan o aceptan compensaciones, prestaciones, dádivas, obsequios o regalos de cualquier persona u organización, debido a que están conscientes que ello compromete sus funciones y que el ejercicio de cualquier cargo público implica un alto sentido de austeridad y vocación de servicio.
[3] Las personas servidoras públicas corresponden a la confianza que el Estado les ha conferido; tienen una vocación absoluta de servicio a la sociedad, y satisfacen el interés superior de las necesidades colectivas por encima de intereses particulares, personales o ajenos al interés general y bienestar de la población.
[4] Las personas servidoras públicas en el ejercicio de sus funciones privilegian el principio de máxima publicidad de la información pública, atendiendo con diligencia los requerimientos de acceso y proporcionando la documentación que generen, obtienen, adquieren, transforman o conservan; y en el ámbito de su competencia, difunden de manera proactiva información gubernamental, como un elemento que genera valor a la sociedad y promueve un gobierno abierto, protegiendo los datos personales que estén bajo su custodia.
[5] Por "expectativa razonable de privacidad" se entiende la confianza que la persona titular ha depositado en el IFT, en su carácter de responsable, respecto a que sus datos personales serán tratados conforme a lo

6. Responsabilidad proactiva y demostrada[6].

VI. Misión y Visión

El Instituto establecerá una misión y visión en la protección de datos personales, y actuará conforme a estas, a efecto de cumplir con los principios, deberes y obligaciones previstas en la LGPDPPSO, los Lineamientos generales y demás normativa derivada y aplicable.

VII. Sistema de Gestión de Seguridad de Datos Personales

La Política especifica los requisitos mínimos y proporciona una guía para implementar, mantener y mejorar continuamente un Sistema de Gestión de Seguridad de Datos Personales en el Instituto.

VIII. Identificación de Procesos de Tratamiento de Datos Personales

Corresponde a las Unidades Administrativas la elaboración y documentación adecuada y completa de su inventario de datos personales y el ciclo de vida de estos, conforme a los formatos elaborados por la Unidad de Transparencia para tales efectos, así como su actualización continua.

El inventario de los datos personales y su ciclo de vida formarán parte del Documento de Seguridad del Instituto, y se encontrarán disponibles para consulta en el Apartado Virtual de Protección de Datos Personales, en el sitio web del Instituto, protegiendo la información de naturaleza reservada o confidencial.

señalado en el aviso de privacidad y en cumplimiento a las disposiciones previstas en la LGPDPPSO, los Lineamientos Generales y demás normativa derivada y aplicable.

[6] Por "responsabilidad proactiva y demostrada" se entenderá que el IFT asume y reconoce su responsabilidad en el cumplimiento a lo dispuesto en la LGPDPPSO, los Lineamientos Generales y demás normativa derivada y aplicable, implementando las medidas administrativas, físicas y técnicas apropiadas a fin de garantizar que el tratamiento es conforme a la LGPDPPSO y los Lineamientos Generales, demostrando dicho cumplimiento documentalmente a través de los medios y mecanismos que el INAI establezca, activamente y de manera continua.

Las personas servidoras públicas que traten datos personales, tienen la obligación de conocer su inventario de datos personales y el ciclo de vida de estos, así como los procesos de tratamiento y el contexto del tratamiento de los datos personales que lleven a cabo o se encuentren a su cargo, en los cuales participen directa o indirectamente, a efecto de llevar a cabo evaluaciones de riesgos continuas que le permitan al Instituto, en su carácter de responsable, identificar y priorizar los factores de riesgo a los que se encuentran expuestos los datos personales, y los derechos y las libertades de las personas titulares.

El Instituto tiene el deber de identificar, conocer y documentar los procesos de tratamiento de datos personales que se lleven a cabo en su nombre y por su cuenta, efectuados por sus encargados y/o prestadores de servicios que no tengan tal carácter, sea que se trate de personas físicas o morales, de carácter nacional o internacional.

IX. Gobierno de Datos

El Instituto deberá desarrollar e implementar la estructura de gobierno de datos, entendido como el proceso por el que se definen políticas y procedimientos para garantizar una gestión de datos personales proactiva y efectiva, permitiendo una comprensión continua de las prioridades en la administración de los riesgos de la organización, en el tratamiento de los datos personales que se encuentran en su posesión.

X. Control Interno

Para asegurar una gestión y tratamiento adecuados de los datos personales en posesión del Instituto es indispensable establecer controles adecuados a partir de una correcta identificación de factores de riesgos (causas), que pudieran afectar el cumplimiento de los principios y deberes en el tratamiento de los datos personales que se encuentran en su posesión, así como los derechos de las personas titulares, de manera eficiente y sin

dilación indebida evitando cualquier tipo de vulneración como las que se mencionan a continuación:

I. La pérdida o destrucción no autorizada;

II. El robo, extravío o copia no autorizada;

III. El uso, acceso o tratamiento no autorizado, o

IV. El daño, la alteración o modificación no autorizada

Asimismo, los controles establecidos deberán supervisarse con finalidad de verificar su eficiencia y eficacia.

XI. Comunicación

El Instituto deberá desarrollar e implementar las actividades apropiadas para permitir que su personal tenga una comprensión adecuada sobre los principios, deberes y obligaciones establecidos en la LGPDPPSO, los Lineamientos Generales y demás normativa aplicable.

Deberá favorecerse y fomentarse el diálogo entre las Unidades Administrativas sobre cómo se procesan los datos personales y los factores de riesgos asociados a estos, para administrar los riesgos de manera efectiva.

XII. Protección Adecuada

El Instituto deberá desarrollar, establecer e implementar medidas, mecanismos y salvaguardas apropiadas para el tratamiento de los datos personales, que permitan prevenir y reaccionar frente a incidentes o vulneraciones en procesos automatizados relacionados con la ciberseguridad, o no automatizados (manuales), teniendo en cuenta la superposición entre la privacidad de las personas titulares, la protección de sus datos personales y la administración de riesgos en el Instituto.

XIII. Procesos y Sistemas de Información Críticos

Le corresponde a cada Unidad Administrativa del Instituto identificar los procesos, sistemas de información, aplicativos y bases de datos personales que tengan un carácter crítico, teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento, así como el riesgo para las personas físicas titulares de los datos, sus derechos y libertades.

XIV. Principios y Deberes

En la gestión y tratamiento de datos personales las personas servidoras públicas del Instituto deberán observar los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad, así como los deberes de seguridad y confidencialidad previstos en la LGPDPPSO, los Lineamientos Generales, y demás disposiciones aplicables.

Las personas servidoras públicas que tengan personal a su cargo, además deberán supervisar el cumplimiento de dichos principios y deberes por parte de las personas servidoras públicas sujetas a su dirección y adoptar las medidas necesarias para su debida aplicación.

1. Principio de Licitud

El tratamiento de los datos personales por parte de las personas servidoras públicas del Instituto deberá realizarse exclusivamente conforme a las facultades o atribuciones que la normatividad aplicable les confiera.

Las personas servidoras públicas del Instituto deberán identificar aquellos ordenamientos o las disposiciones jurídicas específicas que tengan un impacto en el tratamiento de los datos personales, a efecto de aplicar los principios y deberes en el tratamiento de acuerdo al contexto en que éste surja y se efectúe.

2. Principio de Finalidad

El tratamiento de datos personales que efectúen las personas servidoras públicas del Instituto deberá realizarse conforme a finalidades concretas, lícitas, explícitas y legítimas, relacionadas con las atribuciones que la normatividad aplicable les confiera.

Cuando la legislación aplicable no prevea de manera expresa la finalidad del tratamiento de los datos, y ésta se entienda o considere implícita o derivada de alguna atribución o facultad expresa, las personas servidoras públicas del Instituto deberán verificar que el tratamiento sea, en efecto, conforme a la legislación aplicable, cumpliendo de manera íntegra con los demás principios y deberes del tratamiento.

Sólo podrán tratarse datos personales para finalidades distintas, cuando dicho tratamiento sea conforme a las atribuciones legales de las personas servidoras públicas, el objetivo constitucional y legal del Instituto, o medie el consentimiento de la persona titular, con excepción de aquellas hipótesis previstas en los artículos 22 y 70 de la LGPDPPSO.

3. Principio de Lealtad

Las personas servidoras públicas del Instituto no deberán obtener y tratar datos personales, a través de medios engañosos o fraudulentos para lo que deberán privilegiar la protección de los intereses de la persona titular, así como su expectativa razonable de privacidad.

4. Principio de Consentimiento

El tratamiento de los datos personales por parte de las personas servidoras públicas del Instituto deberá realizarse con el consentimiento del titular, cuando resulte procedente, de conformidad con las disposiciones previstas en la LGPDPPSO y los Lineamientos Generales, teniendo en cuenta las excepciones previstas en las disposiciones jurídicas antes mencionadas.

Las personas servidoras públicas deberán determinar caso por caso, si el consentimiento de las personas titulares constituye o no la base jurídica del tratamiento de los datos personales, considerando que, según lo dispuesto por los ordenamientos aplicables, el consentimiento deberá obtenerse de manera libre, específica, informada e inequívoca (condiciones de validez).

La difusión de imágenes concernientes a personas físicas que no tengan el carácter de personas servidoras públicas, en sitios web o redes sociales que lleven a cabo las Unidades Administrativas del Instituto, sea que se encuentren asociadas o no a audio y/o video, requerirá la obtención del consentimiento expreso y por escrito de la persona titular de los datos, desde el momento en que estos se recaben con la finalidad de difusión, divulgación o comunicación correspondiente.

En la obtención del consentimiento expreso y por escrito, que tenga como finalidad ulterior, la difusión de imágenes en sitios web o redes sociales, deberá utilizarse un lenguaje apropiado de conformidad con la categoría o categorías de personas titulares de los datos personales involucradas, señalando de manera clara y específica los efectos o consecuencias de otorgar el consentimiento, así como los riesgos potenciales a los que podrían estar expuestos los datos personales en sitios o plataformas administradas por terceros, externos al Instituto.

Corresponderá a las Unidades Administrativas acreditar que el consentimiento fue obtenido satisfaciendo todas las condiciones para su validez, así como documentar su obtención para efectos de rendición de cuentas frente a la persona titular y al INAI, según corresponda.

5. Principio de Calidad

Las personas servidoras públicas deberán adoptar las medidas necesarias para mantener exactos, completos, correctos y actualizados los datos personales en su posesión, a fin de que no se altere la veracidad de éstos.

Cuando las personas servidoras públicas detecten, identifiquen o tengan conocimiento de que los datos personales que se encuentran en su posesión no son exactos, no se encuentran completos, correctos o actualizados, deberán realizar esfuerzos razonables para garantizar que los datos personales cumplan con el principio de calidad.

Cuando los datos personales que se recaben hayan dejado de ser necesarios para las finalidades que motivaron su tratamiento, deberán ser suprimidos (eliminados), previo bloqueo, conforme a lo previsto en la LGPDPPSO, los Lineamientos Generales y las disposiciones aplicables emitidas por el Área Coordinadora de Archivos del Instituto.

Para determinar los plazos de conservación correspondientes a los datos personales, deberá atenderse lo establecido en el Catálogo de Disposición Documental y demás instrumentos vigentes, considerando los valores primarios y secundarios.

6. Principio de Proporcionalidad

En el ejercicio de las atribuciones y funciones que impliquen un tratamiento de datos personales, y en particular, en los trámites, convocatorias, concursos, procesos y procedimientos que correspondan a las Unidades Administrativas del Instituto, las personas servidoras públicas deberán tratar los datos personales que resulten adecuados, relevantes y estrictamente necesarios para la finalidad que justifica su tratamiento, realizando esfuerzos razonables, conforme al criterio de minimización, para limitar los datos personales tratados (cantidad) al mínimo necesario, así como la duración del tratamiento (temporalidad), con relación a las finalidades que motivan su tratamiento.

Corresponderá a las Unidades Administrativas del Instituto analizar, identificar, establecer y determinar la cantidad de datos personales y la temporalidad mínima del tratamiento de estos, en función de las atribuciones que se ejerzan y la finalidad que justifique el tratamiento de los datos personales.

Cuando se adopten o establezcan formatos para trámites o campos en el diseño de sistemas de información o aplicaciones informáticas, el Área que coordine su puesta en operación, deberá asegurarse que únicamente se recaben los datos personales estrictamente necesarios, procurando en todo momento cumplir con el criterio de minimización, a efecto de recabar la menor cantidad de datos personales posible.

7. Principio de Información

Las personas servidoras públicas del Instituto deberán informar a las personas titulares la existencia y características principales del tratamiento al que serán sometidos sus datos personales, a través de los correspondientes avisos de privacidad.

Todos y cada uno de los tratamientos de datos personales que efectúen las Unidades Administrativas del Instituto deberán ser documentados e informados o puestos a disposición de la persona titular, a través del aviso de privacidad correspondiente.

Las Unidades Administrativas serán responsables de la elaboración y actualización periódica de los avisos de privacidad que conciernan a los procesos de tratamiento de datos personales que efectúen, de conformidad con el inventario de datos personales y los sistemas de tratamiento que tengan establecidos, utilizando los formatos aprobados por el Comité de Transparencia.

Las Unidades Administrativas deberán remitir a la Unidad de Transparencia, los avisos de privacidad actualizados para su publicación en el Apartado Virtual de Protección de Datos Personales, que se encontrará disponible en el sitio web del Instituto.

Con independencia de lo previsto en el párrafo anterior, es responsabilidad de las Unidades Administrativas del Instituto, poner a disposición de manera oportuna y a través de los medios y formatos pertinentes (físicos, electrónicos o en cualquier formato generado por el Instituto), en función de las categorías de personas titulares de que se trate, el o los avisos de privacidad actualizados que correspondan, a partir del momento en el cual se recaben los datos personales.

8. Principio de Responsabilidad

El Instituto actuará conforme al principio de la responsabilidad proactiva y demostrada en el cumplimiento de los principios, deberes y obligaciones establecidos en la LGPDPPSO, los Lineamientos Generales y demás normativa derivada.

El Instituto rendirá cuentas sobre el tratamiento de los datos personales que se encuentran en su posesión a la persona titular de los datos y al INAI, a través de los mecanismos y modalidades que éste último establezca.

El Instituto podrá valerse de estándares o mejores prácticas nacionales o internacionales en materia de protección de datos personales, seguridad de la información y la administración de riesgos, para cumplir con los principios, deberes y obligaciones establecidos en la legislación aplicable, siempre y cuando no se contrapongan con lo previsto en la normativa mexicana de la materia.

Todas las Unidades Administrativas del Instituto tienen la obligación de participar y colaborar activamente en la elaboración, generación y actualización de los insumos y la evidencia documental que permita acreditar el cumplimiento de los principios,

deberes y obligaciones establecidos en la LGPDPPSO, los Lineamientos Generales, y demás normativa derivada y aplicable, bajo la coordinación y supervisión del Comité de Transparencia, en su carácter de autoridad máxima en la materia.

El tratamiento de los datos personales efectuado por el Instituto, en su carácter de responsable, es el resultado y la suma de los tratamientos de datos que efectúe cada una de las Unidades Administrativas del Instituto, a través de las personas servidoras públicas correspondientes, personas prestadoras de servicio social y/o prácticas profesionales.

La responsabilidad de cumplir y demostrar el cumplimiento de los principios, deberes y obligaciones establecidos en la LGPDPPSO, los Lineamientos Generales y demás normativa derivada, en el ejercicio de sus funciones y atribuciones, corresponde a todas y cada una de las personas involucradas en el tratamiento de los datos personales, con independencia de las atribuciones conferidas al Comité de Transparencia y a la Unidad de Transparencia, en términos de lo dispuesto en los artículos 84 y 85 de la LGPDPPSO.

Los mecanismos con los que cuente el Instituto para cumplir con el principio de responsabilidad establecido en la LGPDPPSO y los Lineamientos Generales, se publicarán y encontrarán permanentemente disponibles y actualizados en el Apartado Virtual de Protección de Datos Personales, en la sección de "Información relevante".

XV. Deber de Seguridad

El Instituto establecerá el conjunto de medidas de seguridad (acciones, actividades o mecanismos administrativos, técnicos y físicos), que permitan mitigar la probabilidad e impacto de la materialización respecto de la pérdida o destrucción no autorizada; el robo, extravío o copia no autorizada; el uso, acceso o tratamiento no autorizado, o el daño, la alteración o modificación no autorizada.

Las medidas de seguridad de carácter administrativo, físico, técnico o electrónicas adoptadas por el Instituto deberán ser apropiadas para garantizar un nivel de seguridad adecuado al riesgo al que se encuentren expuestos los datos personales, teniendo en cuenta la sensibilidad de los datos personales tratados, el desarrollo tecnológico, las posibles consecuencias de una vulneración para los titulares, 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, así como para garantizar su confidencialidad, integridad y disponibilidad.

1. Medidas de seguridad administrativas

El Instituto establecerá las 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.

2. Medidas de seguridad técnicas

El Instituto establecerá el 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, con el propósito de desarrollar una cultura laboral que permita alcanzar niveles óptimos de rendimiento, de seguridad de los recursos tecnológicos del Instituto y de protección de la información reservada, confidencial y datos personales que estos recursos almacenan, procesan y/o transfieren.

3. Medidas de seguridad físicas

El Instituto establecerá un conjunto de acciones y mecanismos para proteger el entorno físico de la información que integra los expedientes y de los recursos involucrados en su tratamiento, los cuales, entre otros, consisten en:

1) Sistema de video vigilancia, definido como la integración de sistemas de administración, grabación, área de monitoreo, respaldo de energía, infraestructura de interconexión y cámaras digitales IP con aplicación de analíticos, colocadas en lugares estratégicos al interior y exterior de los inmuebles, que permiten comprobar de forma remota el estado de los inmuebles y de los bienes del Instituto.

2) Sistema contra incendios, integrado por un sistema a base de agua ya que es un sistema compuesto por un conjunto de tuberías, dispositivos y accesorios interconectados entre sí desde una estación de bombeo hasta dispositivos como rociadores, hidrantes, gabinetes contra incendio, extintores, tableros de control, sirenas, estrobos, detectores de humo y temperatura, lo que permite salvaguardar a las personas y los bienes propiedad del instituto.

3) Servicio de Vigilancia intramuros, como parte de las medidas de seguridad de los bienes muebles e inmuebles del Instituto, se cuenta con un estado de fuerza de elementos de diferentes rangos, entre Oficiales, Policías Primero, Policía Segundo, Policía Razo debidamente armados y capacitados para salvaguardar la integridad de las personas servidoras públicas y visitantes, así como los bienes del Instituto.

4) Archivos móviles de alta densidad, fundamentales para la preservación y conservación de la información que integra los expedientes.

5) Procedimiento de consulta, préstamo y seguimiento interno de los expedientes, consistente en llevar un registro de firmas actualizado de las personas servidoras públicas, autorizadas por las personas Titulares de cada Unidad Administrativa, para solicitar expedientes en consulta o préstamo.

Por último, el Instituto establecerá un conjunto de controles físicos incluyendo aquellos controles que permitan proteger los recursos tecnológicos institucionales contra el robo y acceso no autorizado.

4. Documento de Seguridad

El Instituto contará con un Documento de Seguridad, el cual incluirá los elementos mínimos requeridos por el artículo 35 de la LGPDPPSO y los Lineamientos Generales. El Documento de Seguridad será elaborado teniendo en cuenta el ciclo de vida de los datos personales que se encuentran en posesión de las distintas Unidades Administrativas del Instituto.

El Comité de Transparencia coordinará la elaboración e integración del Documento de Seguridad del Instituto. Las Unidades Administrativas coadyuvarán de manera activa elaborando los insumos necesarios para su integración, así como proporcionando la información que permita su integración, según se requiera, para incluir de manera completa y actualizada los elementos a los que hace referencia el artículo 35 de la LGPDPPSO.

El Documento de Seguridad será actualizado de manera continua como resultado de un proceso de mejora continua, derivado del monitoreo y revisión del Sistema de Gestión de Seguridad de Datos Personales. Lo anterior, sin perjuicio de los supuestos previstos en el artículo 36 de la LGPDPPSO.

En la elaboración y actualización del Documento de Seguridad participarán, cuando menos, las personas servidoras públicas que cuenten con el perfil especializado en protección de datos personales, control de riesgos, seguridad de la información y archivo.

XVI. Deber de Confidencialidad

Las personas servidoras públicas del Instituto deberán guardar la confidencialidad de los datos personales a los que tengan acceso en el ejercicio de sus funciones y atribuciones. Lo anterior, sin perjuicio del cumplimiento de las disposiciones en materia de transparencia y acceso a la información pública.

Corresponde a la Unidad de Administración el establecimiento de los controles o mecanismos que tengan por objeto comunicar y asegurar el deber de confidencialidad por parte de las personas servidoras públicas, desde el inicio del proceso de su contratación, y de manera previa a que se les otorgue el acceso, de manera enunciativa pero no limitativa, a sistemas, bases de datos, expedientes, aplicativos o plataformas informáticas que permitan el tratamiento de datos personales.

Sin perjuicio de lo previsto en el párrafo anterior, los Titulares de las Unidades Administrativas podrán establecer controles o mecanismos específicos de confidencialidad, en función de la naturaleza, el ámbito, el contexto y los fines del tratamiento, el riesgo al que se encuentren expuestos los datos personales, así como el riesgo para los derechos y libertades de las personas físicas.

XVII. Derechos ARCOP

El Instituto garantizará sin dilación indebida los derechos de acceso, rectificación, cancelación y oposición, así como el derecho a la portabilidad de datos personales, los cuales se tramitarán de acuerdo con el Procedimiento Interno establecido para tal efecto por la Unidad de Transparencia, el cual será aprobado por el Comité de Transparencia, y será conforme a lo dispuesto en la LGPDPPSO, los Lineamientos Generales y los Lineamientos de Portabilidad.

Las Unidades Administrativas del Instituto tienen la obligación de conocer y aplicar el Procedimiento Interno para garantizar el ejercicio de los derechos de acceso,

rectificación, cancelación y oposición, así como el derecho a la portabilidad de datos personales, en el tramo de responsabilidad que les corresponda conforme a dicho Procedimiento.

El Comité de Transparencia coordinará el diseño, el establecimiento o la adopción de formatos y guías orientativas que permitan a las personas titulares o a sus representantes, el ejercicio efectivo de los derechos de acceso, rectificación, cancelación y oposición, así como el derecho de portabilidad, con el apoyo de las Unidades Administrativas. Los formatos y guías se encontrarán disponibles en el Apartado Virtual de Protección de Datos Personales.

Las Unidades Administrativas del Instituto coadyuvarán en todo momento con la Unidad de Transparencia, proporcionando el apoyo necesario para salvaguardar los derechos de los titulares y otorgando la mayor protección posible a los mismos.

XVIII. Transferencias

Toda transferencia de datos personales que efectúen las Unidades Administrativas del Instituto, sea ésta nacional o internacional, se encuentra sujeta al consentimiento de su titular, salvo las excepciones previstas en los artículos 22, 66 y 70 de la LGPDPPSO.

Las Unidades Administrativas deberán identificar y registrar en su inventario de datos personales y de sistemas de tratamiento, así como en el ciclo de vida que corresponda, las transferencias nacionales o internacionales que lleven a cabo, conforme a los formatos de inventario y ciclo de vida elaborados por la Unidad de Transparencia.

El deber de formalizar y documentar las transferencias de datos personales en el Instituto, se acotará a los supuestos no previstos en el artículos 66 de la LGPDPPSO, en cuyo caso, las Unidades Administrativas deberán documentar mediante la suscripción de cláusulas contractuales, convenios de colaboración o cualquier otro instrumento jurídico, de

manera conjunta con la Unidad de Administración, las transferencias nacionales o internacionales que lleven a cabo, a efecto de demostrar el alcance del tratamiento de los datos personales, así como las obligaciones y responsabilidades asumidas por las partes.

En toda transferencia de datos personales que realicen las personas servidoras públicas del Instituto, deberán comunicar al receptor de los datos personales el aviso de privacidad conforme al cual se tratan los datos personales frente a la persona titular, poniendo a disposición el aviso de privacidad integral o simplificado, o bien, remitiendo el vínculo electrónico que dirija al aviso de privacidad que corresponda, disponible en el Apartado Virtual de Protección de Datos Personales.

XIX. Encargados

El Instituto deberá identificar de manera razonable, mediante la realización de un análisis adecuado, a las personas físicas o jurídicas que actúen como encargados del tratamiento.

Cuando se pretenda realizar un tratamiento de datos personales por cuenta del Instituto, en su carácter de responsable, éste elegirá únicamente un encargado o encargados que ofrezcan garantías suficientes para aplicar medidas físicas, técnicas y administrativas apropiadas, de manera que el nivel de protección de los datos personales sea adecuado, conforme, equiparable o superior al previsto en la LGPDPPSO, los Lineamientos Generales y demás normativa derivada y aplicable.

El Instituto deberá adoptar medidas razonables que le permitan verificar que las personas físicas o morales que actúen como prestadoras de servicios, sea que actúen con el carácter de encargados o no, cumplan con los principios y deberes en el tratamiento de los datos personales, además de que deberá quedar expresamente señalado el

conocimiento y aceptación de las presentes Políticas por parte del responsable, y su encargado o encargados.

La relación que se establezca entre el Instituto, en carácter de responsable, y su encargado o encargados, sea que se trate de personas físicas o morales, de carácter público o privado, deberá formalizarse mediante contrato o cualquier otro instrumento jurídico que decida el Instituto, que permita acreditar la existencia, el alcance y el contenido de la relación jurídica.

Sin perjuicio de que, en la formalización de la relación jurídica entre el Instituto y su encargado o encargados, se observe lo dispuesto en el Título Cuarto de la LGPDPPSO, y el Título Cuarto de los Lineamientos Generales, el contrato o instrumento jurídico que se adopte entre ellos, deberá considerar el contexto particular del tratamiento de los datos personales, adoptando, según sea el caso, cláusulas, mecanismos, salvaguardas o medidas adicionales que permitan asegurar que el tratamiento efectuado por el encargado, a nombre y por cuenta del Instituto, se encuentra adecuado, es conforme, equiparable o superior al nivel de protección previsto en la legislación mexicana en la materia.

XX. Evaluaciones de Impacto en la Protección de Datos Personales

En caso de que las Unidades Administrativas del Instituto pretendan 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, en términos de lo dispuesto en los artículos 75 y 76 de la LGPDPPSO, deberán realizar una Evaluación de impacto en la protección de datos personales, y presentarla a la Unidad de Transparencia, a efecto de que ésta la remita al INAI, quien podrá emitir recomendaciones no vinculantes especializadas en la materia de protección de datos personales.

Cuando dos o más Unidades Administrativas participen en la puesta en operación o modificación de políticas públicas, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que impliquen el tratamiento intensivo o relevante de datos personales, la Evaluación de impacto en la protección de datos personales deberá ser elaborada conjuntamente, a efecto de realizar un análisis integral que permita cumplir con las Disposiciones administrativas de carácter general para la elaboración, presentación y valoración de evaluaciones de impacto en la protección de datos personales.

La elaboración de una Evaluación de impacto en la protección de datos personales será particularmente exigible cuando sea probable que un tipo de tratamiento, en particular si 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.

Las Unidades Administrativas deberán monitorear continuamente los riesgos que se originan como resultado de sus actividades de tratamiento, con el objeto de identificar cuándo llevan a cabo un tratamiento intensivo y relevante, a efecto de determinar la probabilidad de que un determinado tipo de tratamiento de datos representa un **riesgo alto** para los derechos y las libertades de las personas titulares de los datos personales.

La Unidad de Transparencia proporcionará el apoyo y la orientación necesarias, a petición de las Unidades Administrativas, con el objeto de que estas cumplan con su obligación de elaborar en tiempo y forma la Evaluación de impacto en la protección de datos personales que corresponda.

XXI. Gestión de Incidentes y Vulneraciones de Seguridad

La gestión y notificación de vulneraciones de seguridad de los datos personales deberá efectuarse de acuerdo al Plan de Respuesta de Incidentes, el cual preverá las fases de

preparación, identificación, contención, erradicación, recuperación y lecciones aprendidas.

XXII. Notificación de Vulneraciones de Seguridad

En caso de que ocurra una vulneración a la seguridad de los datos personales que sean objeto de un tratamiento manual o no automatizado, la Unidad Administrativa que tenga conocimiento sobre la misma, deberá notificar su ocurrencia a través de la presentación de un informe suscrito por la persona Titular del Área, al Comité de Transparencia, analizando y documentando las causas por las cuales se presentó.

Cuando la vulneración a la seguridad de los datos personales ocurra en sistemas de información o en la infraestructura tecnológica del Instituto, administrada por la DGTIC o por parte de terceros, la Unidad Administrativa que detecte su ocurrencia, o bien, la propia DGTIC en caso de que ésta la hubiere identificado, deberá notificar al Comité de Transparencia, a través de la presentación de un informe suscrito por la persona Titular del Área, analizando y documentando las causas por las cuales se presentó.

En cualquiera de los supuestos anteriores, la documentación y la notificación al Comité de Transparencia, de las causas que originaron la vulneración, deberá realizarse dentro de un plazo no mayor a cuarenta y ocho (48) horas consecutivas, contadas a partir de que se confirme que ocurrió la vulneración, incluyendo la información que resulte necesaria para comprender el origen, el alcance, el impacto y las consecuencias probables de la vulneración para las personas titulares de los datos y para el Instituto.

En cuanto se confirme que ocurrió la vulneración a la seguridad de los datos personales, la Unidad Administrativa involucrada deberá tomar las acciones encaminadas a detonar un proceso de revisión exhaustiva (identificación, contención, erradicación y recuperación) de la magnitud de la afectación.

Si con motivo de la revisión exhaustiva se determina que la vulneración a la seguridad de los datos personales afecta de forma significativa los derechos patrimoniales o morales de las personas titulares, la Unidad Administrativa que hubiese detectado la vulneración, o bien, la DGTIC, dependiendo de si se trata de una vulneración que haya tenido como objeto datos personales sujetos a un tratamiento no automatizado (manual) o automatizado, deberá notificar su ocurrencia a través de la Unidad de Transparencia a la persona titular y al INAI, dentro de un plazo máximo de setenta y dos (72) horas consecutivas, contadas a partir de que se confirme la ocurrencia de la vulneración de seguridad, y la Unidad Administrativa o la DGTIC, según corresponda, haya empezado a tomar las acciones encaminadas a detonar un proceso de mitigación de la afectación.

La notificación de la ocurrencia de la vulneración deberá contener, cuando menos, los elementos previstos en los artículos 41 de la LGPDPPSO, y 67 y 68 de los Lineamientos Generales, a fin de que las personas titulares afectadas puedan tomar las medidas correspondientes para la defensa de sus derechos.

XXIII. Apartado Virtual de Protección de Datos Personales

El Instituto habilitará un micrositio en su sitio web, denominado "Apartado Virtual de Protección de Datos Personales", para consulta de la ciudadanía y las personas servidoras públicas del Instituto, el cual contendrá y concentrará la información relativa a los Avisos de Privacidad aplicables a los tratamientos de los datos personales en posesión del Instituto, los Datos de Contacto de la Unidad de Transparencia, así como diversa Información Relevante en materia de protección de datos personales, la cual será publicada de conformidad con los formatos aprobados por el INAI.

Corresponde a la Unidad de Transparencia la coordinación de las acciones necesarias para la creación, publicación, mantenimiento y actualización del Apartado Virtual de Protección de Datos Personales. Las Unidades Administrativas proporcionarán a la

Unidad de Transparencia el apoyo y los insumos necesarios que permitan la creación, puesta en operación y actualización continua del Apartado Virtual.

XXIV. Grupo de Trabajo de Protección de Datos Personales

El Instituto contará con un Grupo de Trabajo de Protección de Datos Personales conformado por personal especializado en temas de protección de datos personales, seguridad de la información, control interno, administración de riesgos y archivo. El Grupo de Trabajo se integrará y operará de conformidad con las Reglas que para el efecto se establezcan por el Comité de Transparencia.

El Grupo de Trabajo fungirá como un mecanismo permanente de monitoreo y revisión de las acciones, medidas y controles previstos en el Documento de Seguridad, así como uno de los componentes centrales del sistema de supervisión y vigilancia interna para comprobar el cumplimiento de las políticas y programas de protección de datos personales.

XXV. Subenlaces de Transparencia y Protección de Datos Personales

Las Unidades Administrativas designarán a una persona que funja como Subenlace de Transparencia y Protección de Datos Personales, quien será el vínculo entre las Áreas, la Unidad de Transparencia y el Comité de Transparencia, y quien auxiliará a la persona Titular de Unidad Administrativa en el cumplimiento de las obligaciones en materia de protección de datos personales y acceso a la información que correspondan a su Unidad Administrativa.

Las y los Subenlaces de Transparencia y Protección de Datos Personales deberán tener como mínimo el nivel jerárquico de Dirección de Área o su equivalente, y serán designados/as mediante oficio emitido por la persona Titular de Unidad Administrativa, dirigido a la persona Titular de la Unidad de Transparencia.

XXVI. Evaluación del Desempeño

El Instituto deberá evaluar el desempeño y la eficacia del Sistema de Gestión de Seguridad de Datos Personales. Para tal efecto, el Instituto deberá determinar:

1. Cuándo se debe llevar a cabo el seguimiento y la medición;
2. Quién debe hacer el seguimiento y la medición;
3. Cuándo se debe analizar y evaluar los resultados del seguimiento y la medición, y
4. Quién debe analizar y evaluar esos resultados.

El Instituto debe conservar la información documentada adecuada como evidencia de los resultados.

XXVII. Auditorías Externas y/o Internas

El Instituto deberá llevar a cabo auditorías internas y/o externas a intervalos planificados, para proporcionar información acerca de si el Sistema de Gestión de Seguridad de Datos Personales se encuentra implementado y es mantenido de manera eficaz.

XXVIII. Mejora Continua

El Instituto deberá mejorar de manera continua la idoneidad, adecuación y eficacia mediante el establecimiento de acciones de mejora que atiendan las áreas de oportunidad identificadas en el Sistema de Gestión de Seguridad de Datos Personales.

XXIX. Sanciones

Cualquier incumplimiento a esta Política 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.

Fuentes de Consulta

Legislación

- Cámara de Diputados (2017), *Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados*, México. Publicada en el Diario Oficial de la Federación (DOF) el 26 de enero de 2017. Disponible para consulta en el vínculo electrónico: https://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPPSO.pdf

- Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (2018), *Lineamientos Generales de Protección de Datos Personales para el Sector Público*, México. Publicados en el DOF el 26 de enero de 2018. Disponibles para consulta en el vínculo electrónico: https://inicio.inai.org.mx/AcuerdosDelPleno/ACT-PUB-19-12-2017.10.pdf

Otros documentos

- Asociación Española de Normalización – UNE Normalización Española (2021), *UNE-EN ISO/IEC 27701 (Extensión de las Normas ISO/IEC 27001 e ISO/IEC 27002 para la Gestión de Privacidad de la Información, Requisitos y Directrices (ISO/IEC 27701:2019))*, Madrid, España, 90 pp.

- Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (2022), *Recomendaciones para la Elaboración de Políticas Internas de Gestión y Tratamiento de Datos Personales (Sector Público)*, México, 42 pp. Disponibles para consulta en el vínculo electrónico: https://home.inai.org.mx//wp-content/documentos/DocumentosSectorPublico/RecomendacionesPol%C3%ADticasPDP.pdf

Fuentes de Consulta
• National Institute of Standards and Technology (2020), *NIST Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management (Version 1.0)*, U.S. Department of Commerce, 43 pp. Disponible para consulta en el vínculo electrónico: https://www.nist.gov/system/files/documents/2020/01/16/NIST%20Privacy%20Framework_V1.0.pdf • Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE, (Reglamento General de Protección de Datos), OJ 2016 L 119/1. Disponible para consulta en el vínculo electrónico: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32016R0679

Control de cambios			
Fecha	**Autor**	**Versión**	**Referencia del cambio**
09 de octubre de 2018[7]	Comité de Transparencia	1.0	Creación del Documento
16 de diciembre de 2022[8]	Comité de Transparencia	2.0	Actualización del Documento

[7] Aprobada en la Octava Sesión Extraordinaria del Comité de Transparencia, celebrada el 09 de octubre de 2018, mediante el Acuerdo número 08/SE/01/18.
[8] Aprobada en la Vigésima Novena Sesión Extraordinaria del Comité de Transparencia, celebrada el 16 de diciembre de 2022, mediante el Acuerdo número 29/SE/27/22.

Elabora	Revisa	Autoriza
_____ **Julio Alberto Huerta Anguiano** Director de Clasificación y Datos Personales	_____ **Alejandra Martínez Morales** Coordinadora de Transparencia, Acceso a la Información y Gobierno Abierto	_____ **Alejandra Martínez Morales** Coordinadora de Transparencia, Acceso a la Información y Gobierno Abierto, Presidenta Suplente del Comité de Transparencia _____ **José Luis Mancilla Rosales** Director General de Instrumentación de la Unidad de Asuntos Jurídicos, Integrante Suplente del Comité de Transparencia _____ **Héctor Jandette Fuentes** Director de Asesoría Jurídica de la Unidad de Administración, Integrante Suplente del Comité de Transparencia