PROGRAMA DE PROTECCIÓN DE DATOS PERSONALES DE LA COMISIÓN REGULADORA DE TELECOMUNICACIONES

CONTENIDO

I. PRESENTACIÓN

La protección de los datos personales es un derecho humano, reconocido por diversos instrumentos legales y normativos en México, a favor de todas las personas, con independencia de su origen étnico, género, edad, religión, estado civil, o cualquier otra condición o situación que pueda atentar contra su dignidad y/o afectar sus derechos y libertades fundamentales.

La Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados dicta los principios y deberes que rigen la protección de los datos personales, y determina que cualquier autoridad, entidad, órgano y organismo de los poderes ejecutivo, legislativo y judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos, en el ámbito federal, estatal y municipal o de las demarcaciones territoriales de la Ciudad de México, son sujetos obligados de esta Ley.

En este contexto, vale la pena traer a colación que, de conformidad con los artículos 7 y 8 del *Decreto por el que se expide la Ley en Materia de Telecomunicaciones y Radiodifusión y se abroga la Ley Federal de Telecomunicaciones y Radiodifusión* se crea la Comisión Reguladora de Telecomunicaciones como el órgano administrativo desconcentrado de la Agencia de Transformación Digital y Telecomunicaciones, dotada de independencia técnica, operativa y de gestión, cuyo objeto es garantizar el desarrollo eficiente de las telecomunicaciones y la radiodifusión.

En ese sentido, la Comisión Reguladora de Telecomunicaciones es el sujeto obligado y responsable en el tratamiento de datos personales, que recabe en el ámbito de sus funciones y atribuciones, y tiene el deber de implementar medidas administrativas, físicas y técnicas necesarias para proteger los datos personales a los que da tratamiento, contra daños, pérdidas, alteraciones, uso o acceso no autorizado.

En esa tesitura, el artículo 23 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados prevé la obligación de implementar mecanismos para acreditar el cumplimiento de los principios, deberes y obligaciones establecidos en la misma y rendir cuentas sobre el tratamiento de datos personales en su posesión a la persona titular, a la Secretaría Anticorrupción y Buen Gobierno o a las Autoridades garantes, según corresponda. Asimismo, el artículo 24, fracción II, del mismo ordenamiento, contempla el principio de responsabilidad y la necesidad de adoptar mecanismos que aseguren su cumplimiento, entre ellos, la elaboración de políticas y programas de protección de datos personales que sean obligatorios y exigibles al interior de la organización.

En tal sentido, en cumplimiento a lo establecido en los artículos 24, fracciones I y II de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, así como el artículo 47 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público, la Comisión Reguladora de Telecomunicaciones presenta su Programa de Protección de Datos Personales, en el

que se definen las directrices que deben guiar el actuar de las Unidades administrativas en apego a los principios y deberes en la protección de los datos personales.

En ese orden de ideas, el Programa de Protección de Datos Personales se concibe como un instrumento de política interna para establecer un Sistema Integral de Gestión de Datos Personales, entendido este, en términos de lo señalado en el artículo 28 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, como el conjunto de elementos y actividades interrelacionadas para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el tratamiento de datos personales y la seguridad de los mismos.

Así, el presente Programa de Protección de Datos Personales, permite direccionar, operar y prever los controles para el tratamiento del dato personal, así como establecer las bases para la gestión sistemática y continua de los datos bajo resguardo, con el propósito de prevenir riesgos, garantizar el cumplimiento de las disposiciones normativas aplicables y promover la cultura de responsabilidad en el tratamiento de datos personales, con miras al fortalecimiento de la seguridad, integridad y confidencialidad de los datos personales bajo resguardo de la Comisión Reguladora de Telecomunicaciones.

II. DEFINICIONES

I. **Aviso de privacidad:** el documento que se pone a disposición de la persona titular de la información 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;

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

III. **Bloqueo:** la identificación y conservación de datos personales una vez cumplida la finalidad para la cual fueron recabados, con el único propósito de determinar posibles responsabilidades en relación con su tratamiento, hasta el plazo de prescripción legal o contractual de éstas;

IV. **Comisión:** la Comisión Reguladora de Telecomunicaciones;

V. **Comité de Transparencia:** el Comité de Transparencia de la Comisión es el órgano colegiado al que hace referencia el artículo 39 de la Ley General de Transparencia y Acceso a la Información Pública; encargado de aprobar las determinaciones sobre la declaración de inexistencia o la negativa por cualquier causa sobre el ejercicio de derechos ARCOP;

VI. **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;

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

VIII. **Datos personales sensibles:** aquellos que se refieran a la esfera más íntima de la persona titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para ésta;

IX. **Derechos ARCOP:** derecho de acceso, rectificación, cancelación, oposición y portabilidad de datos personales que son regulados por la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados;

X. **Documento de seguridad:** el instrumento que describe y da cuenta de manera general sobre las medidas de seguridad técnicas, físicas y administrativas adoptadas por el responsable para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que posee;

XI. **Inventario de datos personales:** la identificación de la base de datos de tratamiento de las Unidades administrativas por el cual se documenta la información básica de cada tratamiento realizado, con independencia de su forma de almacenamiento, entre lo cual se incluye el ciclo de vida del dato personal, el catálogo de medios por los cuales se recaban, tipos de datos que se tratan y formatos de almacenamiento, las finalidades del tratamiento,

las personas servidoras públicas que tienen acceso a los sistemas de tratamiento, así como los destinatarios de las transferencias que, en su caso, se efectúen;

XII. **Medidas de seguridad:** el conjunto de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permitan proteger los datos personales;

XIII. **Ley General de Datos:** la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados;

XIV. **Lineamientos Generales de Datos:** Lineamientos Generales de Protección de Datos Personales para el Sector Público;

XV. **Programa de Protección de Datos Personales:** el documento que establece 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;

XVI. **Persona encargada:** la persona física o jurídica, pública o privada, ajena a la organización del responsable, que solo o conjuntamente con otros trate datos personales a nombre y por cuenta del responsable;

XVII. **Persona titular:** sujeto a quien pertenecen los datos personales que se recopilan, almacenan y procesan;

XVIII. **Remisión:** toda comunicación de datos personales realizada exclusivamente entre el responsable y la persona encargada, dentro o fuera del territorio mexicano;

XIX. **Receptor:** es el destinatario o tercero a quienes se transfieren los datos personales, ya sea a nivel nacional o internacional, lo cuales pueden ser entidades públicas o privadas cuyas responsabilidades se asocian con la transferencia de los datos personales;

XX. **Supresión:** la baja archivística de los datos personales conforme a las disposiciones jurídicas aplicables en materia de archivos, que resulte en la eliminación, borrado o destrucción de los datos personales bajo las medidas de seguridad previamente establecidas por el responsable;

XXI. **Transferencia:** toda comunicación de datos personales dentro o fuera del territorio mexicano, realizada a persona distinta del titular, del responsable o de la persona encargada;

XXII. **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;

XXIII. **Unidades administrativas**: las áreas adscritas a la Comisión que cuenten o puedan contar con los datos personales objeto de una solicitud presentada en términos de las disposiciones jurídicas aplicables. Estas áreas pueden ser receptoras directas de las solicitudes para el ejercicio de los derechos ARCOP o actuar como intermediarias, remitiendo las solicitudes a las Direcciones Generales de su adscripción para su atención y respuesta, según el caso; y

XXIV. **Unidad de Transparencia:** la Unidad de Transparencia de la Comisión, instancia a la que

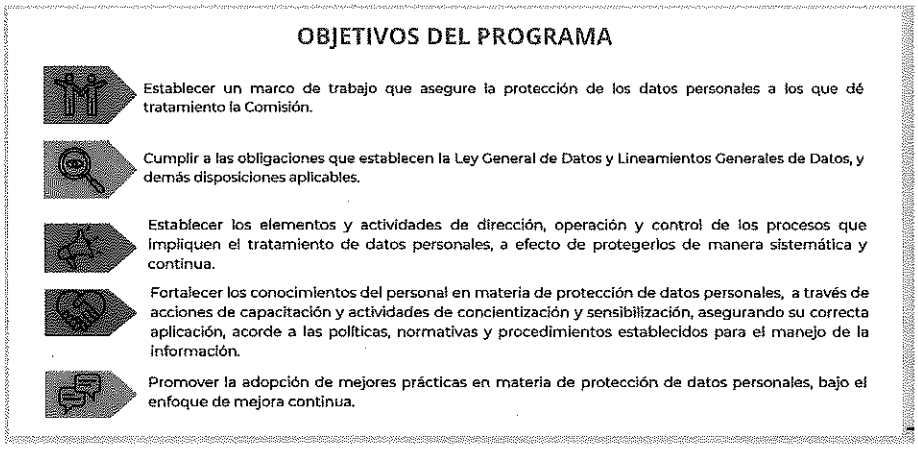
hacen referencia los artículos 3, fracción XX, 41 de la Ley General de Transparencia y Acceso a la Información Pública (Ley General de Transparencia) y 3, fracción XXXII y 79 de la Ley General de Datos, cuyas funciones se encuentran previstas en dichos artículos, siendo la persona titular designada de conformidad con el artículo 20, fracción II de la Ley General de Transparencia.

III. MARCO NORMATIVO

- Constitución Política de los Estados Unidos Mexicanos
- Ley General de Archivos
- Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados
- Ley General de Responsabilidades Administrativas de los Servidores Públicos
- Ley General de Transparencia y Acceso a la Información Pública
- Ley en Materia de Telecomunicaciones y Radiodifusión
- Reglamento Interior de la Agencia de Transformación Digital y Telecomunicaciones
- Reglamento Interior de la Comisión Reguladora de Telecomunicaciones
- Lineamientos Generales de Protección de Datos Personales para el Sector Público

IV. OBJETIVOS DEL PROGRAMA DE PROTECCIÓN DE DATOS PERSONALES

El Programa de Protección de Datos Personales de la Comisión fue diseñado bajo un enfoque integral y normativo alineado en la gestión de los datos personales bajo su custodia. El presente programa define las acciones que permiten garantizar la seguridad de la información, así como la confidencialidad, integridad y disponibilidad de los datos, al tiempo que fomenta una gestión eficiente en cumplimiento de las disposiciones legales aplicables, por lo que, entre sus objetivos, se encuentran:



V. ALCANCES DEL PROGRAMA

El Programa de Protección de Datos Personales es aplicable a todas las Unidades administrativas de la Comisión que en el ejercicio de sus funciones y atribuciones, realicen tratamiento de datos personales.

En virtud que, uno de los objetivos primordiales del Programa de Protección de Datos Personales es cumplir con la Ley General de Datos y demás normativa aplicable en la materia, el Programa abarca todos los principios, deberes y obligaciones previstos en dicha norma para la observancia en el tratamiento de datos personales.

No obstante, se exceptúa de la aplicación del presente Programa de Protección de Datos Personales la información confidencial a la que hace referencia el artículo 115 de la Ley General de Transparencia.

El Programa de Protección de Datos Personales es de observancia obligatoria para todas las personas servidoras públicas adscritas a las Unidades administrativas de la Comisión que realicen tratamiento de datos personales en ámbito de sus atribuciones y funciones, por lo que todos los proyectos o actividades que impliquen dicho tratamiento deberán incorporar desde su etapa de planeación y diseño, el cumplimiento a los principios, deberes y medidas de seguridad establecidos en la Ley General de Datos. Por lo tanto, las Unidades administrativas deberán prever y garantizar la disposición de los recursos humanos, materiales y financieros necesarios para la correcta implementación del Programa de Protección de Datos Personales y el cumplimiento de sus objetivos.

VI. RESPONSABILIDADES DENTRO DEL PROGRAMA

VI.1 Comité de Transparencia

De acuerdo con lo establecido en los artículos 77, 78 de la Ley General de Datos y 47 segundo párrafo de los Lineamientos Generales de Datos, así como el artículo Noveno de los *Lineamientos de Integración y Funcionamiento del Comité de Transparencia de la Comisión Reguladora de Telecomunicaciones*, el Comité de Transparencia es la máxima autoridad en materia de protección de datos personales, tiene la responsabilidad de coordinar, supervisar y ejecutar las acciones necesarias para garantizar el ejercicio del derecho a la protección de los datos personales al interior de la organización.

En razón de lo anterior este órgano colegiado asumirá las siguientes funciones específicas en relación con el presente Programa:

1) Elaborar, aprobar, coordinar y supervisar el Programa, en conjunto con las Unidades administrativas que estime necesario involucrar o consultar;

2) Proponer cambios y mejoras al Programa, a partir de la experiencia de su implementación;
3) Dar a conocer el Programa al interior de la Comisión;
4) Coordinar la implementación del Programa en las Unidades administrativas de la Comisión;
5) Asesorar a las Unidades administrativas en la implementación de este Programa, con el apoyo de las Unidades administrativas técnicas que estime pertinente;
6) Supervisar la correcta implementación del Programa;
7) Elaborar, aprobar, coordinar y supervisar el Programa Anual de Capacitación, en conjunto con las unidades administrativas que estime necesario involucrar o consultar, y
8) Las demás que de manera expresa señale el propio Programa.

VI.2 Unidad de Transparencia

De acuerdo con lo establecido en los artículos 79, 80 de la Ley General de Datos; 84 y demás relativos de los Lineamientos Generales de Datos, a la Unidad de Transparencia le compete, entre otras, las atribuciones siguientes:

1. Elaborar, actualizar cuando corresponda, y proponer al Comité de Transparencia el Programa de Protección de Datos Personales, asegurando su alineación con las disposiciones normativas aplicables;
2. Actuar como órgano de consulta en la materia, brindando asesoría especializada dentro del marco del Programa;
3. Coordinar la aplicación del Programa de Protección de Datos Personales en las Unidades administrativas promoviendo su correcta implementación;
4. Difundir el contenido del Programa de Protección de Datos Personales, garantizando que su alcance y objetivos sean conocidos por todas las Unidades administrativas correspondientes;
5. Orientar a las Unidades administrativas en la implementación del Programa de Protección de Datos Personales, resolviendo dudas y fortaleciendo sus capacidades en materia de protección de datos personales;
6. Dar seguimiento a la implementación del Programa de Protección de Datos Personales por parte de las Unidades administrativas, con el propósito de identificar áreas de mejora y proponer medidas preventivas o correctivas para garantizar el adecuado tratamiento de los datos personales;
7. Informar al Comité de Transparencia sobre los avances, el estado y los resultados derivados de la implementación del Programa de Protección de Datos Personales, facilitando la toma de decisiones informada.

Las atribuciones mencionadas se establecen sin perjuicio de aquellas expresamente conferidas a la Unidad de Transparencia de conformidad con la Ley General de Datos, y los Lineamientos Generales de Datos aplicables.

VI.3 Responsable de Seguridad

Conforme a las atribuciones establecidas en el Reglamento Interior de la Comisión Reguladora de Telecomunicaciones, le corresponde a la Unidad administrativa con facultades para establecer, coordinar y supervisar la seguridad de información y de los sistemas informáticos, coadyuvar con la Unidad de Transparencia a efecto de establecer y mantener las medidas de seguridad técnicas que permitan proteger los datos personales y garantizar su confidencialidad, integridad y disponibilidad.

VI.4 Unidades Administrativas

Las Unidades administrativas que tengan a su cargo el tratamiento de datos personales, deberán colaborar con el Comité de Transparencia en la implementación del presente Programa.

VII. GESTIÓN DE LOS DATOS PERSONALES

El tratamiento de datos personales que realicen las Unidades administrativas de la Comisión, deberán cumplir con los principios, deberes y obligaciones que prevé la Ley General de Datos, con independencia del formato, sistema, 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 el Programa de Protección de Datos Personales 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 de la Comisión, 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, sea que se trate de encargados o no, en lo referente a la protección de datos personales.

El tramo de responsabilidad que les corresponda, estarán delimitadas y acreditadas de conformidad con las funciones y obligaciones establecidas en el Reglamento Interior de la Comisión Reguladora de Telecomunicaciones, los contratos, convenios y/o cualquier otro instrumento jurídico aplicable, que permita delimitar, acreditar y detallar la existencia, alcance y contenido de sus obligaciones en materia de protección de datos personales.

En el presente Programa de Protección de Datos Personales, se identifican las obligaciones que se deberán cumplir en todos los tratamientos de datos personales que realicen las Unidades administrativas de la Comisión, de acuerdo con lo que establece la Ley General de Datos y los

Lineamientos Generales de Datos. Asimismo, el presente documento prevé mejores prácticas para la protección de datos personales, en aquellos tratamientos que así lo permitan.

En la elaboración del Programa de Protección de Datos Personales, se consideran como líneas de acción las siguientes:

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. Identificación y categorización de datos personales

La identificación de los datos personales que se encuentran en posesión de la Comisión es la base para su protección y resguardo. El **"Inventario de datos personales de la Comisión Reguladora de Telecomunicaciones"**, forma parte del **Documento de Seguridad**, en términos de lo dispuesto por el artículo 29, fracción I de la Ley General de Datos. El Inventario reúne y da cuenta de los datos personales, sistemas de tratamiento y demás elementos requeridos por los artículos 27, fracción III y 29, fracción I de la Ley General de Datos, así como el artículo 58 de los Lineamientos Generales de Datos.

A continuación, se muestran de manera enunciativa algunas de las categorías de datos que comúnmente son considerados personales, las cuales podrían ser tratados por las Unidades administrativas de la Comisión y, únicamente son una referencia útil para determinar cuándo se está en presencia de datos personales:

Datos identificativos: El nombre, alias, pseudónimo, domicilio, código postal, teléfono particular, sexo, estado civil, teléfono celular, firma, clave de Registro Federal de Contribuyentes (RFC), Clave Única de Registro de Población (CURP), Clave de Elector, Matrícula del Servicio Militar Nacional, número de pasaporte, lugar y fecha de nacimiento, nacionalidad, edad, fotografía, localidad y sección electoral, y análogos.

Datos laborales: Número de seguridad social, movimientos afiliatorios, documentos de reclutamiento o selección, nombramiento, incidencia, capacitación, actividades extracurriculares, referencias laborales, referencias personales, solicitud de empleo, hoja de servicio, y análogos.

Datos patrimoniales: Bienes muebles e inmuebles de su propiedad, información fiscal, historial crediticio, ingresos y egresos, número de cuenta bancaria y/o CLABE interbancaria de personas físicas, inversiones, seguros, fianzas, servicios contratados, referencias personales, beneficiarios, dependientes económicos, decisiones patrimoniales y análogos.

Datos sobre situación jurídica o legal: La información relativa a una persona que se encuentre o haya sido sujeta a un procedimiento administrativo seguido en forma de juicio o jurisdiccional en materia laboral, civil, penal, fiscal, administrativa o de cualquier otra rama del Derecho, y análogos;

Datos académicos: Trayectoria educativa, avances de créditos, tipos de exámenes, promedio, calificaciones, títulos, cédula profesional, certificados, reconocimientos y análogos.

Datos electrónicos: Firma electrónica, dirección de correo electrónico.

Por otra parte, la Ley General de Datos contempla una figura especial de datos personales, los denominados "**Datos personales sensibles**", que se definen como aquéllos que hacen referencia a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleva un riesgo grave para éste.

Adicionalmente, se listan una serie de datos personales que explícitamente son considerados como sensibles, incluyendo los que revelen aspectos como el origen racial o étnico, el estado de salud, la información genética, las creencias religiosas, filosóficas o morales, las opiniones políticas y la preferencia sexual.

Datos biométricos: Huella dactilar, geometría del rostro, iris, geometría de la mano, biometría vascular, escritura, voz, escritura de teclado y análogos.

Datos sobre la salud: El expediente clínico de cualquier atención médica, historial médico, referencias o descripción de sintomatologías, detección de enfermedades, incapacidades médicas, discapacidades, intervenciones quirúrgicas, vacunas, consumo de estupefacientes, uso de aparatos oftalmológicos, ortopédicos, auditivos, prótesis, estado físico o mental de la persona, así como la información sobre la vida sexual, y análogos.

Datos ideológicos: Ideologías, creencias, opinión política, afiliación política, opinión pública, afiliación sindical, religión, convicción filosófica y análogos.

Datos sobre la 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.

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.

B. Roles y responsabilidades en el tratamiento de datos personales

El artículo 27, fracción II, de la Ley General de Datos establece como una de las actividades para realizar, implementar y mantener medidas de seguridad para la protección de datos personales, definir las funciones y obligaciones de las personas servidoras públicas involucradas en el tratamiento de los datos personales.

En ese sentido, a través del presente Programa de Protección de Datos Personales de la Comisión, ha identificado dos niveles de protección con relación en los siguientes:

Actividades para su cumplimiento	Unidades administrativas responsables
Nivel general: A través de la correcta observancia de las disposiciones previstas en el presente Programa, en virtud de que en este, se plasma un enfoque integral y normativo alineado con la gestión de los datos personales bajo su custodia; asimismo, define las acciones que permiten garantizar la seguridad de la información, así como la confidencialidad, integridad y	Todas las Unidades administrativas de la Comisión que lleven a cabo tratamiento de datos personales.

disponibilidad de los datos, al tiempo que fomenta una gestión eficiente en cumplimiento de las disposiciones legales aplicables.	
Nivel particular: A través de la integración de los **inventarios de datos personales** que se desarrollen por los sistemas de tratamiento de cada una de las Unidades administrativas de la Comisión.	Todas las personas servidoras públicas que lleven a cabo tratamiento de datos personales **en cualquier fase del ciclo de vida**.

VIII. PRINCIPIOS EN EL TRATAMIENTO

El tratamiento de los datos personales que se encuentren en posesión de las Unidades administrativas de la Comisión, deberá realizarse en observancia de 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 • Finalidad • Proporcionalidad • Seguridad • Confidencialidad	• Registro • Organización • Conservación • Elaboración • Utilización • Comunicación • Difusión
Uso	• Calidad • Finalidad • Lealtad • Responsabilidad • Seguridad • Confidencialidad	• Almacenamiento • Posesión • Acceso • Manejo • Aprovechamiento • Divulgación • Transferencia • Disposición
Eliminación	• Calidad • Seguridad	

a) Principio de Licitud

De conformidad con el artículo 11 de la Ley General de Datos, así como el artículo 8 de los Lineamientos Generales de Datos, las personas servidoras públicas de la Comisión deberán llevar a cabo el tratamiento de los datos personales conforme a las disposiciones previstas en la ley de la materia, la legislación mexicana específica o sectorial que resulte aplicable y, en su caso, el derecho internacional, respetando en todo momento los derechos y libertades de las personas titulares.

Para el cumplimiento del principio de licitud, se considera adecuado tener en cuenta las acciones siguientes:

Actividades para su cumplimiento	Unidades administrativas responsables del cumplimiento	Medios para acreditar el cumplimiento
Identificar y **conocer la normativa que regule el tratamiento** de datos personales en los trámites, procesos o procedimientos realizados por las Unidades administrativas de la Comisión.	Todas las Unidades administrativas de la Comisión que lleven a cabo tratamiento de datos personales.	Difusión y capacitación sobre el marco normativo aplicable al tratamiento de los datos personales respectivos.
Identificar y **conocer los principios y deberes del tratamiento** de datos personales, así como los derechos de las personas titulares, contenidos en la normativa vigente en materia de protección de datos personales.		
Llevar a cabo **el tratamiento** de datos personales **con estricto apego a la legislación** aplicable.		

b) Principio de Lealtad

De acuerdo a lo dispuesto en el artículo 13 de la Ley General de Datos, y el artículo 11 de los Lineamientos Generales de Datos, las personas servidoras públicas de la Comisión no deberán obtener ni tratar los datos personales a través de medios engañosos o fraudulentos. Se entiende por medios engañosos y fraudulentos, aquéllos que se utilicen para tratar los datos personales con dolo,

mala fe o negligencia, de conformidad con el artículo 11, fracción I de los citados Lineamientos Generales de Datos.

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 de Datos, 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 de Datos, 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 la normativa aplicable.

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

Actividades para su cumplimiento	Unidades administrativas responsables del cumplimiento	Medios para acreditar el cumplimiento
Verificar que los datos personales no se obtengan con dolo, mala fe o negligencia.	Todas las Unidades administrativas de la Comisión que lleven a cabo tratamiento de datos personales.	Avisos de privacidad actualizados.
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.		

c) Principio de Información

2025 Año de La Mujer Indígena

De conformidad con lo establecido en los artículos 3, fracción III, 20, 21, 22 de la Ley General de Datos, y del 26 a 45 de los Lineamientos Generales de Datos, las personas servidoras públicas de la Comisión deberán informar a la persona titular, mediante el 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.

Medios que facilitan la acreditación del cumplimiento
1. Redactar los Avisos de Privacidad que se requieran conforme a los tratamientos que lleven a cabo las Unidades administrativas. Como regla general, se requerirá un aviso de privacidad por sistema de tratamiento. **2.** Elaborar las dos modalidades para cada Aviso de Privacidad: Simplificado e Integral. **3.** Poner a disposición todos los avisos de privacidad, en sus modalidades simplificada e integral, en el portal de Internet de la Comisión, en la sección que se destine para tal efecto, a fin de que se difunda por medios electrónicos. Por su parte, las Unidades administrativas deberán poner a disposición el aviso de privacidad en los medios que habiliten para la obtención de los datos personales previo a que ocurra el tratamiento.

d) Principio de Consentimiento

Conforme a lo señalado en los artículos 14, 15, 16 de la Ley General de Datos y artículos 12 al 20 de los Lineamientos Generales de Datos, en los casos en que se requiera, las personas servidoras públicas de la Comisión deberán obtener el consentimiento de la persona titular de manera previa al tratamiento de sus datos personales, salvo que se actualice alguna de las excepciones previstas en el artículo 16 de la Ley General de Datos.

De acuerdo con lo dispuesto por el artículo 14 de la Ley General de Datos, 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	Unidades	Medios para acreditar el

	administrativas responsables del cumplimiento	cumplimiento
Llevar a cabo el tratamiento de los datos personales de la persona titular en aquellos casos en los que, conforme a la normativa aplicable, no se requiere consentimiento previo del mismo.	Todas las Unidades administrativas de la Comisión que lleven a cabo tratamiento de datos personales.	No se requiere establecer procedimiento o medio previo cuando se cumpla con una de las excepciones previstas en el artículo 16 de la Ley General de Datos.
Cuando se traten datos personales sensibles la solicitud del consentimiento expreso deberá ser concisa e inteligible, estar redactada en un lenguaje claro y sencillo, de conformidad con el artículo 15, primer párrafo de la Ley General de Datos.		Consentimiento expreso por las personas titulares de los datos personales.
El consentimiento deberá ser tácito siguiendo las reglas establecidas en el artículo 15, segundo párrafo de la Ley General de Datos. Asimismo, en el caso de que la persona titular no manifieste su negativa, se entenderá que ha otorgado su consentimiento tácito para el tratamiento de sus datos personales, salvo prueba en contrario.		Procedimiento para la puesta a disposición del aviso de privacidad y en su caso la solicitud del consentimiento.
Cuando los datos personales se obtengan de manera indirecta 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		Aviso de privacidad. Procedimiento para la puesta disposición del aviso de privacidad y en su caso la solicitud del consentimiento.

informada de la persona titular, mediante la que autorice el tratamiento de sus datos personales de manera tácita o expresa, según corresponda.		Consentimiento expreso otorgado.
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.		Procedimiento interno de atención a solicitudes para el ejercicio de derechos ARCOP.

e) Principio de Proporcionalidad

Conforme a lo dispuesto en los artículos 19 de la Ley General de Datos, 24 y 25 de los Lineamientos Generales de Datos, los datos personales deberán tratarse sólo 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 Unidades administrativas de la Comisión por la normatividad que le resulte aplicable.

Actividades para su cumplimiento	Unidades administrativas responsables del cumplimiento	Medios para acreditar el cumplimiento
Identificar qué datos personales se requieren para el cumplimiento de cada una de las finalidades.	Todas las Unidades administrativas de la Comisión que lleven a cabo tratamiento de datos personales.	Avisos de privacidad. Documentos, expedientes, archivos o bases de datos correspondientes al tratamiento.
Analizar y revisar que se soliciten sólo aquellos datos personales que resultan indispensables para cumplir con las		

finalidades de que se trate.		Normatividad que establezca, en su caso, los datos personales que deberán solicitarse para el tratamiento específico.
Requerir el mínimo posible de datos personales para lograr las finalidades para las cuales se tratan.		

f) Principio de Finalidad

En términos de lo dispuesto por los artículos 12 de la Ley General de Datos, 9 y 10 de los Lineamientos Generales de Datos, el tratamiento de los datos personales que efectúen las Unidades administrativas de la Comisión 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 Unidades administrativas de la Comisión deberán llevar a cabo las recomendaciones siguientes:

Actividades de cumplimiento	Unidades administrativas responsables del cumplimiento	Medios para acreditar el cumplimiento
Identificar el marco normativo que otorga las atribuciones a las Unidades administrativas de la Comisión para tratar los datos personales.	Todas las Unidades administrativas de la Comisión que lleven a cabo tratamiento de datos personales.	Marco normativo
Verificar que la finalidad del tratamiento sea compatible con las atribuciones expresas conferidas a las Unidades administrativas de la Comisión.		Aviso de privacidad Inventario de datos personales Documentos que se generen en el tratamiento
Verificar que la finalidad del tratamiento sea compatible con las atribuciones expresas conferidas a las Unidades administrativas de la Comisión.		
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 de la Comisión, en función de la Unidad administrativa 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.		

g) Principio de Calidad

Exactitud, actualización y pertinencia de los datos personales

Conforme a lo dispuesto por los artículos 17, 18 de la Ley General de Datos, 21, 22 y 23 de los Lineamientos Generales de Datos, los datos personales en posesión de la Comisión deberán ser **exactos, completos, correctos y actualizados** para los fines para los cuales fueron recabados.

Se entenderá que los datos personales son:

I. **Exactos y correctos:** cuando los datos personales en posesión del responsable no presenten errores que pudieran afectar su veracidad;
II. **Completos:** cuando su integridad permite el cumplimiento de las finalidades que motivaron su tratamiento y de las atribuciones del responsable, y
III. **Actualizados:** cuando los datos personales responden fielmente a la situación actual de la persona titular.

Conservación de los datos personales

En términos del artículo 17, último párrafo, de la Ley General de Datos, 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 18 de la Ley General de Datos 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 Unidades administrativas de la Comisión.

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.

Bloqueo de datos personales

Las personas servidoras públicas de la Comisión que sean responsables del tratamiento de datos personales, una vez que estos hayan cumplido con la finalidad para la cual fueron recabados, deberán proceder a su bloqueo.

Durante este periodo, los datos no podrán ser objeto de tratamiento y, una vez transcurrido el plazo de prescripción legal, se realizará su supresión en la base de datos correspondiente.

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

Actividades de cumplimiento	Unidades administrativas responsables del cumplimiento	Medios para acreditar el cumplimiento
Implementar medidas para que los datos personales se actualicen y, en su caso, corrijan o completeen, en las distintas bases de datos que estén a cargo de la Unidad administrativa.	Todas las Unidades administrativas de la Comisión que lleven a cabo tratamiento de datos personales.	Base de datos actualizada y correcta. Registros en donde consten las actualizaciones realizadas, en aquellos casos en que las mismas hayan resultado procedentes.
Establecer procedimientos, métodos y técnicas orientadas a la supresión definitiva de los datos personales,		Documento que contenga el establecimiento o identificación de

considerando los atributos de irreversibilidad; seguridad y confidencialidad.		los plazos de conservación de los datos personales.

h) Principio de Responsabilidad

Con fundamento en los artículos 23, 24 de la Ley General de Datos, y los artículos del 46 al 54 de los Lineamientos Generales de Datos, las Unidades administrativas de la Comisión deberán velar por el cumplimiento de todos los principios del tratamiento, adoptar las medidas necesarias para su aplicación, y demostrar que cumplen con sus obligaciones en materia de protección de datos personales. Para el cumplimiento del principio de responsabilidad, se tienen en cuenta principalmente las siguientes acciones:

Actividades de cumplimiento	Unidades administrativas responsables del cumplimiento	Medios para acreditar el cumplimiento
Mantener actualizadas las políticas y programas de datos personales y seguridad de la información para determinar las modificaciones que se requieran.	Todas las Unidades administrativas de la Comisión que lleven a cabo tratamiento de datos personales.	Políticas y/o programas de protección de datos personales, y de seguridad de la información, actualizados. Acciones de supervisión y vigilancia. Programa de capacitación para las personas servidoras públicas de la Comisión.
Revisar y fortalecer el sistema de supervisión y vigilancia interna y/o externa, para comprobar el cumplimiento de las políticas de protección de datos personales.		
Incluir cursos y temas sobre las obligaciones y demás deberes en materia de protección de datos personales.		

IX. DEBERES EN EL TRATAMIENTO

a) Seguridad

De conformidad con los artículos 25 de la Ley General de Datos y 55 de los Lineamientos Generales de Datos, 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 autorizado, así como para garantizar su confidencialidad, integridad y disponibilidad.

Medios que facilitan la acreditación del cumplimiento
• Documento de seguridad de la Comisión • 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 acuerdo a lo establecido en el artículo 36 de la Ley General de Datos y 71 de los Lineamientos Generales de Datos, las personas servidoras públicas de la Comisión 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 su relación con la Comisión, y sin menoscabo de lo establecido en las disposiciones de acceso a la información pública.

Medios que facilitan la acreditación del cumplimiento
• Implementación de controles para la confidencialidad de los datos personales • Contratos celebrados por la Comisión que contienen cláusulas de confidencialidad

Encargados

En cumplimiento a lo dispuesto en los artículos 53, 55 de la Ley General de Datos, 108, 109 y 110 de los Lineamientos Generales de Datos, las Unidades administrativas de la Comisión 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 la Comisión, en su carácter de responsable del tratamiento.

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

Contratación de proveedores de servicios de cómputo en la nube

En términos de los artículos 57, 58 de la Ley General de Datos y 111 de los Lineamientos Generales de Datos, en la contratación de proveedores de servicios de cómputo en la nube y similares, la Unidad administrativa requirente en coordinación con la Unidad administrativa técnica de la Comisión tendrán la obligación de establecer mecanismos 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 Ley General de Datos, los Lineamientos Generales de Datos y demás disposiciones que resulten aplicables en la materia.

Transferencia de datos personales

Conforme a lo dispuesto por los artículos 3, fracción XXX, y del 59 al 64 de la Ley General de Datos, y los artículos del 113 al 118 de los citados Lineamientos Generales de Datos, las transferencias nacionales e internacionales de datos personales que realicen las Unidades administrativas de la Comisión, 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	Unidades administrativas responsables	Medios para acreditar el 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.	Todas las Unidades administrativas de la Comisión que lleven a cabo tratamiento de datos personales.	Cláusulas contractuales, convenios de colaboración u otro instrumento jurídico mediante los cuales se formalicen las transferencias de datos personales.
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 tercero receptor se obliga a proteger los datos personales conforme a los principios y deberes que establece la Ley General de Datos y las disposiciones que resulten aplicables en la materia.		
Comunicar el Aviso de Privacidad correspondiente al tercero receptor en las transferencias nacionales e internacionales que se lleven a cabo.		

X. EVALUACIÓN DE IMPACTO EN LA PROTECCIÓN DE DATOS PERSONALES

En términos de lo dispuesto por los artículos 68, 69, 71, 72, 73 de la Ley General de Datos y 120 de los Lineamientos Generales de Datos, y 10 de las Disposiciones administrativas de carácter general para la elaboración, presentación y valoración de evaluaciones de impacto en la protección de datos personales, cuando las personas servidoras públicas de la Comisión pretendan 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 dichos ordenamientos impliquen el tratamiento intensivo o relevante de datos personales, deberán realizar una **Evaluación de impacto en la protección de datos personales** y presentarla ante la Secretaría Anticorrupción y Buen Gobierno.

Actividades para su cumplimiento	Unidades administrativas

	responsables
Identificar los tratamientos de datos personales que puedan ser considerados intensivos o relevantes, en términos del artículo 69 de la Ley General de Datos 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 Unidades administrativas de la Comisión que lleven a cabo tratamiento de datos personales.

Portabilidad de datos personales

En términos del artículo 51 de la Ley General de Datos, el derecho a la portabilidad de los datos personales confiere a las personas titulares la prerrogativa de obtener una copia de los datos objeto de tratamiento en un formato electrónico estructurado y comúnmente 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 que sea posible la portabilidad, los datos personales deben ser sujetos a tratamiento por la Comisión, a través de medios electrónicos, en un formato estructurado y comúnmente utilizado, y ser proporcionados a la persona titular en un formato de similar naturaleza, que le permita seguir utilizándolos.

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

A través del 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 las amenazas y vulnerabilidades a efecto de reducir la probabilidad de que ocurran los incidentes de seguridad.

Asimismo, como parte de las acciones para la seguridad de los datos personales, y con fundamento en el artículo 29 de la Ley General de Datos, la Comisión debe elaborar el Documento de Seguridad, en el cual se describan las medidas de seguridad adoptadas, para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que se encuentran en su posesión.

Respuesta a incidentes o vulneraciones de seguridad

Además de las que señale la Ley General de Datos, los Lineamientos Generales de Datos y demás normatividad aplicable, se considerarán como vulneraciones de seguridad, en cualquier fase del tratamiento de los datos personales, al menos, las siguientes:

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

La gestión y notificación de vulneraciones de seguridad se llevará a cabo conforme a lo previsto en las Medidas de Seguridad Administrativas que se establezcan en el Documento de Seguridad. En dicho documento, 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 34 de la Ley General de Datos y 66 de los Lineamientos Generales de Datos, que establecen la obligación a cargo de la Comisión de informar sin dilación alguna a la persona titular de los datos personales, y a la Autoridad Garante, las vulneraciones que afecten de forma significativa, 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.

En términos de los artículos 35 de la Ley General de Datos y 67 de los Lineamientos Generales de Datos, el procedimiento para llevar a cabo la notificación, gestión y respuesta ante incidencias contarán con un registro técnico en el que se describirán entre otras cosas, el tipo de incidencia, circunstancias, acciones, consecuencias, descripción de los hechos.

Al elaborar el acta circunstanciada de los hechos ocurridos tendrá que contener una descripción detallada de las circunstancias en torno a la vulneración en la que se detalle:

- Fecha y hora en la que se produjo y/o detectó la incidencia.
- Momento y lugar donde se produjo y/o detectó la incidencia.

- La hora y fecha del inicio de la investigación sobre la vulneración.
- Descripción detallada de los hechos.
- Naturaleza del incidente, las categorías y el posible número de personas afectadas.
- Los sistemas de tratamiento y los datos personales involucrados.
- Posibles consecuencias derivadas de la vulneración ocurrida.
- Acciones implementadas que derivan de la incidencia.
- Recomendaciones a las personas titulares de los datos comprometidos.
- El medio puesto a disposición de las personas titulares para que pueda obtener mayor información al respecto.
- Nombre y firma de quienes intervinieron.

Al ocurrir una vulneración de seguridad, el responsable de la seguridad de la información deberá analizar la causa probable y diseñar, proponer e implementar, un plan de trabajo preventivo y correctivo para adecuar las medidas de seguridad que prevengan la ocurrencia de nuevos incidentes.

Sensibilización y capacitación

Con fundamento en el artículo 24, fracción III, de la Ley General de Datos y 48 de los Lineamientos Generales de Datos, la Comisión implementará un programa de capacitación y actualización del personal sobre las obligaciones y demás deberes en materia de protección de datos personales.

Dicho 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 la Ley General de Datos.

Sanciones

Cuando la Unidad de Transparencia tenga conocimiento del incumplimiento de alguna de las obligaciones previstas dentro del presente Programa solicitará a la Unidad administrativa correspondiente llevar a cabo las acciones que resulten necesarias para subsanar dicho incumplimiento y evitar incidentes futuros o situaciones de riesgo para la protección de los datos personales.

Asimismo, si alguna Unidad administrativa se negara a colaborar con la Unidad de Transparencia en la atención de las solicitudes para el ejercicio de los derechos ARCOP, de conformidad con el artículo 105 de los Lineamientos Generales de Datos dará aviso al superior jerárquico para que le ordene realizar sin demora las acciones conducentes.

En caso de que la Unidad de Transparencia observe un acto u omisión sobre el que deba conocer el Órgano Interno de Control, se hará de conocimiento de dicha entidad; si la misma se encuentra relacionada con la sustanciación de un recurso de revisión en que el que se pudo haber incurrido en una probable responsabilidad por el incumplimiento de las obligaciones previstas en la Ley General de Datos y demás disposiciones que resulten aplicables en materia, se remitirá a la Secretaría Anticorrupción y Buen Gobierno dentro del día hábil siguiente a su recepción para el trámite que corresponda, de conformidad con lo previsto en los artículos 86, 96, 97 y 103 de la Ley General de Datos.

FECHA DE ELABORACIÓN Y/O ÚLTIMA MODIFICACIÓN:

Ciudad de México, a 9 de diciembre de 2025, mediante **ACUERDO-CTCRT/2SO/05/2025** adoptado en la Segunda Sesión Ordinaria, las personas integrantes del Comité de Transparencia de la Comisión Reguladora de Telecomunicaciones, aprueban por unanimidad de votos el "Programa de Protección de Datos Personales de la Comisión Reguladora de Telecomunicaciones".

PRESIDENTA

PAULINA ORTEGA GARCÍA
TITULAR DE LA UNIDAD DE TRANSPARENCIA

INTEGRANTE

FORTUNATO ANTONIO HERNÁNDEZ
RESPONSABLE DEL ÁREA COORDINADORA DE ARCHIVO

INTEGRANTE

CÉSAR ALFONSO ESPINOSA PALAFOX
TITULAR DEL ÓRGANO INTERNO DE CONTROL EN LA AGENCIA DE TRANSFORMACIÓN DIGITAL Y TELECOMUNICACIONES

SECRETARIO TÉCNICO

ISRAEL ADRIÁN JIMÉNEZ CAMERO
SUBDIRECTOR DE TRANSPARENCIA