



GOBIERNO DE LA
CIUDAD DE MÉXICO

SECRETARÍA DE LA CONTRALORÍA GENERAL
UNIDAD DE TRANSPARENCIA



CIUDAD DE MÉXICO, A 09 DE ENERO DE 2024

OFICIO: SCG/UT/0019/2024

ASUNTO: ACTUALIZACIÓN DEL "REGISTRO
ELECTRÓNICO DE SISTEMAS DE DATOS
PERSONALES"

DIRECCIONES GENERALES
DIRECCIÓN DE CONTRALORÍA CIUDADANA
DIRECCIÓN DE VIGILANCIA MÓVIL
DIRECCIÓN DE MEJORA GUBERNAMENTAL
PRESENTES

Por medio del presente y con fundamento en los artículos 3, fracción XXIX, 36, 37, 38, 39, 40 y 76, fracción VIII de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México, expongo y solicito lo siguiente:

Con la finalidad de actualizar el denominado "Registro Electrónico de Sistemas de Datos Personales", se solicita a las Unidades Administrativas de la Secretaría de la Contraloría General que informen el número y nombre de sistemas a su cargo y el estado en que se encuentran, es decir, si estos se encuentran vigentes.

En caso de que se considere necesaria la creación, modificación o supresión de Sistemas de Datos Personales, les solicito de la manera más atenta que remitan en breve término los Acuerdos respectivos.

Es importante hacer de su conocimiento que los Sistemas de Datos Personales de los sujetos obligados de la Ciudad de México se encuentran disponibles para consulta en la siguiente dirección electrónica:

<https://datospersonales.infocdmx.org.mx/ConsultaPublica.aspx>

Av. Arcos de Belén No. 2, piso 9, Colonia Doctores,
Alcaldía Cuauhtémoc, Ciudad de México, C.P. 06720
Tel: 56276700 Ext: 54062



CIUDAD INNOVADORA
Y DE DERECHOS



GOBIERNO DE LA
CIUDAD DE MÉXICO

SECRETARÍA DE LA CONTRALORÍA GENERAL
UNIDAD DE TRANSPARENCIA



Se adjunta archivo digital del acuerdo 0218/SO/25-01/2023, documento que servirá como guía para la elaboración de los Acuerdos; en caso de alguna duda puede solicitar una mesa de trabajo a esta Unidad de Transparencia.

Sin otro en particular, reciba un cordial saludo.

ATENTAMENTE

LEONIDAS PÉREZ HERRERA
TITULAR DE LA UNIDAD DE TRANSPARENCIA
EN LA SECRETARÍA DE LA CONTRALORÍA GENERAL
Elaboró Daniel Pérez Merino



ACUERDO 0218/SO/25-01/2023

ACUERDO MEDIANTE EL CUAL SE ABROGAN LOS LINEAMIENTOS GENERALES SOBRE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE SUJETOS OBLIGADOS DE LA CIUDAD DE MÉXICO Y SE APRUEBAN LOS LINEAMIENTOS DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE SUJETOS OBLIGADOS DE LA CIUDAD DE MÉXICO.

CONSIDERANDO

1. DEL INSTITUTO

1.1 Que el siete de febrero de dos mil catorce, se promulgó en el Diario Oficial de la Federación, el Decreto por el que se reforman y adicionan diversas disposiciones de la Constitución Política de los Estados Unidos Mexicanos (Constitución Federal), en materia de transparencia, modificando entre otros los artículos 6º y 116, fracción VIII, los cuales establecen la creación de órganos autónomos, especializados e imparciales, responsables de garantizar el derecho de acceso a la información y de protección de datos personales en posesión de los sujetos obligados.

1.2 Que, en cumplimiento al artículo segundo transitorio del Decreto de reforma en materia de transparencia, el Congreso de la Unión expidió la Ley General de Transparencia y Acceso a la Información Pública (Ley General de Transparencia), la cual fue publicada el cuatro de mayo de dos mil quince en el Diario Oficial de la Federación, que entró en vigor al día siguiente de su publicación de acuerdo con lo dispuesto en su artículo Primero Transitorio.

1.3 Que, de conformidad con el artículo 37 de la Ley de Transparencia, Acceso a la Información Pública y Rendición de Cuentas de la Ciudad de México (Ley de Transparencia), publicada en la Gaceta Oficial de la Ciudad de México el seis de mayo del dos mil dieciséis, el Instituto de Transparencia, Acceso a la Información Pública, Protección de Datos Personales y Rendición de Cuentas de la Ciudad de México, (Instituto o INFO CDMX) es un órgano autónomo de la Ciudad de México, especializado, independiente, imparcial y colegiado, con personalidad jurídica y patrimonio propios, con plena autonomía técnica, de gestión y financiera, con capacidad para decidir sobre el ejercicio de su presupuesto y determinar su organización interna, funcionamiento y resoluciones, responsable de garantizar el cumplimiento de la Ley, dirigir y vigilar el ejercicio de los Derechos de Acceso a la Información y la Protección de Datos Personales, conforme a los principios y bases establecidos por el artículo 6o. y 16 de la Constitución Federal, la Constitución Política de la Ciudad de México, las Leyes Generales y las Leyes locales aplicables. En su organización, funcionamiento y control, el Instituto se regirá por los principios de certeza, legalidad, independencia, imparcialidad, eficacia, objetividad, profesionalismo, transparencia y máxima publicidad.



1.4 Que en el artículo Segundo Transitorio de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (Ley General de Datos), la cual fue publicada el veintiséis de enero de dos mil diecisiete, en el Diario Oficial de la Federación, se estableció la obligación de ajustar las leyes vigentes de las entidades federativas en materia de protección de datos personales, a las disposiciones previstas en dicha norma general, en un plazo de seis meses siguientes a partir de su entrada en vigor.

1.5 Que en los artículos 157, último párrafo, y Quinto Transitorio de la Ley General de Datos, se establece la obligación de emitir Lineamientos de carácter general por parte de los órganos garantes de las entidades federativas.

1.6 Que, el cinco de febrero de dos mil diecisiete, se publicó en la Gaceta Oficial de la Ciudad de México el Decreto por el que se expidió la Constitución Política de la Ciudad de México (Constitución local), que en su artículo 7, apartado E, numerales 2, 3 y 4, estableció el deber de proteger la información que se refiera a la privacidad y los datos personales, en los términos y con las excepciones previstas en la Constitución Federal y las leyes; asimismo prohibió cualquier injerencia arbitraria, oculta o injustificada en la vida de las personas y dispuso que toda persona tiene derecho al acceso, rectificación, cancelación y portabilidad de sus datos personales, así como a manifestar su oposición respecto del tratamiento de estos.

1.7 Que, en términos del artículo 46, apartado A, inciso d), de la Constitución local se dispuso que el Instituto es un organismo autónomo de carácter especializado e imparcial, con personalidad jurídica y patrimonio propio, plena autonomía técnica y de gestión, capacidad para decidir sobre el ejercicio de su presupuesto y para determinar su organización interna de conformidad con lo previsto en las leyes correspondientes.

1.8 Que, en sesión solemne del Congreso de la Ciudad de México, celebrada el dieciocho de diciembre de dos mil dieciocho, se designó y tomó la protesta a las Comisionadas María del Carmen Nava Polina y Marina Alicia San Martín Reboloso, así como de los Comisionados Julio César Bonilla Gutiérrez y Rodrigo Arístides Guerrero García para conformar la nueva integración del Pleno del INFO CDMX.

1.9 Que, el 08 de diciembre de 2020, el Congreso de la Ciudad de México, en sesión solemne, designó y tomó protesta a la Comisionada Ciudadana Laura Lizette Enríquez Rodríguez, para formar parte del Pleno del INFO CDMX.

1.10 Que las comisionadas y los comisionados designaron como Comisionado Presidente al Doctor Arístides Rodrigo Guerrero García, en términos de los artículos 49, numeral 2, de la Constitución local; 44 de la Ley de Transparencia local; y 4, fracción II, del Reglamento Interior del Instituto, mediante Acuerdo 2594/SO/15-12/2021, en la Trigésima Octava Sesión Ordinaria, de fecha 15 de diciembre de 2021.



2. DE LA COMPETENCIA Y ATRIBUCIONES DEL INSTITUTO, ASÍ COMO DE SU DIRECCIÓN DE DATOS PERSONALES, EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES.

2.1 Que, conforme a lo establecido en el artículo 49, numeral 1, de la Constitución local; este Instituto es el organismo garante de los derechos de acceso a la información pública y la protección de datos personales. Su funcionamiento se regirá por los principios de certeza, legalidad, independencia, imparcialidad, eficacia, objetividad, profesionalismo, transparencia y máxima publicidad.

2.2 Que, el diez de abril de dos mil dieciocho, se publicó en la Gaceta Oficial de la Ciudad de México, el Decreto por el que se expidió la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México (Ley de Datos local). Esta Ley en sus artículos 1 y 2, fracciones I, II, III y IV, establece su carácter de orden público y de observancia general en la Ciudad de México y que todas sus disposiciones, según corresponda, en el ámbito de su competencia, son de aplicación y observancia directa para los sujetos obligados de la Ciudad de México. Adicionalmente, la Ley de Datos establece tanto las bases mínimas y condiciones que regirán el tratamiento lícito de los datos personales, la protección de éstos y el ejercicio de los Derechos de Acceso, Rectificación, Cancelación y Oposición (ARCO), mediante procedimientos sencillos y expeditos, así como los mecanismos para garantizar el cumplimiento y la aplicación de las medidas de apremio previstas.

2.3 Que, el veintisiete de febrero de dos mil diecinueve, mediante acuerdo número 0313/SO/27-02/2019, el Pleno aprobó por unanimidad el Reglamento Interior del Instituto de Transparencia, Acceso a la Información Pública, Protección de Datos Personales y Rendición de Cuentas de la Ciudad de México, publicado el once de abril de dos mil diecinueve en la Gaceta Oficial de la Ciudad de México.

2.4 Que, el día cinco de junio de dos mil diecinueve, el Pleno del Instituto aprobó los Lineamientos Generales sobre Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México (Lineamientos de Datos) bajo el Acuerdo 1335/SO/05-06/2019, conformando en un solo cuerpo normativo, el desarrollo de las disposiciones previstas en la Ley de Datos, ello con la finalidad de facilitar, hacer más comprensible y simple el conocimiento y la exigibilidad del derecho a la protección de datos personales en el sector público de la Ciudad de México.

2.5 Que, el Pleno de la Suprema Corte de Justicia de la Nación, mediante sesión celebrada el once de junio de dos mil diecinueve, resolvió las Acciones de inconstitucionalidad 47/2018 y su acumulada 48/2018, promovidas por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales y la entonces Comisión de



Derechos Humanos del Distrito Federal, respectivamente, en la que se declararon inválidos los artículos 15, 21, 44, párrafo segundo y tercero, 77, 79, fracción V, en su porción normativa "preferentemente" y 95, de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México.

2.6 Que, en virtud de los resolutivos de la acción de inconstitucionalidad, específicamente del resolutivo sexto, se condenó al Congreso de la Ciudad de México para que, en el siguiente periodo ordinario de sesiones, legislara para suprimir los vicios advertidos en la sentencia a lo previsto en el artículo 21 de la Ley de Datos. Por lo que, debido a ello, resultó necesario reformar los Lineamientos de Datos, suprimiendo todas las porciones normativas declaradas inválidas, con el fin de tener certeza jurídica, toda vez que la citada resolución tiene alcances generales.

2.7 Que, atendiendo a las consideraciones vertidas en el párrafo anterior, mediante Acuerdo 2264/SO/14-08/2019 por el que se reforman los Lineamientos de Datos, se añadió, entre otras, la descripción de que el aviso de privacidad se pondrá a disposición en las dos modalidades: simplificado e integral, desarrollando lo que debe contener cada aviso de privacidad en los preceptos del 18 al 32 de dichos Lineamientos.

2.8 Que, el día veintidós de abril de dos mil veintidós fue aprobado por el Pleno del Instituto, el Acuerdo 1596/SO/27-04/2022 mediante el cual se reformaron los Lineamientos de Datos, a efecto de modificar el formato para la elaboración de los acuerdos de creación, modificación y/o supresión de sistemas de datos personales, así como el formato para la elaboración de los avisos de privacidad simplificado e integral, además de añadir el formato de publicación en Gaceta Oficial de la Ciudad de México, ello con la finalidad de brindar una herramienta que, a manera de referencia, les otorgue una mayor eficacia y eficiencia a los responsables en el cumplimiento de sus obligaciones en materia de protección de datos personales.

2.9 Que, conforme a lo establecido en los artículos 78 de la Ley de Datos local, el Instituto es el órgano encargado de dirigir y vigilar el cumplimiento de la Ley, así como de las normas que de ella deriven; siendo la autoridad encargada de garantizar la protección y el tratamiento correcto y lícito de datos personales.

2.10 Que, de igual forma, el artículo 79, fracción XVII, de la Ley de Datos local, señala entre las atribuciones de este Instituto el establecer en su ámbito de competencia, políticas y lineamientos para el manejo, tratamiento y protección de los sistemas de datos personales que estén en posesión de sujetos obligados, así como expedir aquellas normas que resulten necesarias para el cumplimiento de la Ley de Datos.

2.11 Que, en el artículo 25, fracción I, del Reglamento Interior del Instituto, se establece que es atribución de la Dirección de Datos Personales, proponer al Pleno, previa asesoría de la Dirección de Asuntos Jurídicos, a través de la Comisionada Presidenta o del



Comisionado Presidente, políticas, lineamientos y demás normatividad de observancia general que se considere necesaria para la tutela, tratamiento, seguridad y protección de los datos personales en posesión de los Sujetos Obligados, así como las modificaciones que resulten pertinentes.

3. DE LAS FACULTADES DEL PLENO Y DEL PRESIDENTE DEL INSTITUTO

3.1 Que, en términos de lo dispuesto en los artículos 39, 55, 61, 62 y 63, de la Ley de Transparencia, el Pleno del Instituto es el órgano superior de dirección que tiene la responsabilidad de vigilar el cumplimiento de las disposiciones constitucionales y legales en materia de transparencia, acceso a la información y protección de datos personales en la Ciudad de México por disposición de la Ley General, la Ley de Transparencia y demás normativa aplicable. Asimismo, está facultado para velar por los principios de certeza, legalidad, independencia, imparcialidad, eficacia, objetividad, profesionalismo, transparencia y máxima publicidad que guían las actividades del Instituto.

3.2 Que, los artículos 9 y 10 del Reglamento Interior del Instituto, establecen que el Pleno funcionará y tomará sus decisiones de manera colegiada; y que es la autoridad frente a las Comisionadas y Comisionados Ciudadanos en su conjunto y en lo particular, y sus resoluciones son obligatorias para éstos, aunque estén ausentes o sean disidentes al momento de tomarlas.

3.3 Que, en el artículo 12, fracción XIII, del Reglamento Interior del Instituto, se establece que es atribución del Pleno dictar políticas, lineamientos, acuerdos, y demás normatividad necesaria para ejercer las atribuciones previstas en la Constitución local, la Ley de Transparencia, la Ley de Datos Personales, la Ley Anticorrupción local y demás normatividad aplicable.

3.4 Que, el Comisionado Presidente del Instituto, con fundamento en el artículo 13, fracción V, del Reglamento Interior del Instituto, tiene la atribución de someter a la aprobación del Pleno, a propuesta propia o de cualquier otro Comisionado Ciudadano, las normas, lineamientos y demás documentos necesarios para el cumplimiento de las atribuciones del Instituto.

4. DE LA ABROGACIÓN DE LOS LINEAMIENTOS GENERALES SOBRE PROYECTO DE DATOS PERSONALES EN POSESIÓN DE SUJETOS OBLIGADOS DE LA CIUDAD DE MÉXICO Y LA APROBACIÓN DE LOS LINEAMIENTOS DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE SUJETOS OBLIGADOS DE LA CIUDAD DE MÉXICO.

4.1 Qué, en términos de los artículos 79, fracciones IX y XVII, de la Ley de Datos, el Instituto cuenta con atribuciones de vigilar el cumplimiento de la Ley de Datos y demás disposiciones



que resulten aplicables en la materia, así como establecer políticas y lineamientos para el manejo, tratamiento y protección de los sistemas de datos personales que estén en posesión de sujetos obligados, así como expedir aquellas normas que resulten necesarias para el cumplimiento de la Ley de Datos.

4.2 Que, derivado del estudio y análisis a los Lineamientos de Datos, con base en la experiencia de su implementación en la práctica, se encontraron oportunidades de mejora. Por lo cual, resultó necesario llevar a cabo su actualización y fortalecimiento. Esto permitirá contar con unos Lineamientos de Datos más apegados y homologados a lo establecido en las disposiciones previstas en la Ley de Datos. Así como también, que los sujetos obligados puedan cumplir de manera óptima con sus obligaciones respecto al tratamiento y protección de los datos personales en su poder.

4.3 Que, entre las mejoras a impactar en el presente documento normativo, se encuentran:

- a) Se cambia la denominación de los Lineamientos de Datos, para quedar como "Lineamientos de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México".
- b) Se adicionan nuevas definiciones al artículo 2, que permitirán comprender con mayor precisión el contenido de las disposiciones previstas en los Lineamientos.
- c) Se homologa en todo el documento el término de Registro Electrónico de Sistemas de Datos Personales, así como el término de Ley de Datos.
- d) Se incluye la definición de lo que se entenderá por consentimiento expreso.
- e) Se precisa que, en el aviso de privacidad, el responsable deberá describir cada una de las finalidades por las cuales se tratan datos personales de conformidad a lo dispuesto en el acuerdo de creación, o en su caso, de modificación del sistema de datos personales.
- f) Se da mayor claridad sobre los sitios o medios donde se podrá consultar el aviso de privacidad integral.
- g) Se hace la precisión de que cada sistema de datos personales deberá contar con su documento de seguridad respectivo.
- h) Se modificó el artículo relativo a las acciones del Instituto derivadas de notificaciones de vulneraciones de seguridad.
- i) Se cambió lo que refiere al deber de confidencialidad por el principio de confidencialidad.
- j) Se especifica que, para acreditar el cumplimiento de las obligaciones en materia de datos personales, la carga de la prueba recaerá en el responsable en todo momento.
- k) En el apartado de sistemas de datos personales, se hace la diferenciación entre cuándo debe el responsable crear, modificar o suprimir un sistema, así como el contenido o consideraciones por cada una de estas acciones.
- l) Se deroga el contenido relativo a la prueba confesional, debido a que en el artículo 98 de la Ley de Datos, se establece que se podrán ofrecer todo tipo de pruebas o alegatos excepto la confesional.



- m) Se modifica lo relativo a las diligencias para mejorar el procedimiento de sustanciación del recurso de revisión.
- n) Se modifican los artículos del título noveno, relativo las investigaciones previas y del procedimiento de verificación por denuncia y oficio, con la finalidad de establecer las etapas de dichos procedimientos y los plazos de cada etapa.

4.4 Que, entre los aspectos normativos que se adicionan, se encuentran los relativos a:

- a) A través del artículo 10 se adicionan los conceptos que hacen alusión al principio de lealtad.
- b) A través del artículo 17 se adicionan los conceptos que hacen alusión al principio de calidad.
- c) A través del artículo 21 se adicionan los conceptos que hacen alusión al principio de información.
- d) Mediante el artículo 35 se detalla la información que el responsable deberá dar a conocer al titular de los datos en el aviso de privacidad, respecto a las transferencias que se realicen.
- e) Se adicionó el artículo 45 relativo a la implementación de mecanismos para acreditar el cumplimiento de los principios, deberes y obligaciones que establece la normativa en materia de datos personales.
- f) Se adiciona el artículo 66 en el cual se diferencia entre los sistemas de datos personales físicos y automatizados.
- g) En el artículo donde se describen las categorías de datos personales se añade un párrafo que hace alusión a los datos que podrán ser especialmente protegidos.
- h) Se adiciona un artículo relativo al objeto de la portabilidad de los datos personales.
- i) En el artículo 125 se adiciona la obligación de que los sujetos obligados deben respaldar al oficial de protección de datos personales en todas sus acciones y decisiones en función de las atribuciones que tenga y conforme a la normativa en materia de protección de datos.
- j) En las funciones del Enlace, se añade que este deberá atender las verificaciones previstas en el artículo 112 de la Ley de Datos.
- k) Se adiciona en el artículo 133, los documentos con los cuales aquellas personas que demuestren tener un interés jurídico o legítimo, ya sea el heredero o el albacea de la persona fallecida, podrán acreditar su personalidad.
- l) Se añade al título noveno el capítulo III relativo a cumplimiento de las resoluciones.
- m) Se adiciona el artículo 205 relativo a la Imposición y ejecución de las amonestaciones públicas a partidos políticos.
- n) Se adiciona mediante los artículos 210 a 212, los criterios para determinar las medidas de apremio, las reglas generales y medios para llevar a cabo su notificación.

4.5. Que las mejoras y adiciones propuestas están en congruencia con el contenido de la Ley de Datos local y responden a los principios de calidad, confidencialidad, consentimiento, finalidad, información, lealtad, licitud, proporcionalidad, transparencia y temporalidad.



4.6 Que, derivado de los múltiples cambios señalados, se propone ~~abrogar~~ los Lineamientos Generales sobre Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México.

4.7 Que, en virtud de lo anterior, y en ejercicio de sus atribuciones, el Comisionado Presidente del Instituto, somete a consideración del Pleno, el Acuerdo por el que se aprueban los **Lineamientos de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México**.

Por las consideraciones y fundamentos anteriormente expuestos, el Pleno del Instituto de Transparencia, Acceso a la Información Pública, Protección de Datos Personales y Rendición de Cuentas de la Ciudad de México emite el siguiente:

ACUERDO

PRIMERO. Se abrogan los Lineamientos Generales sobre Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México.

SEGUNDO. Se aprueban los Lineamientos de Protección de Datos Personales en Posesión de sujetos obligados de la Ciudad de México conforme al documento que, como anexo, forma parte del presente acuerdo.

TERCERO. Se instruye a la Secretaría Técnica para que realice las acciones necesarias para publicar el presente Acuerdo y su anexo en la Gaceta Oficial de la Ciudad de México.

CUARTO. Se instruye a la Secretaría Técnica para que realice las acciones necesarias para publicar el presente Acuerdo y su anexo en el Portal de Internet del Instituto de Transparencia, Acceso a la Información Pública, Protección de Datos Personales y Rendición de Cuentas de la Ciudad de México.

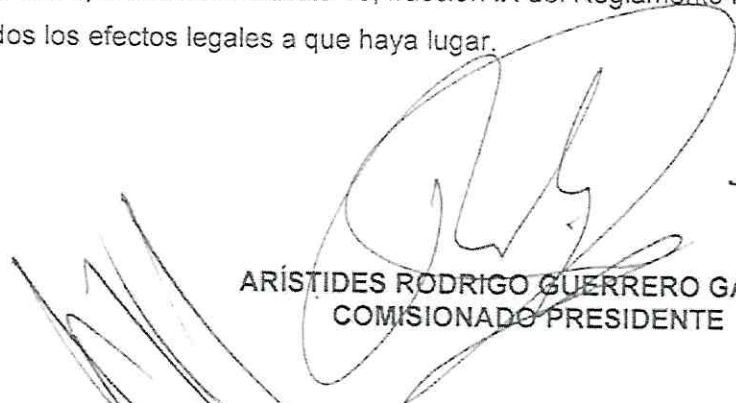
QUINTO. El presente Acuerdo y su anexo, entrarán en vigor al día siguiente de su publicación en la Gaceta Oficial de la Ciudad de México.

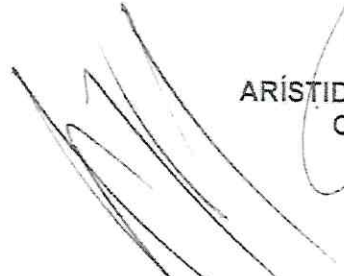


INSTITUTO DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN PÚBLICA Y PROTECCIÓN
DE DATOS PERSONALES Y RENDICIÓN DE CUENTAS DE LA CIUDAD DE MÉXICO



Así lo acordó, en Sesión Ordinaria celebrada el veinticinco de enero de dos mil veintitrés, por unanimidad de votos, de los integrantes del Pleno del Instituto de Transparencia, Acceso a la Información Pública, Protección de Datos Personales y Rendición de Cuentas de la Ciudad de México, integrado por las Comisionadas y los Comisionados Ciudadanos, que firman al calce, ante Hugo Erik Zertuche Guerrero, Secretario Técnico, de conformidad con lo dispuesto en el artículo 15, fracción IX del Reglamento Interior de este Instituto, para todos los efectos legales a que haya lugar.



ARÍSTIDES RODRIGO GUERRERO GARCÍA
COMISIONADO PRESIDENTE


JULIO CÉSAR BONILLA GUTIÉRREZ
COMISIONADO CIUDADANO


LAURA LIZETTE ENRÍQUEZ RODRÍGUEZ
COMISIONADA CIUDADANA


MARÍA DEL CARMEN NAVA POLINA
COMISIONADA CIUDADANA


MARINA ALICIA SAN MARTÍN REBOLLOSO
COMISIONADA CIUDADANA


HUGO ERIK ZERTUCHE GUERRERO
SECRETARIO TÉCNICO



INSTITUTO DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN PÚBLICA Y RENDICIÓN DE CUENTAS DE LA CIUDAD DE MÉXICO



LINEAMIENTOS DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE SUJETOS OBLIGADOS DE LA CIUDAD DE MÉXICO

TÍTULO PRIMERO DISPOSICIONES GENERALES

CAPÍTULO ÚNICO DEL OBJETO Y ÁMBITO DE VALIDEZ SUBJETIVO Y OBJETIVO DE LOS LINEAMIENTOS

Objeto

Artículo 1. Los presentes Lineamientos tienen por objeto desarrollar las disposiciones previstas en la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México.

Definiciones

Artículo 2. Además de las definiciones previstas en el artículo 3 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México, para efectos de los presentes Lineamientos se entenderá por:

- I. **Autenticación:** Comprobación de la identidad de aquella persona autorizada para el tratamiento de datos personales.
- II. **Biometría:** Método de reconocimiento de personas basado en sus datos biométricos.
- III. **Dato biométrico:** Propiedades físicas, fisiológicas, de comportamiento o rasgos de la personalidad, atribuibles a una sola persona y que son medibles.
- IV. **Documentos:** Los expedientes, reportes, estudios, actas, resoluciones, oficios, correspondencia, acuerdos, directivas, directrices, circulares, contratos, convenios, instructivos, notas, memorandos, estadísticas, o bien cualquier otro registro en posesión de los sujetos obligados sin importar su fuente o fecha de elaboración. Los documentos podrán estar en cualquier soporte, demás análogos escrito, impreso, sonoro, visual, electrónico, informático u holográfico.
- V. **Enlace:** Persona servidora pública que fungirá como vínculo entre el sujeto obligado y el Instituto para atender los asuntos relativos a la Ley en la materia.
- VI. **Identificación oficial vigente:** Se considera como identificación oficial vigente a la credencial para votar, licencia, credencial del INAPAM, pasaporte, credencial del ISSSTE o del IMSS, y/o carnet (IMSS, ISSSTE, PEMEX), las cuales deben contar con fecha de nacimiento, fecha de expedición y fotografía.



- VII. **Incidencia:** Cualquier anomalía que afecte o pudiera afectar la seguridad de los datos personales.
- VIII. **Inmovilización:** Medida cautelar que consiste en la interrupción temporal en el uso de un sistema de datos personales ordenada por el Instituto en los supuestos de tratamiento ilícito de datos de carácter personal.
- IX. **Lineamientos:** Lineamientos de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México.
- X. **Ley de Datos:** Ley de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México.
- XI. **Oficial de Protección de Datos Personales:** Especialista en materia de protección de datos personales, adscrito a la Unidad de Transparencia con suficiente jerarquía para implementar las disposiciones de la Ley de Datos y los presentes Lineamientos al interior del sujeto obligado.
- XII. **Registro Electrónico de Sistemas de Datos Personales:** Aplicación informática desarrollada por el Instituto para la inscripción de los sistemas de datos personales en posesión de los sujetos obligados de la Ciudad de México para su custodia y protección.
- XIII. **Responsable de Seguridad de Sistema de Datos Personales:** Persona designada por el responsable del sistema de datos personales a quien se le asigna formalmente las funciones de coordinar y supervisar la implementación de las medidas de seguridad aplicables en función de las atribuciones en el tratamiento de los datos personales.
- XIV. **Responsable del Sistema de Datos Personales:** Persona servidora pública que decide sobre el tratamiento de los datos personales, su finalidad, la protección y las medidas de seguridad de los mismos.
- XV. **Sistema de Verificaciones o SIVER:** La plataforma informática mediante la cual se podrán realizar las verificaciones previstas en el artículo 112 y las auditorías establecidas en el artículo 116, ambos de la Ley de Datos.
- XVI. **Soporte físico:** Son los medios de almacenamiento inteligibles a simple vista, es decir, que no requieren de ningún aparato que procese su contenido para examinar, modificar o almacenar los datos; es decir, documentos, oficios, formularios impresos llenados "a mano" o "a máquina", fotografías, placas radiológicas, carpetas, expedientes, demás análogos.
- XVII. **Soporte electrónico:** Son los medios de almacenamiento inteligibles solo mediante el uso de algún aparato con circuitos electrónicos que procese su contenido para examinar, modificar o almacenar los datos; es decir, cintas magnéticas de audio, video y datos, fichas de microfilm, discos ópticos (CDs y DVDs), discos magnéticos de audio, video y datos, fichas de microfilm, discos ópticos (CDs y DVDs), discos magnéticos (flexibles y duros), tarjetas de memoria (USB y SD) y demás medios de almacenamiento masivo no volátil.



XVIII. Suspensión: Medida cautelar ordenada por el Instituto que consiste en la interrupción temporal en el tratamiento de determinados datos personales contenidos en un sistema de datos personales.

XIX. Tipos de Fuentes de Acceso Público: Para efectos de lo previsto en el artículo 5 de la Ley de Datos, se considerarán de manera enunciativa más no limitativa como fuentes de acceso público:

- a) Las páginas de Internet o medios remotos o locales de comunicación electrónica, óptica y de otra tecnología, siempre que el sitio donde se encuentren los datos personales esté concebido para facilitar información al público y esté abierto a la consulta general;
- b) Los directorios telefónicos en términos de la normativa específica;
- c) Los diarios, gacetas o boletines oficiales, de acuerdo con su normativa;
- d) Los medios de comunicación social, y
- e) Los registros públicos conforme a las disposiciones que les resulten aplicables.

Ámbito de validez subjetivo

Artículo 3. Los presentes Lineamientos serán aplicables a cualquier autoridad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, fideicomisos y fondos públicos del Gobierno de la Ciudad de México y partidos políticos del ámbito local que en el ejercicio de sus atribuciones y funciones lleven a cabo tratamientos de datos personales de personas físicas, en términos de lo dispuesto en la Ley de Datos y los presentes Lineamientos, así como al Instituto.

Quedan excluidos del ámbito de aplicación de los presentes Lineamientos los sindicatos y cualquier otra persona física o moral que reciba y ejerza recursos públicos o realice actos de autoridad en el ámbito local, de conformidad en el artículo 1 de la Ley de Datos.

Ámbito de validez objetivo

Artículo 4. Los presentes Lineamientos serán aplicables al tratamiento de datos personales de personas físicas que obren en soportes físicos y/o electrónicos a que se refiere el artículo 4 de la Ley de Datos.

Para efectos de lo dispuesto en el artículo 3, fracciones IX y X de la Ley de Datos y los presentes Lineamientos, los datos personales podrán estar expresados en forma: numérica, alfabética, gráfica, alfanumérica, fotográfica, acústica, o en cualquier otro formato.

Tratamiento de datos personales de menores y adolescentes



Artículo 5. En el tratamiento de datos personales de menores de edad, el responsable deberá privilegiar el interés superior de la niñez, y adolescencia en términos de las disposiciones previstas en la Ley de los Derechos de Niñas, Niños y Adolescentes de la Ciudad de México, así como observar lo dispuesto en la Ley de Datos y los presentes Lineamientos.

Interpretación

Artículo 6. Los presentes Lineamientos se interpretarán conforme a lo dispuesto en el artículo 7 de la Ley de Datos.

TÍTULO SEGUNDO PRINCIPIOS Y DEBERES

CAPÍTULO ÚNICO DE LOS PRINCIPIOS DE PROTECCIÓN DE DATOS PERSONALES

Principios generales de protección de datos personales

Artículo 7. En todo tratamiento de datos personales el responsable deberá observar los siguientes principios rectores de la protección de datos personales: calidad, confidencialidad, consentimiento, finalidad, información, lealtad, licitud, proporcionalidad, transparencia y temporalidad previstos en el artículo 9 de la Ley de Datos.

Finalidad

Artículo 8. Para efectos de lo previsto en el artículo 10 primer párrafo de la Ley de Datos y los presentes Lineamientos se entenderá que las finalidades son:

- I. **Concretas:** cuando el tratamiento de los datos personales atiende a la consecución de fines específicos o determinados, sin que admitan errores, distintas interpretaciones o provoquen incertidumbre, dudas o confusión en el titular;
- II. **Explícitas:** cuando se expresan y se dan a conocer de manera clara en el aviso de privacidad las finalidades relativas al tratamiento de datos personales;
- III. **Lícitas:** cuando las finalidades que justifiquen el tratamiento de los datos personales son acordes con las atribuciones o facultades del responsable, conforme a lo previsto en la legislación mexicana y el derecho internacional que le resulte aplicable, y
- IV. **Legítimas:** cuando las finalidades que motivan el tratamiento de los datos personales se encuentran habilitadas por el consentimiento del titular, salvo que se actualice algunas de las causales de excepción previstas en el artículo 16 de la Ley de Datos.

Tratamiento para finalidades distintas



Artículo 9. En el tratamiento de datos personales para finalidades distintas a aquellas que motivaron su tratamiento original a que se refiere el artículo 10 segundo párrafo de la Ley de Datos, el responsable deberá considerar:

- I. La expectativa razonable de protección de datos personales del titular, basada en la relación que tiene con este;
- II. La naturaleza de los datos personales;
- III. Las consecuencias del tratamiento posterior de los datos personales para el titular, y
- IV. Las medidas adoptadas para que el tratamiento posterior de los datos personales cumpla con las disposiciones previstas en la Ley de Datos y los presentes Lineamientos.

Lealtad

Artículo 10. En términos de lo dispuesto en el artículo 11 de la Ley de Datos, se entenderá:

- I. Por medios engañosos o fraudulentos, aquellos que el responsable utilice para tratar los datos personales con dolo, mala fe o negligencia;
- II. Que el responsable privilegia los intereses del titular cuando el tratamiento de datos personales que efectúa no da lugar a una discriminación o trato injusto o arbitrario contra éste, y
- III. Por expectativa razonable de protección de datos personales, la confianza que el titular ha depositado en el responsable respecto a que sus datos personales serán tratados conforme a lo señalado en el aviso de privacidad y en cumplimiento a las disposiciones previstas en la Ley de Datos y los presentes Lineamientos.

Consentimiento

Artículo 11. El consentimiento será la manifestación de la voluntad libre, específica, informada e inequívoca del titular de forma verbal, por escrito, por medios electrónicos, ópticos, signos inequívocos o por cualquier otra tecnología, de acuerdo con lo dispuesto en la fracción IV del artículo 12 de la Ley de Datos.

Para la obtención del consentimiento, el responsable deberá facilitar al titular un medio sencillo y gratuito a través del cual pueda manifestar su voluntad, mismo que deberá permitir acreditar de manera indubitable y, en su caso, documentar que el titular otorgó su conocimiento ya sea a través de una declaración o una acción afirmativa clara.

El silencio, las casillas previamente marcadas, la inacción del titular o cualquier otra conducta o mecanismo similar a los mencionados no podrán considerarse como consentimiento del titular.



La carga de la prueba para acreditar la obtención del conocimiento expreso, **correrá a cargo** del responsable.

Consentimiento expreso

Artículo 12. Se entenderá como consentimiento expreso a aquel que se otorga de forma concreta, clara y directa, por parte del titular de los datos personales, autorizando realizar el tratamiento de datos personales que se informa, a través de la declaración de su voluntad, que podrá realizarse por escrito o de forma verbal, a través de su firma autógrafa, firma electrónica, o cualquier mecanismo de autenticación que al efecto se establezca

Consentimiento escrito y verbal

Artículo 13. Para efectos de lo dispuesto en el artículo 12 de la Ley de Datos y los presentes Lineamientos se entenderá que el titular otorga su consentimiento:

- I. De manera verbal cuando lo externe de forma presencial o mediante el uso de cualquier otra tecnología que permita la interlocución oral, en ambos casos, ante la persona que represente al responsable, y
- II. De forma escrita cuando manifieste su voluntad en un documento físico o electrónico, a través de una declaración en sentido afirmativo, firma autógrafa, huella dactilar, firma electrónica o cualquier mecanismo o procedimiento equivalente autorizado por la normativa aplicable.

Obtención del consentimiento del titular cuando los datos personales se recaban directamente de este

Artículo 14. El responsable deberá obtener el consentimiento del titular para el tratamiento de sus datos personales, de manera previa, cuando los recabe directamente de este y, en su caso, sea requerido conforme al artículo 12 de la Ley de Datos y de los presentes Lineamientos.

Para los efectos de los presentes Lineamientos, se entenderá que el responsable obtiene los datos personales directamente del titular, cuando este los proporciona a la persona que lo representa de manera presencial o por algún medio que permita su entrega directa como podrán ser medios electrónicos, ópticos, sonoros, visuales, vía telefónica, internet o cualquier otra tecnología y/o medio.

Obtención del consentimiento del titular cuando los datos personales se recaben indirectamente de este

Artículo 15. Cuando el responsable recabe datos personales indirectamente del titular y se requiera de su consentimiento conforme a lo previsto en el artículo 12 de la Ley de Datos y de los presentes Lineamientos, este no podrá tratar los datos personales hasta que cuente con la manifestación de la voluntad libre, específica e informada del titular, mediante la cual autoriza el tratamiento de los mismos ya sea de manera tácita o expresa, según corresponda.



Para los efectos de los presentes Lineamientos, se entenderá que el responsable obtiene los datos personales indirectamente del titular cuando no han sido proporcionados en los términos a que se refiere el artículo anterior, segundo párrafo de los presentes Lineamientos.

Revocación del consentimiento

Artículo 16. En cualquier momento, el titular podrá revocar el consentimiento que ha otorgado para el tratamiento de sus datos personales sin que se le atribuyan efectos retroactivos a la revocación, a través del ejercicio de los derechos de cancelación y oposición de conformidad con lo dispuesto en la Ley de Datos, los presentes Lineamientos y demás normativa aplicable.

Calidad

Artículo 17. Para efectos del artículo 17, primer párrafo, de la Ley de Datos, se entenderá que los datos personales son:

- I. **Exactos y correctos:** cuando los datos personales en posesión del responsable no presentan 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 del titular.

Presunción de calidad de los datos personales cuando se obtienen indirectamente del titular.

Artículo 18. Cuando los datos personales hayan sido obtenidos indirectamente del titular, el responsable deberá adoptar medidas de cualquier naturaleza, dirigidas a garantizar que estos responden al principio de calidad, de acuerdo con la categoría de datos personales, así como las condiciones y medios del tratamiento.

Supresión de los datos personales

Artículo 19. En la supresión de los datos personales a que se refieren los artículos 17 párrafo segundo y 18 de la Ley de Datos, el responsable deberá establecer políticas, métodos y técnicas orientadas a la supresión definitiva de estos, de tal manera que la probabilidad de recuperarlos y reutilizarlos sea imposible.

Al establecer las políticas, métodos y técnicas a que se refiere el párrafo anterior, el responsable debe considerar, tanto los siguientes atributos mínimos como los medios de almacenamiento, físicos y/o electrónicos en los que se encuentren los datos personales:

- I. **Irreversibilidad:** que el procedimiento utilizado no permita recuperar los datos personales;



- II. **Seguridad y confidencialidad:** que en la eliminación definitiva de los datos personales se consideren los principios de temporalidad y confidencialidad, así como el deber de seguridad a que se refieren la Ley de Datos y los presentes Lineamientos, y
- III. **Favorable al medio ambiente:** que el método utilizado produzca el mínimo de emisiones y desperdicios que afecten el medio ambiente.

Criterio de minimización

Artículo 20. El responsable deberá realizar todos los esfuerzos razonables para limitar los datos personales tratados al mínimo necesario, con relación a las finalidades que motivan su tratamiento.

Información

Artículo 21. El responsable deberá informar a los titulares, a través del aviso de privacidad, la existencia y las características principales del tratamiento al que serán sometidos sus datos personales. Por regla general, todo responsable está obligado a cumplir con el principio de información y poner a disposición del titular el aviso de privacidad de conformidad con lo dispuesto en los artículos 3, fracción II, 9, numeral 6, 20, 21 de la Ley de Datos y los presentes Lineamientos, con independencia de que no se requiera el consentimiento del titular para el tratamiento de sus datos personales.

Objeto del aviso de privacidad

Artículo 22. El aviso de privacidad tiene por objeto informar al titular sobre los alcances y condiciones generales del tratamiento a que serán sometidos sus datos personales, a fin de que este en posibilidad de tomar decisiones informadas sobre el uso de estos y, en consecuencia, mantener el control y disposición de los mismos.

Características del aviso de privacidad

Artículo 23. El aviso de privacidad deberá caracterizarse por ser sencillo con la información necesaria, expresado en lenguaje claro y comprensible y con una estructura y diseño que facilite su entendimiento, para lo cual deberá atender al perfil de los titulares a quienes será dirigido, con la finalidad de que sea un mecanismo de información práctico y eficiente.

En el aviso de privacidad queda prohibido:

- I. Usar frases inexactas, ambiguas o vagas;
- II. Incluir textos o formatos que induzcan a los titulares a elegir una opción en específico;
- III. Marcar previamente casillas, en caso de que estas se incluyan, para que los titulares otorguen su consentimiento, o bien;
- IV. Incluir declaraciones orientadas, afirmando que el titular ha consentido el tratamiento de sus datos personales sin manifestación alguna de su parte, y



V. Remitir a textos o documentos que no estén disponibles para los titulares

Medios de difusión del aviso de privacidad

Artículo 24. El responsable podrá difundir, poner a disposición o reproducir el aviso de privacidad en formatos físicos y electrónicos, ópticos, sonoros, visuales, o de cualquier otra tecnología que permita su eficaz comunicación y deberá ubicar el aviso de privacidad en un lugar visible que facilite la consulta del titular y que le permita acreditar fehacientemente el cumplimiento de esta obligación ante el Instituto.

Indistintamente de lo señalado en el párrafo anterior, el responsable deberá poner a disposición el aviso de privacidad al menos en los siguientes medios:

- I. Físicos: De manera visible y accesible;
- II. Electrónicos: Deberá estar publicado y disponible en el medio electrónico institucional.

En todos los casos, la carga de la prueba para acreditar la puesta a disposición del aviso de privacidad recaerá en el responsable.

Modalidades del aviso de privacidad

Artículo 25. El aviso de privacidad se pondrá a disposición del titular en dos modalidades: simplificado e integral:

- I. El aviso simplificado deberá contener la siguiente información:
 - a) La denominación del responsable;
 - b) Nombre del Sistema de Datos Personales;
 - c) Las finalidades del tratamiento para las cuales se obtienen los datos personales, distinguiendo aquéllas que requieran el consentimiento del titular;
 - d) Cuando se realicen transferencias de datos personales que requieran consentimiento, se deberá informar: Las autoridades, poderes, entidades, órganos y organismos gubernamentales de los tres órdenes de gobierno y las personas físicas o morales a las que se transfieren los datos personales, así como, las finalidades de estas transferencias;
 - e) Los mecanismos y medios disponibles para que el titular, en su caso, pueda manifestar su negativa para el tratamiento de sus datos personales para finalidades y transferencias de datos personales que requieren el consentimiento del titular, y
 - f) El sitio donde se podrá consultar el aviso de privacidad integral.
- II. El aviso de privacidad integral, además de lo dispuesto en la fracción anterior, deberá contener:
 - a) El domicilio del responsable;
 - b) Los datos personales que serán sometidos a tratamiento, identificando aquéllos que son sensibles;



- c) El fundamento legal que faculta al responsable para llevar a cabo el tratamiento;
- d) Las finalidades del tratamiento para las cuales se obtienen los datos personales, distinguiendo aquellas que requieren el consentimiento del titular;
- e) Los mecanismos, medios y procedimientos disponibles para ejercer los derechos ARCO;
- f) El domicilio de la Unidad de Transparencia, y
- g) Los medios a través de los cuales el responsable comunicará a los titulares los cambios al aviso de privacidad.

Momentos para la puesta a disposición del aviso de privacidad

Artículo 26. El responsable deberá poner a disposición del titular, el aviso de privacidad simplificado en un primer momento, lo cual no le impide que pueda dar a conocer el aviso de privacidad integral, desde un inicio, si así lo prefiere, conforme a las siguientes reglas:

- I. De manera previa a la obtención de los datos personales, cuando los mismos se obtengan directamente del titular, independientemente de los formatos o medios físicos y/o electrónicos utilizados para tal fin, o
- II. Al primer contacto con el titular o previo al aprovechamiento de los datos personales, cuando éstos se hubieren obtenido de manera indirecta del titular.

El aviso de privacidad integral deberá estar disponible y publicado, de manera permanente, en el medio físico y electrónico con que cuente el sujeto obligado, los cuales corresponden a lo informado en el aviso de privacidad simplificado, a efecto de que el titular lo consulte en cualquier momento.

Denominación del responsable en el aviso de privacidad

Artículo 27. El responsable deberá señalar su denominación completa y podrá incluir de manera adicional, la denominación, abreviada o acrónimos con los cuales es identificado comúnmente por el público en general, concretamente por el público objetivo a quien va dirigido el aviso de privacidad simplificado.

Finalidades descritas en el aviso de privacidad en ambas modalidades

Artículo 28. El responsable deberá describir puntualmente cada una de las finalidades para las cuales se traten los datos personales de conformidad a lo dispuesto en el acuerdo de creación, o en su caso, de modificación del sistema de datos personales.

Mecanismos y medios para manifestar la negativa del titular en el aviso de privacidad simplificado



Artículo 29. El responsable deberá incluir o informar sobre los mecanismos y medios que tiene habilitados para que el titular pueda manifestar su revocación del consentimiento como negativa para el tratamiento de sus datos personales para aquellas finalidades que requieran de su consentimiento en términos de la Ley de Datos y de los presentes Lineamientos, así como para la transferencia de sus datos personales cuando su autorización sea exigible en términos de lo previsto en la Ley de Datos.

El responsable podrá valerse de la inclusión de casillas u opciones de marcado en el propio aviso de privacidad, o bien, cualquier otro medio que determine pertinente, siempre y cuando el medio esté disponible al momento en que el titular consulte el aviso de privacidad y permita que este manifieste su negativa, previo al tratamiento de sus datos personales o la transferencia de estos, según corresponda.

Sitio donde se podrá consultar el aviso de privacidad integral

Artículo 30. El responsable deberá señalar en el aviso de privacidad simplificado el sitio electrónico, el lugar físico y en su caso, el mecanismo implementado para que los titulares puedan conocer el aviso de privacidad integral, a través de los medios de contacto oficiales de la unidad de transparencia.

El responsable deberá considerar el perfil de los titulares, la forma en que mantiene contacto o comunicación con éstos, que sean gratuitos, de fácil acceso, con la mayor cobertura posible y que estén debidamente habilitados y disponibles en todo momento para consulta del titular.

Datos personales en el aviso de privacidad integral

Artículo 31. El responsable deberá referir los datos personales solicitados para el tratamiento que llevará a cabo, tanto los que recaba directamente del titular, así como aquellos que obtiene indirectamente, distinguiendo expresamente los datos personales de carácter sensible.

El responsable deberá cumplir con esta obligación, identificando puntualmente cada uno de los datos personales solicitados para el tratamiento que llevará a cabo.

El responsable deberá considerar los tipos de datos de acuerdo con las categorías de datos personales, en función de lo que establece el artículo 67 de los presentes Lineamientos.

El responsable deberá señalar la existencia del sistema de datos personales en el cual están resguardados los datos personales, en cumplimiento a lo establecido en los artículos 3, fracción XXIX, 36 y 37 de la Ley de Datos.

Fundamento legal en el aviso de privacidad

Artículo 32. El responsable deberá señalar el o los artículos, apartados, fracciones, incisos y nombre de los ordenamientos o disposición normativa vigente que le faculta o le confiera atribuciones para realizar el tratamiento de datos personales que informa en el aviso de privacidad, precisando su fecha de publicación o, en su caso, la fecha de la última reforma o modificación, con independencia de que dicho tratamiento requiera del consentimiento del titular.



Mecanismos y medios para el ejercicio de los derechos ARCO en el aviso de privacidad integral

Artículo 33. El responsable deberá informar sobre los mecanismos, medios y procedimientos habilitados para atender las solicitudes para el ejercicio de los derechos ARCO.

En el caso del procedimiento, el responsable podrá describirlo puntualmente en el aviso de privacidad, o bien, remitir al titular a los medios que tiene disponibles para que conozca dicho procedimiento.

En ambos casos, el responsable deberá informar, al menos, lo siguiente:

- I. Los requisitos que deberá contener la solicitud para el ejercicio de los derechos ARCO a que se refiere señalados en el artículo 41 de la Ley de Datos;
- II. Los medios a través de los cuales el titular podrá presentar solicitudes para el ejercicio de los derechos ARCO;
- III. Los formularios, sistemas y otros métodos simplificados que, en su caso, el Instituto hubiere establecido para facilitar al titular el ejercicio de sus derechos ARCO;
- IV. Los medios habilitados para dar respuesta a las solicitudes para el ejercicio de los derechos ARCO;
- V. La modalidad o medios de reproducción de los datos personales;
- VI. Los plazos establecidos dentro del procedimiento, los cuales no deberán contravenir lo previsto en los artículos 49, 50, 51, 52 y 53 de la Ley de Datos, y
- VII. El derecho que tiene el titular de presentar un recurso de revisión ante el Instituto en caso de estar inconforme con la respuesta.

Domicilio en el aviso de privacidad integral

Artículo 34. El responsable deberá indicar su domicilio, así como la ubicación precisa de la oficina de su Unidad de Transparencia, incluyendo la calle, número, piso, colonia, alcaldía, código postal y entidad federativa. Asimismo, podrá incluir otros datos de contacto que, de manera enunciativa mas no limitativa, son: dirección de su página de internet, correo electrónico institucional y número telefónico, habilitados para la atención del público en general.

Información de las transferencias de datos personales en el aviso de privacidad integral



Artículo 35. Para informar al titular sobre las transferencias, nacionales y/o internacionales de datos personales que, en su caso, efectúe y que no requieran de su consentimiento, el responsable deberá indicar lo siguiente en el aviso de privacidad integral:

- I. Los destinatarios o terceros receptores, de carácter público o privado, nacional y/o internacional, de los datos personales; identificando cada uno de éstos por su nombre, denominación o razón social;
- II. Las finalidades de las transferencias de los datos personales relacionadas por cada destinatario o tercero receptor.
- III. El fundamento legal que lo faculta o autoriza para llevarlas a cabo, señalando el o los artículos, apartados, fracciones, incisos y nombre de los ordenamientos o disposición normativa vigente.

Cambios al aviso de privacidad

Artículo 36. El responsable deberá señalar el o los medios disponibles a través de los cuales hará del conocimiento del titular los cambios o actualizaciones efectuadas tanto al aviso de privacidad simplificado, como al aviso de privacidad integral, así como indicar la fecha de elaboración, o bien, de su última actualización.

Casos en los que se requiere un nuevo aviso de privacidad

Artículo 37. El responsable deberá poner a disposición del titular, un nuevo aviso de privacidad, de conformidad con la Ley de Datos y los presentes Lineamientos cuando:

- I. Cambie su identidad;
- II. Requiera recabar datos personales sensibles adicionales a aquellos informados en el aviso de privacidad original, los cuales no se obtengan de manera directa del titular y se requiera de su consentimiento para el tratamiento de los datos adicionales;
- III. Cambie las finalidades señaladas en el aviso de privacidad original, o
- IV. Modifique las condiciones de las transferencias de datos personales o se pretendan realizar transferencias no previstas inicialmente y el consentimiento del titular sea necesario.

Políticas y programas de protección de datos personales

Artículo 38. El responsable deberá implementar políticas y programas de protección de datos personales para establecer los elementos y actividades de dirección, operación y control de todos los procesos que impliquen un tratamiento de datos personales. Dichos procesos deberán estar sustentados en las atribuciones y funciones explícitas del responsable. Todo lo anterior, a efecto de proteger estos de manera sistemática y continua de conformidad con lo ordenado por el artículo 23, fracciones I y II de la Ley de Datos.



Las políticas y programas de protección de datos personales a que se refiere el párrafo anterior de los presentes Lineamientos deberán ser aprobados, coordinados y supervisados por su Comité de Transparencia.

El responsable deberá prever y autorizar recursos, de conformidad con la normativa que resulte aplicable, para la implementación y cumplimiento de estos.

Capacitación

Artículo 39. Con relación al artículo 23, fracción III de la Ley de Datos, el responsable deberá establecer anualmente un programa de capacitación y actualización en materia de protección de datos personales dirigidos a su personal y a encargados, el cual deberá ser aprobado, coordinado y supervisado por el Comité de Transparencia.

Asimismo, en términos del artículo 26, fracción VIII de la Ley de Datos, la capacitación relativa a los sistemas de datos personales corresponde al responsable.

Sistemas de supervisión y vigilancia

Artículo 40. Para el adecuado cumplimiento de lo establecido en el artículo 23 fracciones IV y V de la Ley de Datos, por regla general, el responsable deberá revisar las políticas y programas de seguridad y el sistema de supervisión y vigilancia implementado, al menos, cada dos años. Lo anterior, salvo los casos en los que el responsable realice modificaciones sustanciales a los tratamientos de datos personales que lleve a cabo y, en consecuencia, amerite una actualización previa al plazo establecido en el presente artículo.

Garantía del ejercicio de los derechos ARCO

Artículo 41. El responsable deberá garantizar a las personas en todo momento, el ejercicio de los derechos de Acceso, Rectificación, Cancelación y Oposición, en cumplimiento a lo ordenado en el artículo 23, fracción VI de la Ley de Datos, para lo cual deberá brindar asesoría de manera accesible respecto a dudas o quejas de los titulares, mantener comunicación directa, y considerar el perfil de cada persona.

Protección de datos personales por diseño

Artículo 42. En el diseño, desarrollo e implementación de políticas públicas, programas, servicios, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento de datos personales, el responsable deberá aplicar medidas de carácter administrativo, técnico, físico, u otras de cualquier naturaleza que le permitan cumplir de forma efectiva todas las obligaciones previstas en la Ley de Datos y los presentes Lineamientos. Ello, de conformidad con lo dispuesto en el artículo 23, fracción VII de la Ley de Datos.

Para el propósito señalado en el párrafo anterior, el responsable deberá considerar los avances tecnológicos, los costos de implementación, la naturaleza, el ámbito, el contexto, los fines del tratamiento de los datos personales, los riesgos de diversa probabilidad y gravedad que entraña



este para el derecho a la protección de datos personales a los titulares, así como a otros factores que considere relevantes.

Protección de datos personales por defecto

Artículo 43. El responsable deberá implementar las medidas técnicas y organizativas necesarias orientadas a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales estrictamente necesarios para cumplir con su finalidad.

Tratamiento de datos personales sensibles

Artículo 44. El responsable no podrá llevar a cabo el tratamiento de datos personales cuando tenga como efecto la discriminación de los titulares por su origen étnico o racial, su estado de salud presente, pasado o futuro, su información genética, sus opiniones políticas, su religión o creencias filosóficas o morales y/o su preferencia sexual.

Implementación de mecanismos para acreditar el cumplimiento de los principios, deberes y obligaciones

Artículo 45. El responsable deberá adoptar políticas e implementar mecanismos para asegurar y acreditar el cumplimiento de los principios, deberes y demás obligaciones establecidas en la Ley de Datos y los presentes Lineamientos; así como establecer aquellos mecanismos necesarios para evidenciar dicho cumplimiento ante los titulares y el Instituto.

Adicionalmente a lo dispuesto en los artículos 22 y 23 de la Ley de Datos, en la adopción de las políticas e implementación de mecanismos a que se refiere el presente artículo, el responsable deberá considerar, de manera enunciativa más no limitativa, el desarrollo tecnológico y las técnicas existentes; la naturaleza, contexto, alcance y finalidades del tratamiento de los datos personales; las atribuciones y facultades del responsable y demás cuestiones que considere convenientes. Para el cumplimiento de la presente obligación, el responsable podrá valerse de estándares, mejores prácticas nacionales o internacionales, esquemas de mejores prácticas, o cualquier otro mecanismo que determine adecuado para tales fines.

Deber de seguridad

Artículo 46. El responsable deberá establecer y mantener medidas de seguridad de carácter administrativo, físico y técnico para la protección de los datos personales en su posesión de conformidad con lo previsto en los artículos 24, 25, 26 y 27 de la Ley de Datos, con el objetivo de impedir, que cualquier tratamiento de los datos personales contravenga las disposiciones de dicho ordenamiento y los presentes Lineamientos.

Las medidas de seguridad a las que se refiere el párrafo anterior constituyen los mínimos exigibles, por lo que el responsable podrá adoptar las medidas adicionales que estime necesarias para brindar mayores garantías en la protección de los datos personales en su posesión.

Lo anterior, sin perjuicio de lo establecido por aquellas disposiciones vigentes en materia de seguridad de la información emitidas por otras autoridades, cuando estas contemplen una mayor



protección para el titular o complementen lo dispuesto en la Ley de Datos y en los presentes Lineamientos.

Contenido de las políticas internas de gestión y tratamiento de los datos personales

Artículo 47. El responsable deberá incluir en el diseño e implementación de las políticas internas para la gestión y el tratamiento de los datos personales de acuerdo con lo establecido en el artículo 26, fracción I de la Ley de Datos, al menos lo siguiente:

- I. El cumplimiento de todos los principios, deberes, derechos y demás obligaciones en la materia, de conformidad con lo previsto en la Ley de Datos y los presentes Lineamientos;
- II. Los roles y responsabilidades específicas de los involucrados internos y externos dentro de su organización, relacionados con el tratamiento de datos personales que efectúen;
- III. Las sanciones en caso de incumplimiento;
- IV. La identificación del ciclo de vida de los datos personales respecto de cada tratamiento que se efectúe; considerando la obtención, almacenamiento, uso, procesamiento, divulgación, retención, destrucción o cualquier otra operación realizada durante dicho ciclo en función de las finalidades para las que fueron recabados;
- V. El proceso general para el establecimiento, actualización, monitoreo y revisión de los mecanismos y medidas de seguridad; considerando el análisis de riesgo realizado previamente al tratamiento de los datos personales, y
- VI. El proceso general de atención de los derechos ARCO.

Funciones y obligaciones

Artículo 48. El responsable deberá establecer y documentar los roles y las responsabilidades del personal involucrado en el tratamiento de datos personales de conformidad con el artículo 26, fracción II de la Ley de Datos, así como la cadena de rendición de cuentas de todas las personas que traten datos personales en su organización, conforme al sistema de gestión implementado.

El responsable deberá establecer mecanismos para asegurar que todas las personas involucradas en el tratamiento de datos personales en su organización conozcan sus funciones para el cumplimiento de los objetivos del sistema de gestión, así como las consecuencias de su incumplimiento.

Inventario de datos personales



Artículo 49. Con relación a lo previsto en el artículo 26, fracción III de la Ley de Datos, el responsable deberá elaborar un inventario con la información básica de cada tratamiento de datos personales contenidos en el sistema respectivo.

El inventario que deberá contar por lo menos con los siguientes elementos:

- I. El catálogo de medios físicos y electrónicos a través de los cuales se obtienen los datos personales;
- II. Las finalidades de cada tratamiento de datos personales;
- III. El catálogo de los tipos de datos personales que se traten, indicando si son sensibles o no;
- IV. El catálogo de formatos de almacenamiento, así como la descripción general de la ubicación física y/o electrónica de los datos personales;
- V. La lista de las personas servidoras públicas que tienen acceso a los sistemas de tratamiento;
- VI. En su caso, el nombre completo o denominación o razón social del encargado y el instrumento jurídico que formaliza la presentación de los servicios que brinda al responsable, y
- VII. En su caso los destinatarios o terceros receptores de las transferencias que se efectúen, así como las finalidades que justifican estas.

Ciclo de vida de los datos personales en el inventario de estos

Artículo 50. Aunado a lo dispuesto en el numeral anterior de los presentes Lineamientos, en la elaboración del inventario de datos personales, el responsable deberá considerar el ciclo de vida de los datos personales conforme a lo siguiente:

- I. La obtención de los datos personales;
- II. El almacenamiento de los datos personales;
- III. El uso de los datos personales conforme a su acceso, manejo, aprovechamiento, monitoreo y procesamiento, lo que incluye los sistemas físicos y/o electrónicos utilizados para tal fin;
- IV. La divulgación de los datos personales considerando las remisiones y transferencias que, en su caso, se efectúen;
- V. El bloqueo de los datos personales, en su caso, y
- VI. La cancelación, supresión o destrucción de los datos personales.



El responsable deberá identificar el riesgo inherente de los datos personales, contemplando su ciclo de vida y los activos involucrados en su tratamiento, como podrían ser hardware, software, personal o cualquier otro recurso humano o material que resulte pertinente considerar.

Análisis de riesgos

Artículo 51. Para dar cumplimiento al artículo 26, fracción IV de la Ley de Datos, el responsable deberá realizar un análisis de riesgos de los datos personales tratados considerando lo siguiente:

- I. Los requerimientos regulatorios, códigos de conducta o mejores prácticas de un sector específico;
- II. El valor de los datos personales de acuerdo con su clasificación previamente definida y su ciclo de vida;
- III. El valor y exposición de los activos involucrados en el tratamiento de los datos personales;
- IV. Las consecuencias negativas para los titulares que pudieran derivar de una vulneración de seguridad ocurrida, y
- V. Los factores previstos en el artículo 25 de la Ley de Datos.

Análisis de la brecha

Artículo 52. Para el debido cumplimiento de la obligación establecida en el artículo 26, fracción V de la Ley de Datos, en la realización del análisis de brecha el responsable deberá considerar lo siguiente:

- I. Las medidas de seguridad existentes y efectivas;
- II. Las medidas de seguridad faltantes, y
- III. La existencia de nuevas medidas de seguridad que pudieren remplazar a uno o más controles implementados actualmente.

Plan de trabajo

Artículo 53. De conformidad con lo dispuesto en el artículo 26 fracción VI de la Ley de Datos, el responsable deberá elaborar un plan de trabajo que defina las acciones a implementar de acuerdo con el resultado del análisis de riesgos y del análisis de brecha, en el cual debe dar prioridad a las medidas de seguridad más relevantes e inmediatas a establecer.

Para lo anterior, el responsable debe tomar en consideración los recursos designados; el personal interno y externo en su organización y las fechas compromiso para la implementación de las medidas de seguridad nueva o faltante.

Monitoreo y supervisión periódica de las medidas de seguridad implementadas



Artículo 54. Con relación al artículo 26, fracción VII de la Ley de Datos, el responsable deberá evaluar y medir los resultados de las políticas, planes, procesos y procedimientos implementados en materia de seguridad y tratamiento de los datos personales, a fin de verificar el cumplimiento de los objetivos propuestos y, en su caso, implementar mejoras de manera continua.

Para cumplir con lo dispuesto en el párrafo anterior del presente artículo, el responsable deberá monitorear continuamente lo siguiente:

- I. Los nuevos activos que se incluyan en la gestión de riesgos;
- II. Las modificaciones necesarias a los activos, como podría ser el cambio o migración tecnológica, entre otras;
- III. Las nuevas amenazas que podrían estar activas dentro y fuera de su organización que no han sido valoradas;
- IV. La posibilidad de que vulnerabilidades nuevas o incrementadas sean explotadas por las amenazas correspondientes;
- V. Las vulnerabilidades identificadas para determinar aquellas expuestas a amenazas nuevas o pasadas que vuelvan a surgir;
- VI. El cambio en el impacto o consecuencias de amenazas valoradas, vulnerabilidades y riesgos en conjunto, que resulten en el nivel inaceptable de riesgo, y
- VII. Los incidentes y vulneraciones de seguridad ocurridas.

Aunado a lo previsto en las fracciones anteriores del presente artículo, el responsable deberá contar con un programa de auditoría, interno y/o externo, para monitorear y revisar la eficacia del sistema de gestión.

Capacitación

Artículo 55. Para el cumplimiento de lo previsto en el artículo 26, fracción VIII de la Ley de Datos, el responsable deberá diseñar e implementar programas a corto, mediano y largo plazo que tengan por objeto capacitar a los involucrados internos y externos de su organización, considerando sus roles y responsabilidades asignadas para el tratamiento y seguridad de los datos personales y el perfil de sus puestos.

En el diseño e implementación de los programas de capacitación, el responsable deberá tomar en cuenta lo siguiente:

- I. Los requerimientos y actualizaciones del sistema de gestión;
- II. La legislación vigente en materia de protección de datos personales y las mejores prácticas relacionadas con el tratamiento de estos;



- III. Las consecuencias del incumplimiento de los requerimientos legales o requisitos organizacionales, y
- IV. Las herramientas tecnológicas relacionadas o utilizadas para el tratamiento de los datos personales y para la implementación de las medidas de seguridad.

Sistema de gestión

Artículo 56. El responsable deberá implementar un sistema de gestión en términos de lo dispuesto en el artículo 27 de la Ley de Datos, el cual permita planificar, establecer, implementar, operar, monitorear, revisar, mantener y mejorar las medidas de seguridad de carácter administrativo, físico y técnico aplicadas a los datos personales; tomando en consideración los estándares nacionales e internacionales en materia de protección de datos personales y seguridad de la información.

Documento de seguridad

Artículo 57. El documento de seguridad de cada sistema de datos personales deberá contener, como mínimo, lo siguiente:

- I. El inventario de datos personales en los sistemas de datos;
- II. Las funciones y obligaciones de las personas que intervengan en el tratamiento de datos personales, usuarios y encargados, en el caso de que los hubiera;
- III. Registro de incidencias;
- IV. Identificación y autenticación;
- V. Control de acceso; gestión de soportes y copias de respaldo y recuperación;
- VI. El análisis de riesgos;
- VII. El análisis de brecha;
- VIII. Responsable de seguridad de sistema de datos personales;
- IX. Registro de acceso y telecomunicaciones;
- X. Los mecanismos de monitoreo y revisión de las medidas de seguridad;
- XI. El plan de trabajo, y
- XII. El programa general de capacitación.



El responsable elaborará e implementará las normas internas de seguridad que serán obligatorias para todas las personas autorizadas que intervienen en el tratamiento de datos personales debiendo tomar en cuenta lo dispuesto en la Ley de Datos y en los presentes Lineamientos.

El responsable deberá actualizar el documento de seguridad anualmente, o cuando se produzcan modificaciones relevantes en el tratamiento de los datos que impliquen un cambio en el nivel de riesgo; ante acciones de mejora continua derivadas del monitoreo del sistema de seguridad; ante una vulneración ocurrida; ante la implementación de acciones preventivas y correctivas derivadas de una vulneración de seguridad, o bien por recomendación del Instituto.

Manejo de incidentes para mitigar las vulneraciones a la seguridad

Artículo 58. El responsable deberá implementar medidas de seguridad para prevenir que se presente un incidente, así como poder identificar una vulneración de seguridad. Para ello deberá considerar lo siguiente:

- I. **Preparación:** Para la gestión de incidentes, se deberá designar a una persona, equipo o área que deberá contar con políticas específicas, acceso a los activos y herramientas para el monitoreo y atención de las alertas de seguridad, en función del tamaño del sujeto obligado.
- II. **Respaldo:** El responsable deberá crear respaldos o copias de seguridad al menos mensualmente, con la finalidad de poder recuperar la información en caso de que la misma sea dañada, robada o destruida de archivos o documentos, así como restaurar la operación normal de sus sistemas de datos personales.
- III. **Respuesta:** El sujeto obligado deberá contar con hardware y software destinados a atender una alerta de seguridad, y comenzar la mitigación en caso de confirmar un incidente, en función de los activos del Responsable, y de las medidas de seguridad existentes, incluyendo de manera enunciativa y no limitativa lo siguiente: antivirus portátiles, discos duros y/o dispositivos de memoria exclusivos para incidentes, herramientas, cables, software para analizar tráfico de red y listas de revisión y de comandos.
- IV. **Identificación:** Una vez identificado un incidente, es necesario buscar alertas adicionales a la detonante y determinar su alcance total por al menos dos personas involucradas en la detección del incidente, una para evaluar los activos que pudieran ser afectados, y otra para documentar y recabar evidencia.
- V. **Contención:** Una vez identificado el incidente se debe proceder al aislamiento de los sistemas y la puesta en operación de respaldos en el corto plazo para reducir los efectos de un incidente. Posteriormente se debe proseguir con la contención del incidente a largo plazo y se deben identificar las vulnerabilidades explotadas en los activos, así como las medidas de seguridad que pudieron hacer falta, para su posterior implementación.
- VI. **Mitigación:** Para la mitigación del incidente es necesaria la implementación de medidas de seguridad y el tratamiento profundo del incidente para minimizar la posibilidad de que se vuelva a repetir, mediante la recolección de evidencia para el análisis forense digital, con



herramientas especiales de hardware y software propio o subcontratado a fin de obtener más información para revertir sus efectos.

VII. Recuperación: Se deberá dar seguimiento a las medidas implementadas en la mitigación, y garantizar que los activos que fueron afectados se reintegran a los sistemas de datos personales, una vez que se encuentren funcionales o que cuenten con las medidas de seguridad que los soporten.

VIII. Bitácora: Finalmente es necesario completar la documentación respecto al incidente, y comunicar a las partes interesadas el estado de la seguridad de los activos después de lo sucedido mediante un reporte final dentro de los 15 días posteriores y generar un archivo histórico o bitácora que permita a los encargados de la respuesta a incidentes contar con una base de conocimiento, que pueda ser utilizada para entrenar a los usuarios, o a nuevos integrantes del equipo de respuesta a incidentes para la mejora continua.

Plazo para notificar las vulneraciones de seguridad

Artículo 59. De conformidad con lo dispuesto en el artículo 33 de la Ley de Datos el responsable deberá informar, dentro de un plazo máximo de setenta y dos horas, al titular y al Instituto, en cuanto se confirme que ocurrió la vulneración y el responsable haya empezado a tomar las acciones encaminadas a detonar un proceso de mitigación de la afectación. Asimismo, el responsable realizará las acciones necesarias para la revisión exhaustiva de la magnitud de la afectación, a fin de que los titulares afectados tomen en su caso, las medidas correspondientes para la defensa de sus derechos. El Instituto podrá verificar las medidas de mitigación, niveles de seguridad y documento de gestión para recomendar las medidas pertinentes para la protección de los datos del titular.

El plazo a que se refiere el párrafo anterior comenzará a correr el mismo día natural en que el responsable confirme la vulneración de seguridad.

Notificación de las vulneraciones de seguridad al Instituto

Artículo 60. En la notificación al Instituto a que se refiere el artículo anterior, el responsable deberá informar por escrito presentado en el domicilio del Instituto, o bien, a través de cualquier otro medio que se habilite para tal efecto, al menos, lo siguiente:

- I. La hora y la fecha de la identificación de la vulneración;
- II. La hora y fecha del inicio de la investigación sobre la vulneración;
- III. La naturaleza del incidente o vulneración ocurrida;
- IV. La descripción detallada de las circunstancias en torno a la vulneración ocurrida;
- V. Las categorías y número aproximado de titulares afectados;
- VI. Los sistemas de tratamientos y datos personales comprometidos;



VII. Las acciones correctivas realizadas de forma inmediata, y

VIII. Cualquier otra información y documentación que considere conveniente hacer del conocimiento del Instituto.

Notificación de las vulneraciones de seguridad del titular

Artículo 61. En la notificación que realice el responsable al titular, sobre las vulneraciones de seguridad a que se refieren los artículos 31 y 33 para los efectos del diverso 34 de la Ley de Datos y los presentes Lineamientos, deberá informar, al menos, lo siguiente:

- I. La naturaleza del incidente o vulneración ocurrida;
- II. Los datos personales comprometidos;
- III. Los derechos del titular o medidas que este pueda adoptar para proteger sus intereses;
- IV. Las acciones correctivas realizadas de forma inmediata;
- V. Los medios a disposición del titular para que pueda obtener mayor información al respecto;
- VI. La descripción de las circunstancias generales en torno a la vulneración ocurrida, que ayuden al titular a entender el impacto del incidente, y
- VII. Cualquier otra información y documentación que considere conveniente para apoyar a los titulares.

El responsable deberá notificar el informe directamente al titular de la información a través de los medios que establezca para tal fin. Para seleccionar y definir los medios de comunicación, el responsable deberá considerar, según ello resulte aplicable, el perfil de los titulares, la forma en que mantiene contacto o comunicación con estos, que sean gratuitos; de fácil acceso, con la mayor cobertura posible y que estén debidamente habilitados y disponibles en todo momento para el titular.

Acciones del Instituto derivadas de notificaciones de vulneraciones de seguridad

Artículo 62. En términos de lo previsto en los artículos 33 y 34 de la Ley de Datos, una vez que le sea notificada una vulneración de seguridad al Instituto, éste podrá emitir recomendaciones que deberán ser solventadas en el tiempo establecido en el documento notificado al responsable.

Emisión de recomendaciones no vinculantes

Artículo 63. El Instituto podrá publicar directrices, recomendaciones y mejores prácticas en materia de seguridad de los datos personales, de acuerdo con los estándares nacionales e internacionales



actuales en la materia, con la finalidad de proveer los mecanismos y herramientas que orienten y faciliten al responsable el cumplimiento del deber de seguridad previsto en la Ley de Datos y los presentes Lineamientos.

Principio de confidencialidad

Artículo 64. El responsable deberá establecer controles o mecanismos que tengan por objeto que todas aquellas personas que intervengan en cualquier fase del tratamiento de los datos personales guarden confidencialidad respecto de estos, obligación que subsistirá aún después de finalizar sus relaciones con el mismo.

Carga probatoria para el cumplimiento de obligaciones materia de protección de datos personales

Artículo 65. La carga de la prueba para acreditar el cumplimiento de las obligaciones previstas en el presente capítulo, en todo momento, recaerá en el responsable.

Para tal efecto, el Instituto podrá emitir herramientas que orienten el cumplimiento de las obligaciones previstas en el presente capítulo, así como aquellas establecidas en la Ley de Datos y los presentes Lineamientos.

Sistemas de datos personales

Artículo 66. Los sistemas de datos personales se distinguen en:

- I. **Físicos:** Conjunto ordenado de datos de carácter personal que para su tratamiento están contenidos en registros manuales, impresos, sonoros, magnéticos, visuales u holográficos, estructurado conforme a criterios específicos relativos a personas físicas que permitan acceder sin esfuerzos desproporcionados a sus datos personales, y
- II. **Automatizados:** Conjunto ordenado de datos de carácter personal que permita acceder a la información relativa a una persona física utilizando una herramienta tecnológica.

Categorías de datos personales

Artículo 67. Los datos personales contenidos en los sistemas, tomando en cuenta su naturaleza, se clasificarán, de manera enunciativa, más no limitativa, de acuerdo con las siguientes categorías:

- I. **Identificación:** El nombre, domicilio, teléfono particular, teléfono celular, firma, clave del Registro Federal de Contribuyentes (RFC), Clave Única de Registro de Población (CURP), Matrícula del Servicio Militar Nacional, número de pasaporte, lugar y fecha de nacimiento, nacionalidad, edad, fotografía y demás análogos;
- II. **Electrónicos:** Las direcciones electrónicas, tales como, el correo electrónico no oficial, dirección IP (Protocolo de Internet), dirección MAC (dirección Media Access Control o dirección de control de acceso al medio), así como el nombre del usuario, contraseñas, firma



electrónica; o cualquier otra información empleada por la persona, para su identificación en Internet u otra red de comunicaciones electrónicas;

- III. **Laborales:** Documentos de reclutamiento y selección, nombramiento, incidencia, capacitación, actividades extracurriculares, referencias laborales, referencias personales, solicitud de empleo, hoja de servicio y demás análogos;
- IV. **Patrimoniales:** Los correspondientes a bienes muebles e inmuebles, información fiscal, historial crediticio, ingresos y egresos, cuentas bancarias, seguros, fianzas, servicios contratados, referencias personales y demás análogos;
- V. **Datos sobre procedimientos administrativos y/o jurisdiccionales:** La información relativa a una persona que se encuentre 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;
- VI. **Datos académicos:** Trayectoria educativa, calificaciones, títulos, cédula profesional, certificados y reconocimientos y demás análogos;
- VII. **Datos de tránsito y movimientos migratorios:** Información relativa al tránsito de las personas dentro y fuera del país, así como información migratoria;
- VIII. **Datos sobre la salud:** El expediente clínico de cualquier atención médica, referencias o descripción de sintomatologías, detección de enfermedades, incapacidades médicas, discapacidades, intervenciones quirúrgicas, vacunas, consumo de estupefacientes, uso de aparatos oftalmológicos, ortopédicos, auditivos, prótesis, así como el estado físico o mental de la persona;
- IX. **Datos biométricos:** huellas dactilares, ADN, geometría de la mano, características de iris y retina, forma de caminar y demás análogos;
- X. **Datos personales de naturaleza pública:** aquellos que por mandato legal sean accesibles al público.

Los datos contenidos en las categorías señaladas podrán ser clasificados como datos especialmente protegidos cuando estos refieran a la esfera más íntima de su titular o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para el titular, esto de conformidad con lo establecido en el artículo 3, fracción X, de la Ley de Datos.

Creación de sistemas de datos personales



Artículo 68. El responsable determinará la creación de un sistema de datos personales cuando derivado de la normativa aplicable, se cuente con la atribución para llevar a cabo la acción que involucra un tratamiento de datos personales.

Toda creación de sistemas de datos personales sólo podrá efectuarse mediante la publicación de un Aviso en la Gaceta Oficial de la Ciudad de México, en el cual se indique la liga electrónica donde se podrá consultar el acuerdo de creación respectivo, en términos de lo establecido en el artículo 37 fracción I de la Ley de Datos. Debiendo considerar que, dicha publicación preferentemente deberá dictarse previamente al tratamiento de los datos personales por parte del sujeto obligado.

El responsable deberá notificar al Instituto respecto a la creación del sistema de datos personales, dentro de los diez días hábiles siguientes a la publicación del aviso en la Gaceta Oficial de la Ciudad de México, y conforme a lo establecido en el artículo 37 fracción I de la Ley de Datos, así como realizar su debida inscripción en el Registro Electrónico de Sistemas de Datos Personales.

Modificación de los sistemas de datos personales

Artículo 69. El responsable determinará la modificación del sistema de datos personales cuando se presente un cambio que afecte su integración o tratamiento, y derivado del cual se requiera actualizar la información de dicho sistema de datos personales.

Se habla de un cambio que afecta la integración o tratamiento de un sistema de datos personales cuando éste sufre alteraciones en alguno de los criterios establecidos en los artículos 37 fracción II de la Ley de Datos.

Toda modificación sólo podrá efectuarse mediante la publicación de un aviso en la Gaceta Oficial de la Ciudad de México, en el cual se indique la liga electrónica donde se podrá consultar el acuerdo de modificación respectivo, en términos de lo establecido en el artículo 37 fracción I de la Ley de Datos. Dicha publicación deberá dictarse preferentemente previo a que se implemente la modificación del sistema de datos personales por parte del sujeto obligado.

El responsable deberá notificar al Instituto respecto a la modificación del sistema de datos personales, dentro de los diez días hábiles siguientes a la publicación del aviso en la Gaceta Oficial de la Ciudad de México, y conforme a lo establecido en el artículo 37 fracción I de la Ley de Datos, así como realizar la actualización respectiva del sistema en el Registro Electrónico de Sistemas de Datos Personales.

Contenido del acuerdo de creación o modificación de un sistema de datos personales

Artículo 70. El acuerdo de creación o modificación de sistemas de datos personales deberá contener cuando menos, lo siguiente:

- I. La identificación del sistema de datos personales, en la cual deberá indicarse su denominación, la finalidad o finalidades de los sistemas de datos personales; la normativa aplicable; así como los usos y transferencias previstos;



- II. La estructura básica del sistema de datos personales y la descripción de los tipos de datos incluidos y, en su caso, de los datos sensibles, los cuales deberán ser especialmente protegidos, así como las restantes categorías de datos de carácter personal, incluidas en el mismo y el modo de tratamiento utilizado en su organización;
- III. Las instancias responsables del tratamiento del sistema de datos personales: titular del sujeto obligado, usuarios y encargados, si los hubiera;
- IV. Las áreas ante las que podrán ejercerse los derechos de acceso, rectificación, cancelación y oposición, para lo cual deberá proporcionarse en todo caso, domicilio oficial y dirección electrónica del área ante la cual podrán presentar las solicitudes respectivas;
- V. El procedimiento a través del cual podrán ejercerse los derechos de acceso, rectificación, cancelación y oposición, y
- VI. El nivel de seguridad y los mecanismos de protección exigibles.

Supresión de los sistemas de datos personales

Artículo 71. La supresión de un sistema de datos personales implica la eliminación o borrado del sistema considerando las medidas previamente establecidas para el soporte documental. En ese sentido, el responsable determinará la supresión del sistema de datos personales cuando éste haya cumplido con su finalidad y/o ciclo de vida, o bien que el sujeto obligado deje de tener a su cargo la atribución para realizar el tratamiento de los datos personales relacionada con la finalidad del sistema; lo anterior siempre y cuando no exista una previsión expresa en una ley que exija su conservación.

Toda supresión de sistemas de datos personales sólo podrá efectuarse mediante la publicación de un aviso en la Gaceta Oficial de la Ciudad de México, en el cual se indique la liga electrónica donde se podrá consultar el acuerdo de supresión respectivo, en términos de lo establecido en el artículo 37 fracción I de la Ley de Datos, considerando que, dicha publicación deberá dictarse con al menos, treinta días hábiles previos a que se lleve a cabo la supresión del sistema por parte del sujeto obligado.

El responsable deberá notificar al Instituto respecto a la supresión del sistema de datos personales, dentro de los diez días hábiles siguientes a la publicación del aviso en la Gaceta Oficial de la Ciudad de México, y conforme a lo establecido en el artículo 37 fracción I de la Ley de Datos, así como realizar el borrado del sistema en el Registro Electrónico de Sistemas de Datos Personales una vez cumplidos los treinta días hábiles.

Contenido del acuerdo de supresión sistemas de datos personales



Artículo 72. En caso de que el titular del sujeto obligado o el responsable del sistema de datos personales determine la supresión del mismo deberá elaborar el acuerdo respectivo, considerando el ciclo vital, la finalidad, y el destino de los datos protegidos por el sistema.

El acuerdo de supresión deberá contener cuando menos, lo siguiente:

- I. La identificación del sistema de datos personales del que se trate, debiendo indicar su denominación;
- II. Las disposiciones que se dicten para la supresión de los sistemas de datos personales;
- III. El motivo por el cual derivó la supresión del sistema de datos personales, y
- IV. El destino que tendrán los datos personales protegidos por el sistema de datos personales, o en su caso, las previsiones adoptadas para su destrucción.

Registro de los sistemas de datos personales

Artículo 73. Los responsables de los sistemas de datos personales de los sujetos obligados deberán realizar la inscripción, modificación o en su caso el borrado del sistema del que se trate, en el Registro Electrónico de Sistemas de Datos Personales habilitado por el Instituto.

Para llevar a cabo la inscripción o modificación del sistema, en el Registro Electrónico de Sistemas de Datos Personales, se deberán realizar dichas acciones en un plazo no mayor a los diez días hábiles siguientes a la publicación del aviso de creación o modificación en la Gaceta Oficial de la Ciudad de México.

Por lo que respecta al borrado del sistema en el Registro Electrónico de Sistemas de Datos Personales, esta deberá efectuarse una vez cumplidos los treinta días hábiles señalados en el artículo 71 de los presentes Lineamientos.

Contenido del Registro

Artículo 74. El registro de cada sistema contendrá los siguientes campos:

- I. Nombre del Sistema y, en su caso, fecha de publicación en la Gaceta Oficial de la Ciudad de México;
- II. Nombre y cargo del titular del sujeto obligado como responsable del tratamiento y los usuarios;
- III. Finalidad o finalidades del tratamiento, incluyendo la normativa aplicable;
- IV. Naturaleza de los datos personales contenidos en cada sistema;
- V. Formas de recabación, pertinencia, proporcionalidad y calidad de los datos;



derechos ARCO de este, para el conocimiento de derechos sucesorios, en consideración de la relación de parentesco por consanguinidad o afinidad que haya tenido con el titular, el cual se acreditará en términos de las disposiciones legales aplicables.

Pueden alegar interés jurídico, de manera enunciativa mas no limitativa, el albacea, los herederos, los legatarios y los familiares en línea recta sin limitación de grado y en línea colateral hasta el cuarto grado, lo que se acreditara con copia simple del documento delegatorio, pasado ante la fe de notario público o suscrito ante dos testigos.

En el supuesto de que el titular sea un menor de edad, el interés jurídico se acreditará con la copia del acta de defunción del menor, el acta de nacimiento o identificación del menor, así como la identificación de quien ejercía la patria potestad y/o tutela.

En el supuesto de que el titular sea una persona en estado de interdicción o incapacidad declarada por ley o por la autoridad judicial, el interés jurídico se acreditará con la copia de su acta de defunción, su identificación oficial vigente y de quien ejercía la tutela, así como el instrumento legal de designación del tutor.

Medios para la acreditación de la identidad del titular

Artículo 78. El titular podrá acreditar su identidad a través de los siguientes medios siempre y cuando se encuentren vigentes:

- I. Identificación oficial;
- II. Instrumentos electrónicos o mecanismos de autenticación permitidos por otras disposiciones legales o reglamentarias que permitan su identificación fehacientemente, o
- III. Aquellos mecanismos establecidos por el responsable de manera previa, siempre y cuando permitan de forma inequívoca la acreditación de la identidad del titular.

Para efectos de los presentes capítulos, la identidad de los menores de edad se podrá acreditar mediante su acta de nacimiento, clave única de registro de población, credenciales expedidas por instituciones educativas o instituciones de seguridad social, pasaporte, o cualquier otro documento oficial expedidas para tal fin.

La identidad de personas en estado de interdicción o incapacidad declarada por ley o por autoridad judicial, se podrá acreditar mediante su acta de nacimiento, clave única de registro de población, pasaporte o cualquier otro documento o identificación oficial vigente expedida para tal fin.

Medios para la acreditación de la identidad y personalidad del representante



Artículo 79. Cuando el titular ejerza sus derechos ARCO a través de su representante, este deberá acreditar la identidad del titular y su identidad y personalidad presentando ante el responsable lo siguiente:

- I. Copia simple de la identificación oficial vigente;
- II. Identificación oficial vigente del representante, y
- III. Instrumento público; carta poder simple firmada ante dos testigos, a la que deberá anexarse copia simple de las identificaciones oficiales de quienes intervengan, en la suscripción del mismo, o declaración en comparecencia personal del titular.

Acreditación de menores de edad cuando sus padres ejercen la patria potestad

Artículo 80. Cuando el titular sea un menor de edad y sus padres sean los que ejerzan la patria potestad y los que pretendan ejercer los derechos ARCO de este, además de acreditar la identidad del menor, se deberá acreditar la identidad y representación de los padres mediante los siguientes documentos:

- I. Acta de nacimiento del menor de edad, y
- II. Documento de identificación oficial vigente del padre o de la madre que pretenda ejercer el derecho.

Acreditación de menores de edad cuando una persona distinta a sus padres ejerce la patria potestad

Artículo 81. Cuando el titular sea un menor de edad y su patria potestad la ejerce una persona distinta a los padres y esta sea quien presente la solicitud para el ejercicio de los derechos ARCO, además de acreditar la identidad del menor se deberá acreditar la identidad y representación de la persona mediante los siguientes documentos:

- I. Acta de nacimiento del menor de edad;
- II. Documento legal que acredite la posesión de la patria potestad, y
- III. Documento de identificación oficial vigente de quien ejerce la patria potestad.

Acreditación de menores de edad cuando son representados por un tutor

Artículo 82. Cuando el titular sea un menor de edad y la solicitud para el ejercicio de los derechos ARCO la presente su tutor, además de acreditar la identidad del menor, el tutor deberá acreditar su identidad y representación mediante los siguientes documentos:

- I. Acta de nacimiento del menor de edad;
- II. Documento legal que acredite la tutela, y



III. Documento de identificación oficial vigente del tutor.

Acreditación de personas en estado de interdicción o incapacidad declarada por ley o por autoridad judicial

Artículo 83. Cuando el titular sea una persona en estado de interdicción o incapacidad declarada por Ley o por la autoridad judicial, además de acreditar la identidad de la persona, su representante deberá acreditar su identidad y representación mediante los siguientes documentos:

- I. Instrumento legal de designación del tutor, y
- II. Documento de identificación oficial vigente del tutor.

Acreditación de las personas vinculadas a fallecidos

Artículo 84. En términos del artículo 47 último párrafo de la Ley de Datos y su correlativo en los presentes Lineamientos, la persona que acredite tener un interés jurídico deberá presentar ante el responsable los siguientes documentos:

- I. Acta de defunción del titular;
- II. Documentos que acrediten el interés jurídico de quien pretende ejercer el derecho, y
- III. Documento de identificación oficial vigente de quien solicita el ejercicio de los derechos ARCO.

Solicitud para el ejercicio de los derechos ARCO

Artículo 85. En la solicitud para el ejercicio de los derechos ARCO, el responsable no podrá imponer o solicitar mayores requerimientos informativos a los previstos en el artículo 50 de la Ley de Datos y, en atención al caso concreto, deberá ir acompañada de copia simple de los documentos previstos en los presentes Lineamientos.

Además de lo señalado en el párrafo anterior, el responsable deberá observar lo siguiente:

- I. Cuando se trate de una solicitud para el ejercicio de acceso a datos personales, el titular podrá acompañar a esta, en su caso, el medio magnético, electrónico o el mecanismo a través del cual requiere la reproducción de estos, el cual también podrá entregarse una vez que el titular sea notificado sobre la procedencia del ejercicio del derecho solicitado, de conformidad con lo previsto en el artículo 50, párrafo segundo de la Ley de Datos;
- II. Cuando el titular no pueda cubrir los costos de reproducción y/o envío de sus datos personales en virtud de su situación socioeconómica, deberá manifestar tal circunstancia en su solicitud a efecto de que la Unidad de Transparencia del responsable determine lo conducente conforme a lo previsto en el artículo 48 párrafo cuarto de la Ley de Datos;



- III. Tratándose de solicitudes de rectificación de datos personales, el titular, además de indicar lo señalado en el artículo 50 de la Ley de Datos, podrá aportar la documentación que sustente la modificación solicitada, y
- IV. En las solicitudes para el ejercicio de los derechos ARCO, el titular podrá aportar las pruebas que estime pertinentes para acreditar la procedencia de su solicitud, las cuales deberán acompañarse a la misma desde el momento de su presentación.

En caso de que el titular o, en su caso, su representante acuda personalmente a las instalaciones del responsable a presentar una solicitud para el ejercicio de los derechos ARCO, sus personas servidoras públicas deberán orientarlos sobre la localización de la Unidad de Transparencia.

Asistencia de la Unidad de Transparencia

Artículo 86. La Unidad de Transparencia del responsable deberá auxiliar y orientar al titular en la elaboración de las solicitudes para el ejercicio de sus derechos ARCO, en todo momento, y en especial en aquellos casos en que el titular no sepa leer ni escribir, así como informar sobre la obligación del titular de acreditar su identidad y, en su caso, la identidad y personalidad de su representante.

Para el caso de las personas con discapacidad, la Unidad de Transparencia del responsable garantizará la atención de cada uno de los titulares, de acuerdo con su situación particular, y facilitar en todo momento la información que estos requieren para el ejercicio de sus derechos ARCO.

Orientación a los titulares en materia de protección de datos personales

Artículo 87. Adicionalmente a lo establecido por el artículo 76, fracción I de la Ley de Datos, el responsable por medio de la Unidad de Transparencia deberá contar con medios de comunicación funcionales y eficientes para orientar a los titulares en materia de protección de datos y en su caso atender dudas y quejas, los cuales deberán ser de fácil acceso y con la mayor cobertura posible; considerando el perfil de los titulares y la forma en que se mantiene contacto o comunicación directa o cotidiana con ellos, así como estar, en todo momento, habilitado.

Medidas especiales para personas con capacidades diferentes y hablantes de lengua indígena

Artículo 88. El responsable garantizará que las personas con algún tipo de discapacidad o hablantes de lengua indígena, puedan ejercer, en igualdad de circunstancias, sus derechos ARCO, para lo cual deberá promover acuerdos con instituciones públicas especializadas que pudieran auxiliarle en la recepción y entrega de las respuestas a solicitudes para el ejercicio de los derechos ARCO y las resoluciones a los recursos de revisión que se presenten en lengua indígena, braille o cualquier formato que se requiera en función de las diferentes capacidades del titular, en forma más eficiente.

Sin perjuicio de lo anterior, el responsable podrá adoptar las siguientes medidas:

- I. Contar con equipos de cómputo con tecnología adaptada, escritura braille y lectores de texto;



- II. Reservar lugares de estacionamiento para personas con discapacidad;
- III. Contar con intérpretes oficiales de lenguas indígenas;
- IV. Facilitar la utilización del lenguaje de señas o cualquier otro medio o modo de comunicación;
- V. Brindar las facilidades para el acceso de perros guías o animales de apoyo;
- VI. Apoyar en la lectura de documentos;
- VII. Contar con rampas para personas con discapacidad, o
- VIII. Cualquier otra medida física o tecnológica que ayude a las personas con discapacidad y/o hablantes de lengua indígena a ejercer de manera eficiente sus derechos ARCO.

En ningún caso, las personas referidas en el presente artículo serán objeto de discriminación en el ejercicio de sus derechos.

Acuse de recibido

Artículo 89. El responsable deberá dar trámite a toda solicitud para el ejercicio de los derechos ARCO y entregar el acuse de recibido que corresponda.

El responsable deberá registrar las solicitudes para el ejercicio de los derechos ARCO que se presenten mediante escrito libre en el sistema electrónico habilitado para tal efecto por el Instituto, conforme a la normativa que resulte aplicable.

En caso de que la solicitud para el ejercicio de los derechos ARCO en escrito libre se presente directamente ante una unidad administrativa distinta a la Unidad de Transparencia, la unidad administrativa deberá remitir la solicitud a la Unidad de Transparencia a más tardar al día siguiente de su presentación.

Para tal efecto, la solicitud para el ejercicio de los derechos ARCO se entenderá por recibida en la fecha en que fue presentada en la unidad administrativa del responsable, lo anterior, de conformidad con lo previsto y para los efectos del artículo 49 de la Ley de Datos.

Prevención al titular

Artículo 90. En el caso de que la información proporcionada por el titular en su solicitud para el ejercicio de los derechos ARCO sea insuficiente para atenderla por no satisfacer alguno de los requisitos previstos en el artículo 50 de la Ley de Datos, o bien, no se acompañe copia simple de los documentos a que se refieren los presentes Lineamientos y el Responsable no cuente con elementos para subsanarla, deberá prevenir al titular, por una sola vez y dentro de los cinco días



hábiles contados a partir del día siguiente al que recibió la solicitud, para que aporte los elementos o documentos necesarios para dar trámite a la misma.

El titular contará con un plazo de diez días hábiles para atender la prevención, contados a partir del día siguiente al de la notificación.

La prevención tendrá el efecto de interrumpir el plazo que tiene el responsable para dar respuesta a la solicitud para el ejercicio de los derechos ARCO, por lo que el cómputo de dicho plazo se reanudará al día siguiente del desahogo de la prevención por parte del titular.

Transcurrido el plazo sin que el titular haya desahogado la prevención, se tendrá por no presentada la solicitud para el ejercicio de los derechos ARCO.

Turno de las solicitudes para el ejercicio de los derechos ARCO

Artículo 91. La Unidad de Transparencia del responsable deberá turnar las solicitudes para el ejercicio de los derechos ARCO admitidas, de conformidad con la Ley de Datos y los presentes Lineamientos, a la o las unidades administrativas que conforme a sus atribuciones, facultades, competencias o funciones puedan o deban poseer los datos personales sobre los que versen las solicitudes, en atención a la normativa que les resulte aplicables.

Reproducción y certificación de datos personales

Artículo 92. La información será entregada sin costo, cuando implique la entrega de hasta sesenta hojas simples. La certificación de documentos y su costo, se regirá por lo dispuesto en los artículos 48 de la Ley de Datos y demás legislación al efecto aplicable.

Respuesta del responsable y plazo para emitirla

Artículo 93. En la respuesta a una solicitud para el ejercicio de los derechos ARCO, el responsable deberá señalar:

- I. Los costos de reproducción, certificación y/o envío de los datos personales o de las constancias que acrediten el ejercicio efectivo de los derechos ARCO que, en su caso, correspondan;
- II. El plazo que tiene el titular para realizar el pago correspondiente, el cual no podrá ser menor de tres días hábiles contados a partir del día siguiente de que se notifique la respuesta a que se hace referencia en el presente artículo; además de señalar que una vez que el titular o, en su caso, su representante realice el pago deberá remitir copia del recibo correspondiente, con la identificación del número de folio de la solicitud para el ejercicio de los derechos ARCO que corresponda, a más tardar al día siguiente de realizarse el pago y a través del medio que señaló para oír y recibir notificaciones, o bien, presentar personalmente copia ante la Unidad de Transparencia del responsable, y
- III. El derecho que le asiste al titular para interponer un recurso de revisión ante el Instituto, en caso de inconformidad por la respuesta recibida.



La respuesta adoptada por el responsable podrá ser notificada al titular en su Unidad de Transparencia o en las oficinas que tenga habilitadas para tal efecto, previa acreditación de su identidad y, en su caso, de la identidad y personalidad de su representante de manera presencial por la plataforma nacional o por correo certificado en caso que se hubiere presentado presencialmente en las oficinas del sujeto obligado y exista constancia de la acreditación de la titularidad de los datos, no procederá la notificación a través de representante para estos últimos medios.

Plazo para hacer efectivo los derechos ARCO

Artículo 94. En caso de resultar procedente el ejercicio de los derechos ARCO, el responsable deberá hacerlo efectivo en un plazo no mayor a diez días hábiles contados a partir del día siguiente en que se hubiere notificado la respuesta del titular.

Previo a hacer efectivo el ejercicio de los derechos ARCO, el responsable deberá acreditar la identidad del titular y, en su caso, la identidad y personalidad con la que actúe su representante de conformidad con lo dispuesto el artículo 47 de la Ley de Datos y los presentes Lineamientos, así como verificar la realización del pago de los costos de reproducción, envío o certificación que, en su caso, se hubiere establecido.

La acreditación de la identidad del titular y, en su caso, la identidad y personalidad del representante a que se refiere el párrafo anterior, se deberá llevar a cabo mediante la presentación de los documentos originales que correspondan, siempre y cuando el titular o su representante se presenten en la Unidad de Transparencia del responsable para levantar una constancia de tal situación, la respuesta a su solicitud para el ejercicio de los derechos ARCO podrá ser notificada a través de los medios electrónicos que determine el titular.

Acceso a datos personales

Artículo 95. La obligación de acceso de los datos personales se dará por cumplida cuando el responsable ponga a disposición del titular, previa acreditación de su identidad y, en su caso, la identidad y personalidad de su representante, los datos personales a través de consulta directa, en el sitio donde se encuentren, o mediante la expedición de copias simples, copia certificadas, medios magnéticos, ópticos, sonoros, visuales u holográfico, o cualquier otra tecnología que determine el titular, dentro del plazo de quince días hábiles a que se refiere el artículo 49 de la Ley de Datos y de conformidad con lo dispuesto en dicho ordenamiento y los presentes Lineamientos.

Rectificación de datos personales

Artículo 96. La obligación de rectificar los datos personales se dará por cumplida cuando el responsable notifique al titular, previa acreditación de su identidad y, en su caso, la identidad y personalidad de su representante, una constancia que acredite la rectificación solicitada, dentro del plazo de quince días hábiles a que se refiere el artículo 49 de la Ley de Datos y de conformidad con lo dispuesto en dicho ordenamiento y los presentes Lineamientos.



En la constancia a que se refiere el párrafo anterior del presente artículo, el responsable deberá señalar, al menos, el nombre completo del titular, los datos personales rectificados, así como la fecha a partir de la cual fueron rectificados los datos personales en sus registros, archivos, sistemas de información, expedientes, bases de datos o documentos en su posesión.

Cancelación de datos personales

Artículo 97. La obligación de cancelar los datos personales se dará por cumplida cuando el responsable notifique al titular, previa acreditación de su identidad y, en su caso la identidad y personalidad de su representante, una constancia que señale:

- I. Los documentos, bases de datos personales, archivos, registros, expedientes, y/o sistemas de tratamiento donde se encuentren los datos personales objeto de cancelación;
- II. El periodo de bloqueo de los datos personales, en su caso;
- III. Las medidas de seguridad de carácter administrativo, físico, y técnico implementadas durante el periodo de bloqueo, en su caso, y
- IV. Las políticas, métodos y técnicas utilizadas para la supresión definitiva de los datos personales, de tal manera que la probabilidad de recuperarlos o reutilizarlos sea mínima.

El responsable deberá notificar al titular la constancia a que se refiere el párrafo anterior de los presentes Lineamientos dentro del plazo de quince días hábiles establecido en el artículo 49 de la Ley de Datos y de conformidad con lo dispuesto en dicho ordenamiento y los presentes Lineamientos.

Oposición de datos personales

Artículo 98. La obligación de cesar el tratamiento de los datos personales se dará por cumplida cuando el responsable notifique al titular, previa acreditación de su identidad y, en su caso, la identidad y personalidad de su representante, una constancia que señale dicha situación dentro del plazo de quince días hábiles a que se refiere el artículo 49 de la Ley de Datos y de conformidad con lo dispuesto en dicho ordenamiento y los presentes Lineamientos.

Envío de datos personales o constancias por correo certificado

Artículo 99. Sólo procederá el envío por correo certificado de los datos personales o de las constancias del ejercicio efectivo de los derechos ARCO, cuando la solicitud sea presentada personalmente por el titular ante el responsable, no medie representación alguna del titular, y no se trate de menores de edad o de datos personales de fallecidos.

Envío de datos personales o constancias por medios electrónicos

Artículo 100. Sólo procederá el envío por medios electrónicos de los datos personales o de las constancias que acrediten el ejercicio efectivo de los derechos ARCO, cuando el titular hubiere



acreditado fehacientemente su identidad y, en su caso, la identidad y personalidad de su representante mediante cualquier mecanismo de los términos previstos en la Ley de Datos y los presentes Lineamientos.

La Unidad de Transparencia del responsable deberá dejar constancia de la acreditación del titular y, en su caso, de su representante, a que se refiere el párrafo anterior.

Disponibilidad de los datos personales o constancias que acrediten el ejercicio efectivo de los derechos

Artículo 101. La Unidad de Transparencia del responsable deberá tener a disposición del titular y, en su caso, de su representante los datos personales en el medio de reproducción solicitado y/o las constancias que acrediten el ejercicio efectivo de los derechos ARCO durante un plazo máximo de sesenta días, contados a partir del día siguiente en que se hubiere notificado la respuesta de procedencia al titular.

Transcurrido el plazo a que se refiere el párrafo anterior, el responsable deberá dar por concluida la atención a la solicitud para el ejercicio de los derechos ARCO y proceder a la destrucción del material en el que se reprodujeron los datos personales o de las constancias que acrediten el ejercicio efectivo de los derechos ARCO.

Lo anterior, sin perjuicio del derecho que le asiste al titular de presentar una nueva solicitud de derechos ARCO ante el responsable.

Causales de improcedencia de ejercicio de los derechos ARCO

Artículo 102. Cuando el responsable niegue el ejercicio de los derechos ARCO por actualizarse alguno de los requisitos o supuestos previstos en el artículo 50 de la Ley de Datos, la respuesta deberá constar en una resolución de su Comité de Transparencia que confirme la improcedencia del ejercicio de los derechos ARCO.

Incompetencia notoria y parcial del responsable

Artículo 103. Cuando la Unidad de Transparencia del responsable determine la notoria incompetencia de este para atender la solicitud para el ejercicio de los derechos ARCO, deberá comunicar tal situación al titular dentro del plazo de tres días hábiles a que se refiere el artículo 51, primer párrafo de la Ley de Datos, y en su caso, orientarlo con el responsable competente, sin que sea necesario una resolución del Comité de Transparencia que confirme la notoria incompetencia.

Si el responsable es competente para atender parcialmente la solicitud para el ejercicio de los derechos ARCO deberá dar respuesta en el ámbito de su respectiva competencia, dentro del plazo de quince días hábiles a que se refiere el artículo 49 de la Ley de Datos y de conformidad con dicho ordenamiento y los presentes Lineamientos.

Inexistencia de los datos personales



Artículo 104. La resolución del Comité de Transparencia a que se refiere el artículo 51 segundo párrafo de la Ley de Datos deberá contar con los elementos mínimos que permitan al titular tener la certeza de que se utilizó un criterio de búsqueda exhaustivo; así como señalar las circunstancias de tiempo, modo y lugar que generaron la inexistencia en cuestión y la unidad administrativa competente de contar con los mismos.

Reconducción de la solicitud para el ejercicio de los derechos ARCO

Artículo 105. En términos de lo previsto en el artículo 51 último párrafo de la Ley de Datos, en caso de que el Responsable advierta que la solicitud para el ejercicio de los derechos ARCO corresponde a un derecho diferente de los previstos en la Ley de Datos y los presentes Lineamientos, deberá reconducir la vía haciéndolo del conocimiento al titular dentro de los tres días hábiles siguientes a la presentación de la solicitud, sin menoscabo de los requisitos, y los plazos establecidos en la vía correcta conforme a la normativa que resulte aplicable.

Trámites específicos

Artículo 106. El responsable podrá establecer los plazos y los procedimientos internos que considere convenientes para recibir, gestionar y dar respuesta a las solicitudes para el ejercicio de los derechos ARCO, pero deberá observar en todo momento los requisitos, condiciones, plazos y términos previstos en la Ley de Datos y los presentes Lineamientos.

Negativa para la tramitación de solicitudes para el ejercicio de los derechos ARCO

Artículo 107. Cuando alguna unidad administrativa del responsable se negare a colaborar con la Unidad de Transparencia en la atención de las solicitudes para el ejercicio de los derechos ARCO, esta dará aviso al superior jerárquico para que le ordene realizar sin demora las acciones conducentes.

Inconformidad del titular por la respuesta recibida o falta de esta

Artículo 108. En términos del artículo 53 de la Ley de Datos, el titular y, en su caso, su representante, podrán presentar un recurso de revisión ante el Instituto por la respuesta recibida o falta de respuesta del responsable, de conformidad con lo establecido en la Ley de Datos y los presentes Lineamientos.

Cumplimiento de las obligaciones para el ejercicio de los derechos ARCO

Artículo 109. La carga de la prueba para acreditar el cumplimiento de las obligaciones previstas en el presente capítulo, recaerá, en todo momento, en el responsable.

Objeto de la portabilidad de los datos personales

Artículo 110. La portabilidad de datos personales tiene por objeto que el titular solicite:

Una copia de sus datos personales que hubiere facilitado directamente al responsable, en un formato estructurado y comúnmente utilizado, que le permita seguir utilizándolos y, en su caso,



entregarlos a otro responsable para su reutilización y aprovechamiento en un nuevo tratamiento, sin que lo impida el responsable al que el titular hubiere facilitado los datos personales, y

La transmisión de sus datos personales a un responsable receptor, siempre y cuando sea técnicamente posible, el titular hubiere facilitado directamente sus datos personales al responsable transmisor y el tratamiento de éstos se base en su consentimiento o en la suscripción de un contrato.

Lo anterior, mediante los lineamientos y parámetros para determinar los supuestos en los que se está en presencia de un formato estructurado y comúnmente utilizado, así como las normas técnicas, modalidades y procedimientos para la transferencia de datos personales que emita el Sistema Nacional.

TÍTULO CUARTO RELACIÓN DEL RESPONSABLE Y ENCARGADO

CAPÍTULO ÚNICO DEL ENCARGADO

Obligación general del encargado

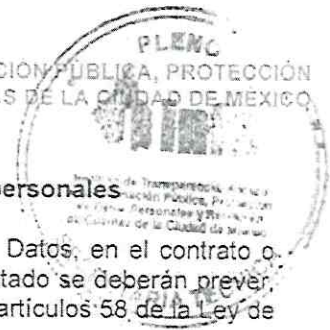
Artículo 111. En términos de lo previsto en los artículos 3, fracción XV y 55 de la Ley de Datos, el encargado es la persona física o jurídica, pública o privada, ajena a la organización del responsable que sola o conjuntamente con otras que tratará datos personales a nombre y por cuenta del responsable, sin modificar las finalidades o decidir sobre el alcance y contenido del tratamiento, sus actuaciones estarán limitadas a los términos fijados por el responsable.

El responsable y el encargado compartirán responsabilidad por las vulneraciones de seguridad ocurridas en el tratamiento de datos personales que efectúe el encargado a nombre y por cuenta del responsable.

Formalización de la prestación de servicios del encargado

Artículo 112. Además de cláusulas generales señaladas en el artículo 56 de la Ley de Datos para la prestación de los servicios del encargado, el responsable deberá prever en el contrato o instrumento jurídico por el que se formalice la prestación de servicios del encargado, las siguientes obligaciones:

- I. Permitir al Instituto o al responsable realizar verificaciones en el lugar o establecimiento donde lleva a cabo el tratamiento de los datos personales;
- II. Colaborar con el Instituto en las investigaciones previas y verificaciones que lleve a cabo en términos de lo dispuesto en la Ley de Datos y los presentes Lineamientos, y proporcionar la información y documentación que se estime necesaria para tal efecto, y
- III. Generar, actualizar y conservar la documentación necesaria que le permita acreditar el cumplimiento de sus obligaciones.



Subcontratación de servicios que impliquen el tratamiento de datos personales

Artículo 113. De acuerdo con lo previsto en el artículo 57 de la Ley de Datos, en el contrato o cualquier instrumento jurídico que suscriba el encargado con el subcontratado se deberán prever, al menos, las cláusulas generales y obligaciones a las que se refieren los artículos 58 de la Ley de Datos y 112 de los presentes Lineamientos.

Proveedores de servicios de cómputo en la nube y otras materias

Artículo 114. Los proveedores de servicios de cómputo en la nube y otras materias a que se refieren los artículos 3, fracción VI, 57 y 58 de la Ley de Datos, para efectos de dicho ordenamiento y los presentes Lineamientos tendrán el carácter de encargados.

En caso de que, en la contratación de servicios de cómputo en la nube y otras materias, el Responsable tenga la posibilidad de convenir con el proveedor las condiciones y los términos de este tipo de servicios que impliquen un tratamiento de los datos personales, en el contrato o instrumento jurídico que suscriban se deberán prever, al menos, las cláusulas generales a que se refiere el artículo 58 de la Ley de Datos y los presentes Lineamientos, lo anterior, no exime al responsable de observar lo previsto en los artículos 57 y 58 de la Ley de Datos y los presentes Lineamientos.

En caso de que el responsable se adhiera a los servicios de cómputo en la nube y otras materias mediante condiciones o cláusulas generales de contratación, deberá cumplir con lo dispuesto en los artículos señalados en el párrafo anterior del presente artículo.

Incumplimiento de las obligaciones del encargado

Artículo 115. En caso de que el encargado y subcontratado incumplan las obligaciones contraídas con el responsable y decidan y determinen, por sí mismos, los fines, medios y demás cuestiones relacionadas con el tratamiento de los datos personales, asumirán el carácter del responsable de conformidad con la normativa que les resulte aplicables en función de su naturaleza pública o privada.

TÍTULO QUINTO TRANSFERENCIAS DE DATOS PERSONALES

CAPÍTULO ÚNICO DE LOS REQUERIMIENTOS PARA LA REALIZACIÓN DE TRANSFERENCIAS NACIONALES Y/O INTERNACIONALES

Condiciones generales de las transferencias de datos personales



Artículo 116. Toda transferencia de datos personales sea nacional o internacional, se encuentra sujeta al consentimiento de su titular, salvo las excepciones previstas en los artículos 16, fracción II y 59 de la Ley de Datos y sin perjuicio de lo dispuesto en el artículo 60 del mismo ordenamiento, la cual deberá ser informada al titular en el aviso de privacidad, con el efecto de limitar el tratamiento de los datos personales transferidos a las finalidades que la justifiquen.

El responsable transferente deberá comunicar al destinatario o receptor de los datos personales el aviso de privacidad, conforme al cual se obligó a tratar los datos personales frente al titular.

Medios para solicitar el consentimiento expreso del titular para la transferencia de sus datos personales

Artículo 117. Cuando la transferencia de datos personales requiera del consentimiento expreso del titular, el responsable podrá establecer cualquier medio que le permita obtener esta modalidad del consentimiento de manera previa a la transferencia de sus datos personales, siempre y cuando el medio habilitado sea de fácil acceso y con la mayor cobertura posible, en consideración del perfil de los titulares y la forma en que mantienen contacto cotidiano común con el titular.

En todos los casos en lo que se traten datos personales sensibles se deberá obtener el consentimiento expreso y por escrito del titular para su tratamiento, salvo en los casos de excepción previstos en el artículo 16 de la Ley de Datos.

Transferencias nacionales de datos personales

Artículo 118. Cuando la transferencia sea nacional, el receptor de los datos personales asumirá el carácter de responsable conforme a la legislación que en esta materia le resulte aplicable a su naturaleza jurídica, pública o privada, y deberá tratar los datos personales con apego a lo dispuesto en dicha legislación y a lo convenido en el aviso de privacidad que le será comunicado por el responsable transferente.

En la suscripción de cláusulas contractuales, convenios de colaboración o cualquier otro instrumento jurídico que se utilice para la formalización de la transferencia, este deberá contener de manera enunciativa más no limitativa, lo siguiente:

1. Los datos del responsable transferente y del responsable receptor (nombre completo de la persona servidora pública, cargo, área de adscripción, domicilio institucional, correo electrónico, teléfono);
2. Objeto del Convenio;
3. Compromisos del responsable y del receptor;
4. Las personas responsables de la operación, seguimiento y administración de la información;
5. Medidas de Seguridad;



6. Vulnerabilidad de la información;
7. Información confidencial y/o acceso restringido a la información;
8. Vigencia;
9. Terminación de la relación;
10. Supresión de la información, y
11. Responsabilidad (aplicable a toda persona que use, sustraiga, divulgue, oculte, altere, mutile, destruya o inutilice, total o parcialmente y de manera indebida los datos personales que se encuentren bajo su custodia o a los cuales tengan acceso o conocimiento con motivo de su empleo, cargo o comisión).

Transferencias internacionales de datos personales

Artículo 119. El responsable sólo podrá transferir datos fuera del territorio nacional, cuando el receptor o destinatario se obligue a proteger los datos personales conforme a los principios, deberes y demás obligaciones similares o equiparables a las previstas en la Ley de Datos y demás normativa aplicable en la materia, así como a los términos previstos en el aviso de privacidad que le será comunicado por el responsable transferente.

Solicitud de opiniones sobre transferencias internacionales de datos personales

Artículo 120. En caso de considerarlo necesario, el responsable podrá solicitar la opinión del Instituto respecto aquellas transferencias internacionales de los datos personales que pretenda efectuar en cumplimiento de lo dispuesto en la Ley de Datos y los presentes Lineamientos de acuerdo con lo siguiente:

- I. El responsable deberá presentar su solicitud directamente en el domicilio del Instituto, o bien, a través de cualquier otro medio que se habilite para tal efecto;
- II. La solicitud deberá describir las generalidades y particularidades de la transferencia internacional de datos personales que se pretende efectuar, con especial énfasis en las finalidades que motivan la transferencia; el o los destinatarios de los datos personales que, en su caso, se pretenda transferir; el fundamento legal que, en su caso, obligue al Responsable a transferir; los datos personales que se pretendan transferir; las categorías de titulares involucrados; la tecnología o medios utilizados para, en su caso, efectuar la transferencia; las medidas de seguridad aplicables; las cláusulas contractuales, convenios de colaboración o cualquier otro instrumento jurídico que se suscriba con el destinatario o receptor, en caso de que resulte exigible, así como cualquier otra información relevante para el caso concreto;
- III. La solicitud deberá ir acompañada de aquellos documentos que el responsable considere conveniente hacer del conocimiento del Instituto;



- IV. Si el Instituto considera que no cuenta con la suficiente información para emitir su opinión técnica, deberá requerir al responsable, por una sola ocasión y en un plazo que no podrá exceder de cinco días hábiles contados a partir del día siguiente de la presentación de la solicitud, la información adicional que considere pertinente;
- V. El responsable contará con un plazo máximo de diez días hábiles, contados a partir del día siguiente de la recepción del requerimiento de información adicional, para proporcionar mayores elementos al Instituto con el apercibimiento de que en caso de no cumplir se tendrá por no presentada su consulta;
- VI. El requerimiento de información adicional tendrá el efecto de interrumpir el plazo que tiene el Instituto para emitir su opinión técnica, por lo que comenzará a computarse a partir del día siguiente de su desahogo;
- VII. El Instituto deberá emitir la opinión técnica que corresponda en un plazo que no podrá exceder de quince días, contados a partir del día siguiente a la recepción de la consulta, el cual no podrá ampliarse, y
- VIII. Si el Instituto no emite su opinión técnica en el plazo señalado en la fracción anterior del presente artículo, se entenderá que su opinión no es favorable respecto a la transferencia internacional de datos personales que se pretenda efectuar.

Cumplimiento de las obligaciones en materia de transferencias de datos personales

Artículo 121. La carga de la prueba para acreditar el cumplimiento de las obligaciones previstas en el presente Capítulo, recaerá, en todo momento, en el responsable.

TÍTULO SEXTO ACCIONES PREVENTIVAS EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES

CAPÍTULO ÚNICO DE LOS ESQUEMAS DE MEJORES PRÁCTICAS, EVALUACIONES DE IMPACTO DE LA PROTECCIÓN DE DATOS PERSONALES Y OFICIAL DE PROTECCIÓN DE DATOS PERSONALES

Parámetros de los esquemas de mejores prácticas



Artículo 122. En los parámetros de esquemas de mejores prácticas a que se refiere el artículo 66 de la Ley de Datos, el Instituto deberá definir, de manera enunciativa mas no limitativa, los alcances, objetivos, características y conformación del sistema de mejores prácticas en materia de protección de datos personales, el cual incluirá el modelo de certificación, así como los requisitos mínimos que deben satisfacer estos esquemas para su evaluación, validación o reconocimiento del Instituto o inscripción en el registro correspondiente.

Evaluaciones de impacto en la protección de datos personales

Artículo 123. En la elaboración, presentación y valoración de las evaluaciones de impacto en la protección de datos personales, así como en la emisión de las recomendaciones no vinculantes, el responsable y el Instituto, según corresponda, deberá observar lo dispuesto en las disposiciones que para tal efecto emita el Sistema Nacional.

Para efectos de los presentes Lineamientos, el responsable estará en presencia de un tratamiento intensivo o relevante de datos personales en la presencia de los factores a que se refiere el artículo 68 de la Ley de Datos.

Designación del oficial de protección de datos personales

Artículo 124. Para aquellos responsables que en el ejercicio de sus funciones sustantivas lleven a cabo tratamientos relevantes o intensivos de datos personales a que se refieren los artículos 67 y, en su caso, 68 de la Ley de Datos, podrán designar a un oficial de protección de datos personales, el cual formará parte de la Unidad de Transparencia.

La persona designada como oficial de protección de datos deberá contar con la jerarquía o posición dentro de la organización del responsable que le permita implementar políticas transversales en esta materia.

El oficial de protección de datos personales deberá ser designado en atención a sus conocimientos, cualidades profesionales, experiencia en la materia, y, en su caso, a la o las certificaciones con que cuente en materia de protección de datos personales.

Funciones del oficial de protección de datos personales

Artículo 125. El oficial de protección de datos personales tendrá las siguientes atribuciones:

- I. Asesorar al Comité de Transparencia respecto a los temas que sean sometidos a su consideración en materia de protección de datos personales;
- II. Proponer al Comité de Transparencia políticas, programas, acciones y demás actividades que correspondan para el cumplimiento de la Ley de Datos y los presentes Lineamientos;
- III. Implementar políticas, programas, acciones y demás actividades que correspondan para el cumplimiento de la Ley de Datos y los presentes Lineamientos, previa autorización del Comité de Transparencia;



- IV. Brindar asesoría permanentemente a las áreas adscritas al responsable en materia de protección de datos personales, y
- V. Las demás que determine el responsable y la normativa que resulte aplicable.

Lo anterior, sin perjuicio de lo señalado en el artículo 76 párrafo segundo de la Ley de Datos.

Los sujetos obligados deberán respaldar al oficial de protección de datos personales en todas sus acciones y decisiones en función de sus atribuciones, siempre y cuando no sean contrarias a la Ley de Datos y sean en función de cumplir con los principios, deberes y obligaciones en materia de datos personales.

Funciones del Enlace

Artículo 126. La persona servidora pública designada como Enlace por el Titular del sujeto obligado tendrá entre sus obligaciones, las siguientes:

- I. Coordinar a los responsables de sistemas de datos personales al interior del sujeto obligado para el cumplimiento de la Ley de Datos, los Lineamientos y demás normativa aplicable;
- II. Supervisar que los responsables mantengan actualizada la inscripción de los sistemas bajo su responsabilidad en el registro electrónico creado por el Instituto;
- III. Coordinar las acciones de capacitación del personal al interior del sujeto obligado en materia de protección de datos personales, y
- IV. Remitir el informe anual a que hace referencia la fracción XI del artículo 23 de la Ley de Datos.
- V. Atender las verificaciones previstas en el artículo 112 de la Ley de Datos, mediante los canales de comunicación que el Instituto determine para ello.

TÍTULO SÉPTIMO MEDIOS DE IMPUGNACIÓN

CAPÍTULO I DE LAS DISPOSICIONES COMUNES A LOS RECURSOS DE REVISIÓN

Principios rectores

Artículo 127. En la sustanciación de los recursos de revisión, el Instituto deberá dar cumplimiento a los requisitos de fundamentación y motivación, así como regirse por los siguientes principios:



- I. **Legalidad:** actuará al margen de lo que estrictamente le está permitido por la Ley de Datos, de tal manera que no realice conductas contrarias a sus atribuciones expresamente conferidas;
- II. **Certeza jurídica:** dará a conocer a las partes, de manera previa, con claridad y seguridad, las reglas, requisitos y procedimientos a que se encuentra sujeta su actuación en la toma de cualquier decisión;
- III. **Independencia:** emitirá decisiones en estricto apego a la normativa que le resulta aplicable, sin tener que acatar a someterse a indicaciones, instrucciones, sugerencias, intereses, presiones o insinuaciones de terceros;
- IV. **Imparcialidad:** se abstendrá de cualquier influencia de terceros y/o de las partes en las decisiones, procesos y procedimientos sometidos a su potestad, o bien, de juicios o valoraciones subjetivas;
- V. **Eficacia:** actuará conforme a una cultura de servicio orientada al logro de sus resultados, mediante el uso responsable y claro de los recursos públicos y la obtención del mayor resultado con el esfuerzo realizado;
- VI. **Objetividad:** realizará sus funciones por las razones señaladas en la legislación que le resulte aplicable y no por valoraciones subjetivas;
- VII. **Profesionalismo:** actuará de manera responsable y seria, de tal manera que el ejercicio de sus funciones se cumpla con eficiencia, y
- VIII. **Transparencia:** su actuación, en el ejercicio de sus funciones públicas, se hará del conocimiento público en atención a la interpretación más amplia y extensiva del derecho a la protección de datos personales.

Acreditación de la identidad y personalidad del representante

Artículo 128. Cuando el titular interponga un recurso de revisión, ante el Instituto, a través de su representante, ambos deberán acreditar su identidad y la personalidad de este último conforme lo dispuesto en los artículos 84 y 85 de la Ley de Datos.

Acreditación de menores de edad cuando sus padres ejercen la patria potestad

Artículo 129. Cuando el titular sea menor de edad y su padre o madre sean los que ejerzan la patria potestad y los que presenten el recurso de revisión, además de acreditar la identidad del menor, se deberá acreditar la identidad del padre o la madre que interpone el recurso mediante los siguientes documentos.

- I. Acta de nacimiento del menor de edad, y



- II. Documento de identificación oficial vigente del padre o de la madre de quien interpone el recurso de revisión.

Para efectos del presente capítulo, la identidad de las y los menores de edad se podrá acreditar mediante su acta de nacimiento, clave única de registro de población, credenciales expedidas por instituciones educativas o instituciones de seguridad social, pasaporte, entre otros documentos utilizados para tal fin.

Acreditación de menores de edad cuando una persona distinta a sus padres ejerce la patria potestad

Artículo 130. Cuando el titular sea menor de edad y su patria potestad la ejerza una persona distinta al padre o la madre y esta es quien presenta el recurso de revisión, deberá acreditar la identidad del menor y su identidad y representación mediante los siguientes documentos:

- I. Acta de nacimiento del menor de edad;
- II. Documento legal que acredite el ejercicio de la patria potestad, y
- III. Documento de identificación oficial vigente de quien ejerce la patria potestad.

Acreditación de menores de edad cuando un tutor ejerce la patria potestad

Artículo 131. Cuando el titular sea menor de edad y el recurso de revisión, lo presente su tutor o tutora, este deberá acreditar la identidad de la o el menor y su identidad y representación mediante los siguientes documentos:

- I. Acta de nacimiento del menor de edad;
- II. Documento legal que acredite el ejercicio de la tutela, y
- III. Documento de identificación oficial de la persona tutora.

Acreditación de personas en estado de interdicción o incapacidad declarada por ley

Artículo 132. Cuando él o la titular sea una persona en estado de interdicción o incapacidad declarada por Ley o por autoridad judicial, su tutor o tutora deberá acreditar la identidad del titular y su identidad y representación mediante los siguientes documentos:

- I. Documento de identificación oficial vigente de la persona en estado de interdicción o incapacidad;
- II. Instrumento legal de designación de la persona tutora, y
- III. Documento de identificación oficial vigente de la persona tutora.



Para efectos del presente capítulo, la identidad de personas en estado de interdicción o incapacidad declarada por ley se podrá acreditar mediante su acta de nacimiento, clave única de registro de población, pasaporte o cualquier otro documento o identificación expedida para tal fin.

Recurso de revisión de personas vinculadas a fallecidos

Artículo 133. En términos del artículo 86 de la Ley de Datos, la interposición de un recurso de revisión de datos personales concernientes a una persona fallecida, podrá realizarla la persona que acredite su identidad en los términos previstos en los artículos 84 y 85 de la Ley de Datos y tener un interés legítimo o jurídico a través del documento respectivo, así como el acta de defunción de la persona fallecida.

Para efectos de la Ley de Datos y los presentes Lineamientos, se entenderá que una persona física tiene interés legítimo cuando, sin tener un derecho subjetivo se ve afectada en su esfera jurídica por su situación subjetiva y particular y por razones de hecho o de derecho. Para lo cual, deberá acreditar la existencia de una norma constitucional en lo que se establezca o tutele algún interés difuso o beneficio de una colectividad determinada; el acto reclamado transgreda ese interés difuso ya sea de manera individual o colectiva, así como la pertenencia a esa colectividad.

Se entenderá por interés legítimo aquel interés personal, individual o colectivo, competente, actual, real y jurídicamente relevante, que puede traducirse en un beneficio a favor del peticionario derivado de una afectación a su esfera jurídica en sentido amplio, que puede ser de índole económica, profesional, de salud, o de cualquier otra.

Para efectos de la Ley de Datos y los presentes Lineamientos, se entenderá por interés jurídico aquel que tiene una persona física que, con motivo del fallecimiento del titular, pretende ejercer los derechos ARCO de este, para el reconocimiento de derechos sucesorios, en consideración a la relación de parentesco por consanguinidad o afinidad que haya tenido con la persona titular, el cual se acreditará en términos de las disposiciones legales aplicables.

Pueden alegarlo, de manera enunciativa más no limitativa, las personas albaceas, herederas, legatarias, familiares en línea recta sin limitación de grado y en línea colateral hasta el cuarto grado, lo que se le acreditará con copia simple del documento delegatorio pasado ante la fe del notario público o suscrito ante dos testigos.

En el supuesto de que la persona titular sea menor de edad, el interés jurídico se acreditará con la copia del acta de defunción, así como la identificación del menor y de quien ejercía la patria potestad y/o tutela.

En el supuesto de que la persona titular sea alguien en estado de interdicción o incapacidad declarada por la Ley, el interés jurídico se acreditará con la copia del acta de defunción, la identificación de la persona fallecida y de quien ejercía la tutela, así como el instrumento legal de designación del tutor.

La persona que demuestre tener un interés jurídico o legítimo, el heredero o el albacea de la persona fallecida, deberá acreditar su identidad y representación mediante lo siguiente:



- I. Documento donde acredite tener un interés legítimo o jurídico;
- II. Acta de defunción de la persona fallecida, y
- III. Documento de identificación oficial vigente de la persona recurrente.

Medios de presentación del recurso de revisión

Artículo 134. De acuerdo con lo dispuesto en el artículo 82 de la Ley de Datos, el Instituto deberá recibir los recursos de revisión a través de cualquiera de los siguientes medios:

- I. Por escrito libre o en el formato aprobado por este presentado en su domicilio;
- II. Por medio de la Unidad de Transparencia del responsable cuya respuesta es objetivo del recurso de revisión.
- III. Por correo electrónico o la plataforma nacional, o bien, a través de cualquier otro sistema electrónico que para tal efecto se autorice;
- IV. Por correo certificado con acuse de recibo, o
- V. Cualquier otro medio que determine.

Se presumirá que la persona titular acepta que las notificaciones le sean efectuadas por el mismo conducto que presentó su escrito, salvo que acredite haber señalado uno distinto para recibir notificaciones.

El Instituto deberá prever mecanismos accesibles para que las personas con discapacidad, así como hablantes de una lengua indígena puedan interponer recursos de revisión de manera enunciativa más no limitativa, contar con lugares de estacionamiento para personas con discapacidad; la asistencia de intérpretes oficiales de lengua indígena; las facilidades para el acceso de perros guía o animales de apoyo, o el apoyo en la lectura de documentos.

Tipos de pruebas y reglas para su ofrecimiento

Artículo 135. En la sustanciación del recurso de revisión, la persona titular, el responsable y/o el tercero interesado podrán ofrecer las pruebas señaladas en el artículo 98 de la Ley de Datos.

En el caso de ofrecer la prueba pericial, se deberá señalar el nombre completo, y especialidad en la ciencia o arte del perito, así como exhibir el interrogatorio que deberá desahogar este, o bien, los puntos sobre los que versará el peritaje.

Los peritos propuestos deberán acreditar que cuentan con título profesional, arte o industria, siempre y cuando la profesión o el arte estuvieren legalmente reglamentados. En caso contrario o cuando la profesión o arte de que se trate, pese a estar reglamentada, no contara con peritos en el lugar, se podrá nombrar a cualquier persona entendida sin que sea necesario que cuente con un título.