

PROTECCIÓN DE DATOS PERSONALES

Herramientas para conocer y
proteger tu información

Versión extendida



Instituto Estatal de Transparencia,
Acceso a la Información y Protección de Datos Personales

PROTECCIÓN DE DATOS PERSONALES

Herramientas para conocer y
proteger tu información

Versión extendida

Instituto Estatal de Transparencia,
Acceso a la Información y
Protección de Datos Personales

PLENO

Brenda Lizeth González Lara

Consejera Presidenta

Félix Fernando Ramírez Bustillos

Consejero Vocal

María Teresa Treviño Fernández

Encargada de Despacho

COORDINACIÓN DE EDICIÓN Y PUBLICACIÓN

Francisco Reynaldo Guajardo Martínez

Director Editorial

Coordinación Editorial

Secretaría de Acceso a la Información

Dirección de Datos Personales

Primera edición: septiembre 2026

Instituto Estatal de Transparencia,

Acceso a la Información y

Protección de Datos Personales (INFONL)

Av. Constitución 1465-1 Centro

Monterrey, Nuevo León

México C.P. 64000

ISBN: 978-968-9780-07-6

Edición y diseño: Ediciones de Laurel S.A. de C.V.

Impreso y hecho en México

Instituto Estatal de Transparencia, Acceso a la Información y Protección de Datos Personales (INFONL). Se autoriza la reproducción total o parcial del contenido de la presente obra, mencionando la fuente.

➤ ÍNDICE

MENSAJE INSTITUCIONAL	5
PRESENTACIÓN	7
OBJETIVO	8
¿A QUIÉN ESTÁ DIRIGIDA?	9
CÓMO USAR ESTE MATERIAL	10
BLOQUE I. EL DIAGNÓSTICO. ¿POR QUÉ DEBERÍA IMPORTARME?	11
Capítulo 1. Tus datos personales, el valor que no sabías que tenían	11
1.1 ¿Qué son los datos personales?	12
1.2 ¿Por qué son importantes?	17
1.3 Ejemplos cotidianos	22
1.4 Privacidad, protección de datos personales y acceso a la información	27
1.5 El derecho a la protección de datos personales en México	31
1.6 ¿Qué leyes protegen tus datos personales?	34
Capítulo 2. Un universo de datos	39
2.1 Datos personales de identificación	40
2.2 Datos personales patrimoniales, financieros, laborales y académicos	43
2.3 Datos personales sensibles	46
2.4 Datos que obran en registros de seguridad, procuración y administración de justicia	50
2.5 Ejemplos ilustrativos	55
Capítulo 3. ¿Quién tiene tus datos y por qué los quiere?	60
3.1 El sector público	60
3.2 El sector privado	66
3.3 Diferencias entre el régimen público y el privado	71
3.4 ¿Cuándo pueden compartir tus datos con terceros?	75
3.5 ¿Qué autoridad puede ayudarte?	79
Capítulo 4. Protege tus datos en el mundo digital	83
4.1 Situaciones que pueden comprometer la protección de tus datos personales	83
4.2 Riesgos al utilizar redes sociales e internet	87
4.3 Buenas prácticas para proteger tu información personal	91
4.4 Casos ilustrativos para aprender	95
BLOQUE II. GUÍA DE SUPERVIVENCIA: CASOS PRÁCTICOS	99
Capítulo 5. Tus datos personales en la vida cotidiana	99
5.1 Tus datos personales al realizar trámites y servicios públicos	99
5.2 La protección de tus datos en escuelas y servicios de salud	104
5.3 Tus datos personales en instituciones financieras	109
5.4 Lo que compartes al utilizar aplicaciones móviles	114

5.5	¿Cómo identificar cuándo te solicitan más datos de los necesarios?	118
5.6	¿Cuándo es necesario entregar una copia de tu identificación oficial?	122
5.7	Cámaras de seguridad, fotografías y videgrabaciones	127
Capítulo 6.	Protección de datos para grupos de atención prioritaria	133
6.1	¿Cómo cuidar la información de niñas, niños y adolescentes?	133
6.2	Proteger los datos personales de las personas adultas mayores	141
6.3	¿Qué pasa con los datos personales de las personas en situación de vulnerabilidad?	148
Capítulo 7.	Tecnologías emergentes y protección de datos personales	155
7.1	¿Cómo utiliza la inteligencia artificial tus datos personales?	155
7.2	¿Qué es el perfilamiento y por qué influye en lo que ves en internet?	159
7.3	Cómo proteger tus datos frente a amenazas digitales	163
7.4	Neurodatos, cuando la tecnología puede conocer lo que piensas	166
BLOQUE III.	TU PODER DE DEFENSA	172
Capítulo 8.	Tus derechos sobre tus datos personales	172
8.1	¿Qué son los derechos ARCOP?	173
8.2	Derecho de Acceso	174
8.3	Derecho de Rectificación	176
8.4	Derecho de Cancelación	178
8.5	Derecho de Oposición	181
8.6	Derecho de Portabilidad	184
8.7	¿Cuándo pueden limitarse estos derechos?	187
Capítulo 9.	¿Cómo ejercer tus derechos paso a paso?	190
9.1	Paso 1. Identifica quién tiene tus datos	191
9.2	Paso 2. Presenta tu solicitud	193
9.3	Paso 3. Espera la respuesta	198
9.4	Plazos que debes conocer	202
Capítulo 10.	¿Qué hacer si tus derechos no son respetados?	205
10.1	Cuando una institución pública no responde	206
10.2	Cuando no estás de acuerdo con la respuesta	209
10.3	¿Qué puede hacer el INFONL?	212
10.4	¿Cómo puede ayudarte el INFONL?	213
Capítulo 11.	Herramientas para protegerte	217
11.1	Formato oficial para ejercer tus derechos ARCOP	217
11.2	Formato para presentar una denuncia	218
11.3	Directorio de autoridades competentes	219
11.4	Sitios oficiales	221
11.5	Micrositios del INFONL	223
11.6	Lista de verificación antes de compartir tus datos	224
REFERENCIAS		227

► MENSAJE INSTITUCIONAL

Vivimos en una época en la que cada interacción digital deja información sobre quiénes somos, qué hacemos y cómo vivimos. Los datos personales tienen un enorme valor, porque forman parte de nuestra identidad y de nuestra vida privada, permiten tomar decisiones sobre nosotros e incluso pueden afectar el ejercicio de nuestros derechos. Por ello, también pueden ser utilizados de manera indebida si no conocemos las medidas para protegerlos.

Proteger los datos personales significa proteger a las personas. Significa proteger su dignidad, su privacidad, su autonomía y su libertad. Por ello, el derecho a la protección de los datos personales no debe entenderse únicamente como una cuestión de seguridad o como el cumplimiento de determinadas obligaciones legales, sino como una garantía fundamental para que cada persona pueda decidir sobre su información y mantener el control sobre aspectos de su vida privada.

En el Instituto Estatal de Transparencia, Acceso a la Información y Protección de Datos Personales de Nuevo León (INFONL) asumimos que proteger los datos personales de la ciudadanía no es un trámite burocrático, sino una responsabilidad constitucional para garantizar un derecho humano fundamental. Por eso, desde hace años impulsamos una cultura de prevención que va más allá de la norma escrita. Hemos llevado esta conversación a espacios públicos como la Feria Internacional del Libro de Monterrey, donde presentamos *Datos Personales en Riesgo. El costo de compartir en línea*, una obra que puso sobre la mesa los riesgos reales que enfrentamos como sociedad. Hemos construido, además, herramientas digitales accesibles, como nuestro micrositio de protección de datos y la guía para ejercer los derechos ARCOP.

En el INFONL trabajamos para que el derecho a la protección de los datos personales sea una realidad tanto para la ciudadanía como para las instituciones públicas. Promovemos una cultura de prevención mediante actividades de difusión y educación; brindamos asesoría técnica a las autoridades para que sus programas, servicios y plataformas incorporen medidas que protejan la información personal desde su diseño; evaluamos periódicamente el cumplimiento



de las obligaciones de los sujetos obligados; y, cuando una persona considera que sus datos personales fueron tratados indebidamente, o existen elementos que hagan presumir una vulneración a este derecho, conocemos e investigamos los procedimientos previstos por la ley para contribuir a su tutela efectiva.

Esta obra es un paso más en ese camino. La escribimos para ti y para quien quiere entender de manera sencilla qué son los datos personales, por qué tienen valor y cómo puedes protegerlos en tu vida cotidiana; para las familias que desean acompañar a sus hijas e hijos en el uso responsable de la tecnología; para quienes utilizan servicios digitales, realizan trámites o compran por internet y quieren tomar decisiones mejor informadas; y para todas las personas que consideran importante que sus datos personales sean tratados con responsabilidad, transparencia y respeto.

El conocimiento es la primera línea de defensa. Esperamos que estas páginas te den las herramientas para ejercerla.

Brenda Lizeth González Lara

Consejera Presidenta

Instituto Estatal de Transparencia, Acceso a la
Información y Protección de Datos Personales

PRESENTACIÓN

Con esta obra buscamos ofrecer una guía clara y directa sobre el valor de la información personal en el mundo actual. Su objetivo es brindar respuestas sencillas sobre qué son los datos personales, cómo se relacionan con nuestra identidad y qué acciones concretas podemos tomar para navegar, tramitar y compartir contenidos en el entorno digital de forma segura.

El contenido de esta obra se desarrolla con base en los principios y derechos reconocidos por la Declaración Universal de los Derechos Humanos, el Pacto Internacional de Derechos Civiles y Políticos, la Convención Americana sobre Derechos Humanos, así como por la Constitución Política de los Estados Unidos Mexicanos, la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, la Ley Federal de Protección de Datos Personales en Posesión de los Particulares y la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Nuevo León, entre otros instrumentos jurídicos que fortalecen la tutela del derecho a la privacidad y a la protección de los datos personales. Sin embargo, más que presentar un compendio de disposiciones legales, esta obra busca traducir ese marco jurídico en conocimiento claro, cercano y útil, para que cualquier persona pueda comprender sus derechos, ejercerlos de manera informada y proteger su información en un entorno cada vez más digital.

El INFONL, en el ejercicio de sus atribuciones legales de promover una cultura de protección de datos en Nuevo León, pone en tus manos esta herramienta como parte de su estrategia de educación ciudadana continua. No es un manual jurídico ni un texto académico, es una obra editorial práctica, escrita en lenguaje cotidiano, que parte de situaciones reales que cualquier persona puede reconocer en su propia vida llenar un formulario en el médico, instalar una aplicación, recibir una llamada sospechosa o compartir una fotografía en redes sociales para explicar qué puedes hacer para proteger tu información.

La protección de datos personales no es un tema reservado a abogados ni a expertos en tecnología. Es un asunto de todas las personas, y todos los días. Esta obra asume eso desde la primera página.

➤ OBJETIVO

Esta obra tiene un propósito central, que cualquier persona que la lea pueda comprender qué son los datos personales y el derecho que tiene a su protección, así como reconocer cuándo están en riesgo y saber qué herramientas tiene a su alcance para proteger sus datos personales y ejercer los derechos que la ley le reconoce.

Para lograrlo, esta obra se propone:

- Explicar, de manera clara y sencilla, los principales derechos, obligaciones y reglas que protegen los datos personales en México, tanto en el ámbito público como en el privado.
- Identificar los riesgos más comunes a los que se expone la información personal en la vida digital y en los trámites cotidianos.
- Orientar sobre el ejercicio de los derechos de Acceso, Rectificación, Cancelación, y Oposición ante instituciones públicas y privadas, y cuando corresponda, del derecho de Portabilidad (ARCOP), considerando las particularidades de su ejercicio ante las autoridades competentes y los particulares.
- Ofrecer rutas claras de acción cuando los derechos de una persona pueden haber sido vulnerados.
- Prestar especial atención a las necesidades de niños, niñas y adolescentes, personas adultas mayores, personas con discapacidad y otros grupos que puedan enfrentar mayores riesgos o barreras para la protección de sus datos personales y el ejercicio de sus derechos.

Al concluir su lectura, se espera que las personas puedan reconocer el valor de sus datos personales, adoptar medidas para protegerlos, identificar posibles riesgos, ejercer de manera informada sus derechos y saber cómo, cuándo y ante quién acudir cuando consideren que su derecho a la protección de sus datos personales no ha sido respetado.

➤ ¿A QUIÉN ESTÁ DIRIGIDA?

Esta obra está dirigida a todas las personas interesadas en conocer y proteger sus datos personales, particularmente a quienes viven, trabajan o realizan trámites en el estado de Nuevo León, sin importar su nivel de estudios, su edad, ni su relación con la tecnología. Ha sido elaborada con un lenguaje claro y accesible para quienes no cuentan con formación jurídica o técnica, pero enfrentan cotidianamente situaciones en el sector público o en el sector privado en las que se solicitan, utilizan, almacenan o comparten sus datos personales.

En particular, resultará especialmente útil para:

- Personas que desean conocer el valor de su información personal, conocer sus derechos y contar con herramientas prácticas para proteger sus datos personales y ejercer los derechos que les reconoce la legislación.
- Madres, padres, personas tutoras y quienes ejercen labores de cuidado, preocupados por la privacidad digital de niñas, niños y adolescentes.
- Personas adultas mayores, quienes pueden enfrentar mayores riesgos de fraude, suplantación de identidad o engaños relacionados con el uso de sus datos personales.
- Personas que realizan trámites ante instituciones públicas y desean saber por qué se les solicita determinados datos, con qué finalidad, cuáles son necesarios, qué pueden hacer cuando consideren que se les pide información excesiva e injustificada y cuáles son sus derechos respecto de ese tratamiento.
- Usuarios de redes sociales y aplicaciones móviles que buscan comprender el alcance de los datos que comparten en línea.
- Personas que realizan trámites ante instituciones privadas, como lo pueden ser las financieras, hospitales, escuelas, en donde se traten datos personales.

Aunque esta obra fue diseñada para la ciudadanía, también puede ser de utilidad para personas servidoras públicas, integrantes de organizaciones de la sociedad civil y cualquier persona interesada en fortalecer sus conocimientos sobre protección de datos personales.



➤ CÓMO USAR ESTE MATERIAL

Esta obra está organizada en tres bloques temáticos que pueden leerse en orden o de manera independiente, según las necesidades e intereses de cada persona.

Bloque I. El diagnóstico. En este bloque se sientan las bases y explica qué son los datos personales, qué tipos existen, quién los usa y cuáles son los riesgos reales a los que se exponen. Es el punto de partida recomendado para quienes se acercan al tema por primera vez.

Bloque II. Guía de supervivencia. Aquí se abordan situaciones concretas de la vida cotidiana como trámites, hospitales, instituciones financieras, aplicaciones y redes sociales. También dedica un capítulo a los grupos en situación de vulnerabilidad y a los nuevos retos que plantean la inteligencia artificial y los algoritmos. Quien busque respuestas a una situación específica puede ir directamente al capítulo que le corresponda.

Bloque III. Tu poder de defensa. Se explica paso a paso cómo ejercer los derechos ARCOP y a qué instituciones acudir cuando algo sale mal. Es la sección de acción, práctica, directa y orientada a resultados.

A lo largo del texto encontrarás ejemplos, casos ilustrativos y cuadros de información destacada que facilitarán la comprensión de cada tema. Al final de varios capítulos se incluyen referencias al micrositio de protección de datos del INFONL y a la guía para ejercer los derechos ARCOP, donde podrás ampliar la información o iniciar un trámite en línea cuando sean autoridades del Estado de Nuevo León.

BLOQUE I.

EL DIAGNÓSTICO. ¿POR QUÉ DEBERÍA IMPORTARME?

Capítulo 1. Tus datos personales, el valor que no sabías que tenían

Introducción

En la actualidad, gran parte de las actividades que realizamos requieren proporcionar información sobre nuestra persona. Inscribirse en una escuela, acudir a una consulta médica, abrir una cuenta bancaria, solicitar un servicio público, realizar compras por internet o utilizar una aplicación móvil son acciones cotidianas que implican compartir datos personales.

Este intercambio de información permite que instituciones públicas, empresas y organizaciones puedan prestar servicios, cumplir obligaciones legales y atender diversas necesidades de la población. Sin embargo, también implica la responsabilidad de proteger esa información y utilizarla de manera adecuada.

Durante las últimas décadas, el desarrollo tecnológico ha transformado de manera significativa la forma en que la información puede ser recopilada, almacenada, organizada y utilizada. Estas nuevas capacidades han generado importantes beneficios y oportunidades para la sociedad; sin embargo, también han incrementado los riesgos relacionados con el tratamiento de la información personal y han planteado nuevos desafíos para la protección de la privacidad y los derechos de las personas (García, 2007).

Conocer qué son los datos personales constituye el primer paso para comprender por qué tienen un valor tan importante y cuáles son los mecanismos que existen para protegerlos. Este capítulo ofrece una explicación clara y accesible sobre los conceptos fundamentales en materia de protección de datos personales, su importancia en la vida cotidiana y el marco jurídico que reconoce este derecho en México.

1.1 ¿Qué son los datos personales?



Los datos personales forman parte de nuestra vida cotidiana. Están presentes en los documentos que nos identifican, en los servicios que utilizamos, en las relaciones que establecemos con instituciones públicas y privadas e, incluso, en muchas de las actividades que realizamos mediante dispositivos electrónicos.

Aunque el término *datos personales* se utiliza con frecuencia, no siempre existe claridad sobre su verdadero significado o sobre el alcance de la información que comprende. En ocasiones se piensa que únicamente hacen referencia al nombre, al domicilio o al número telefónico de una persona; sin embargo, el concepto es mucho más amplio.

De manera general, los datos personales son toda aquella información relacionada con una persona física que permite identificarla o hacerla identificable, ya sea de forma directa o indirecta.

La Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados define los datos personales como "cualquier información concerniente a una persona física identificada o identificable" (LGPDPPSO, 2025, art. 3. fracc. XXI). Esta definición también es retomada por la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP, 2025), lo que permite contar con un concepto uniforme para los sectores público y privado en México. Por su parte, a nivel local esta definición también se establece en el artículo 3, fracción X de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Nuevo León (LPDPPSONL, 2019).

Una persona es *identificada* cuando es posible conocer su identidad de manera inmediata mediante un dato, como su nombre completo acompañado de una fotografía o una credencial oficial. Una persona es *identificable*, en cambio, cuando su identidad puede determinarse a partir de la combinación de diversos datos, aunque cada uno por separado no revele quién es, el conjunto de esa información puede permitir reconocerla.

Por ejemplo, conocer la edad, la profesión, la ciudad donde reside y el lugar donde trabaja una persona puede ser suficiente para identificarla dentro de un grupo reducido.

Esta característica cobra especial relevancia en la actualidad, ya que el uso de tecnologías digitales permite relacionar información proveniente de diferentes fuentes y construir perfiles cada vez más precisos sobre las personas (Mendoza Enríquez, 2021).

Los datos personales están presentes en distintos aspectos de nuestra vida

Cada persona posee características que la distinguen de las demás. Algunas son evidentes, como el nombre o la fotografía; otras forman parte de su vida académica, laboral, patrimonial o de la relación que mantiene con instituciones públicas y privadas.

La siguiente tabla muestra algunos ejemplos de los datos personales que utilizamos con mayor frecuencia.

Tabla 1.1 Ejemplos de datos personales.

Categoría	Ejemplos
Datos de identificación	Nombre, domicilio, teléfono particular, teléfono celular, correo electrónico, estado civil, firma, firma electrónica, RFC, CURP, cartilla militar, lugar de nacimiento, fecha de nacimiento, nacionalidad, edad, nombres de familiares dependientes y beneficiarios, fotografía, costumbres, idioma o lengua, entre otros.
Datos laborales	Documentos de reclutamiento y selección, de nombramiento, de incidencia, de capacitación, puesto, domicilio de trabajo, correo electrónico institucional, teléfono institucional, actividades extracurriculares, referencias laborales, referencias personales, entre otros.
Datos patrimoniales	Bienes muebles e inmuebles, información fiscal, historial crediticio, ingresos y egresos, cuentas bancarias, seguros, afores, fianzas, servicios contratados, referencias personales, entre otros.

Categoría	Ejemplos
Datos de contacto	Domicilio, número telefónico, correo electrónico.
Datos biométricos	Huellas dactilares, imagen facial, voz, iris o retina.
Datos administrativos	Número de seguridad social, número de empleado, matrícula escolar, folios de identificación.
Datos sobre procedimientos administrativos seguidos en forma de juicio y/o jurisdiccionales	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 o administrativa.
Datos académicos	Trayectoria educativa, títulos, cédula profesional, certificados y reconocimientos, entre otros.
Tránsito y movimientos migratorios	Información relativa al tránsito de las personas dentro y fuera del país e información migratoria de las personas, entre otros.
Datos ideológicos	Creencia religiosa, ideología, afiliación política y/o sindical, pertenencia a organizaciones de la sociedad civil y/o asociaciones religiosas, entre otros.
Datos de salud	Estado de salud, historial clínico, alergias, enfermedades, información relacionada con cuestiones de carácter psicológico y/o psiquiátrico, incapacidades médicas, intervenciones quirúrgicas, vacunas, consumo de sustancias tóxicas, uso de aparatos oftalmológicos, ortopédicos, auditivos, prótesis, entre otros.
Características personales	Tipo de sangre, ADN, huella digital, u otros análogos.
Características físicas	Color de piel, color de iris, color de cabello, señas particulares, estatura, peso, complexión, discapacidades, entre otros.
Vida sexual	Preferencia sexual, hábitos sexuales, entre otros.
Origen	Étnico y racial.

No obstante, los datos personales no se limitan a la información contenida en este cuadro. También forman parte de esta categoría los expedientes clínicos, los antecedentes académicos, la información laboral, los datos financieros, las imágenes captadas por sistemas de videovigilancia y, en determinados casos, los registros que se generan al utilizar dispositivos electrónicos o servicios digitales.

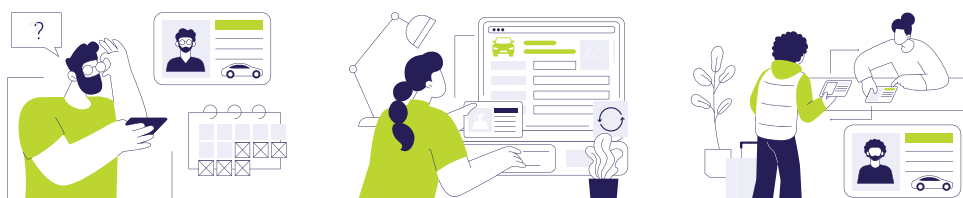
En consecuencia, prácticamente todas las personas generan o proporcionan datos personales en distintos momentos de su vida, ya sea al realizar actividades cotidianas o al acceder a servicios públicos o privados.

Los datos personales

La transformación digital ha ampliado considerablemente la cantidad de información que puede identificar a una persona. Tradicionalmente gran parte de los datos personales se encontraban en documentos impresos o expedientes físicos. Actualmente, una parte importante de esa información se genera y almacena de forma electrónica (Sánchez, 2023).

Cuando una persona utiliza un teléfono inteligente, realiza una búsqueda en internet, solicita un servicio mediante una aplicación o efectúa una compra en línea, generan registros sobre su actividad. En determinados contextos, información como la dirección IP, la ubicación geográfica aproximada, los identificadores de dispositivos electrónicos o el historial de navegación puede constituir un dato personal cuando permite identificar o hacer identificable a una persona (Calcaneo, 2019).

En el contexto digital, esta idea cobra especial relevancia porque una misma persona puede ser identificada a partir de información que, al combinarse, permite reconocerla (IBM, 2025).

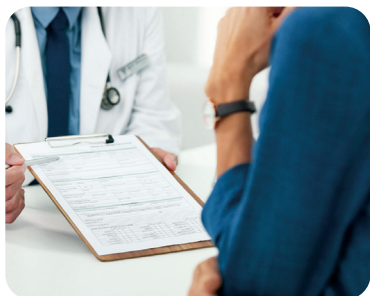


Tus datos personales están protegidos por derechos y obligaciones

Ahora bien, el tratamiento de datos personales implica una relación de derechos y obligaciones.

Por una parte, las personas tienen derecho a conocer quién posee su información, con qué finalidad fue recabada, cómo será utilizada y qué mecanismos existen para ejercer control sobre ella. Por otra parte, las instituciones públicas, y los particulares que traten datos personales tienen la obligación de hacerlo conforme a los principios y deberes previstos en la legislación mexicana vigente en protección de datos personales y demás que resulten aplicables.

Por ello, los datos personales no deben recopilarse, utilizarse o divulgarse de manera arbitraria, su tratamiento debe responder a una finalidad legítima y conforme a los principios y deberes aplicables, además de contar con medidas de seguridad necesarias para su protección.



Ejemplo

Cuando una persona acude a una institución de salud para recibir atención médica, puede proporcionar su nombre, edad, domicilio, datos de contacto y antecedentes médicos para integrar un expediente clínico. Esta información permite brindar una atención adecuada, dar seguimiento

a tratamientos y cumplir diversas obligaciones legales. Sin embargo, la institución tiene la obligación de utilizar y proteger esos datos conforme a las finalidades para las que fueron recabados y a las disposiciones aplicables.

Por ejemplo, si una persona entrega documentación que contiene datos personales para solicitar un apoyo o realizar un trámite, esa información no debe ser divulgada o utilizada para fines distintos a los que justificaron su obtención. Si considera que sus datos fueron tratados de manera indebida o que su derecho a la protección de datos personales ha sido vulnerado, es importante que reconozca los mecanismos y autoridades a los que puede acudir para ejercer sus derechos.



Estos ejemplos muestran que los datos personales son necesarios para la prestación de numerosos servicios y actividades. Por ello, su protección no pretende impedir su utilización, sino asegurar que su tratamiento de la información se realice con respeto a los derechos de las personas.

Concepto clave. Un dato personal no es únicamente aquel que identifica directamente. También puede serlo la información que, por sí sola o combinada con otros datos, permite identificarte o hacerte identificable.

Conclusión. Los datos personales forman parte de nuestra vida cotidiana y pueden revelar información sobre quiénes somos, qué hacemos y distintos aspectos de nuestra vida. Por esta razón, conocer qué información puede considerarse un dato personal es el primer paso para comprender su valor, identificar posibles riesgos y ejercer el derecho a su protección.

1.2 ¿Por qué son importantes?

Los datos personales forman parte de nuestra vida cotidiana y pueden ser necesarios para realizar distintos trámites, recibir servicios o relacionarnos con instituciones públicas y privadas.

En Nuevo León, la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Nuevo León reconoce el derecho de toda persona a la protección de sus datos personales y establece las bases, principios y procedimientos para garantizarlo.

Esto no significa que las instituciones no puedan utilizar datos personales. Significa que, cuando los traten, deben hacerlo conforme a la ley, respetando los principios aplicables y dentro de las facultades que les correspondan.

Además, el tratamiento debe estar relacionado con finalidades concretas, lícitas, explícitas y legítimas, y la institución únicamente debe tratar los datos que sean adecuados, relevantes y estrictamente necesarios para cumplir con esas finalidades.

En pocas palabras, tus datos pueden ser necesarios, pero no pueden utilizarse de cualquier manera. La ley establece reglas para que su tratamiento tenga una finalidad y se realice de manera responsable (LPDPPSONL, 2019, art. 1, 2, 16, 17, 18 y 29).





Los datos personales forman parte de nuestra identidad

Cada persona posee características e información que permiten identificarla o distinguirla de otras. Datos como el nombre, la fotografía, la firma, la voz o las huellas dactilares pueden contribuir a identificar a una persona y, en determinados contextos, a verificar su identidad.

Sin embargo, nuestra identidad no se refleja únicamente en los datos que permiten identificarnos directamente. También existen datos que revelan información sobre distintos aspectos de nuestra vida, como la trayectoria académica, actividad laboral, patrimonial, salud y relaciones familiares.

En conjunto, estos datos reflejan quiénes somos y permiten desarrollar nuestra vida personal, social y profesional. Por ello, su protección constituye una forma de salvaguardar la dignidad y la autonomía de cada individuo. El derecho a la protección de datos personales busca que las personas puedan conocer y ejercer control sobre la información que les concierne, dentro de los límites establecidos por la legislación.

Los datos personales hacen posible el ejercicio de otros derechos

En muchas ocasiones, proporcionar datos personales es indispensable para acceder a derechos y servicios. Por ejemplo, para recibir atención médica es necesario que una institución de salud conozca la identidad del paciente y cuente con información suficiente para brindarle un tratamiento adecuado. De manera similar, una institución educativa requiere determinados datos para inscribir al alumnado, emitir certificados o acreditar estudios.

Asimismo, los datos personales permiten ejercer derechos y acceder a servicios como:

- El acceso a los servicios de salud
- La educación
- La seguridad social
- La identidad jurídica
- La participación en programas públicos
- El ejercicio de los derechos político-electorales
- El acceso a servicios financieros

En estos casos, el tratamiento de los datos personales responde a una finalidad legítima y necesaria para garantizar el adecuado funcionamiento de las instituciones y la prestación de servicios.



Tabla 1.2 Los datos personales y su relación con algunos derechos y servicios.

Derecho o servicio	Ejemplos de datos personales que suelen solicitarse
Salud	Nombre, edad, historial médico, datos de contacto, entre otros.
Educación	Nombre, CURP, domicilio, historial académico, entre otros.
Seguridad social	CURP, número de seguridad social, datos laborales, entre otros.
Programas públicos	Identificación, comprobante de domicilio, información socioeconómica, según corresponda, entre otros.
Servicios financieros	Identificación oficial, RFC, domicilio, información patrimonial, datos biométricos, entre otros.

Fuente: Elaboración propia con base en LPDPPSONL (2019), LGPDPPSO (2025) y LFPDPPP (2025).

El uso indebido de los datos personales puede afectar a las personas

Así como los datos personales son necesarios para acceder a múltiples servicios y realizar diversas actividades, su tratamiento indebido puede afectar a las personas. Cuando la información personal se obtiene, utiliza, modifica, divulga o comparte de manera indebida, pueden presentarse afectaciones que repercutan en distintos ámbitos de la vida de las personas.

Entre las situaciones más frecuentes se encuentran las siguientes:

Tabla 1.3 Posibles afectaciones por el uso indebido de datos personales.

Posible afectación	¿En qué consiste?
Suplantación de identidad	Utilización de datos personales para hacerse pasar por otra persona y realizar actos en su nombre.
Fraudes	Uso de información personal para engañar a una persona y obtener un beneficio económico o patrimonial.
Discriminación	Uso indebido de información relacionada con la salud, discapacidad, origen étnico u otras condiciones para limitar derechos u oportunidades.
Pérdida de privacidad	Divulgación o acceso no autorizado a información personal.
Afectación a la reputación	Difusión de información personal que puede perjudicar la imagen o el prestigio de una persona.

Fuente: Elaboración propia con información de la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (CONDUSEF), Cuida tus datos personales.



No todas estas situaciones tienen la misma gravedad ni ocurren con la misma frecuencia. Sin embargo, muestran la importancia de que los datos personales sean tratados con responsabilidad y conforme al marco jurídico aplicable.

La protección de los datos personales fortalece la confianza

La protección de los datos personales beneficia tanto a las personas como a las instituciones y a las empresas. Cuando una organización informa con claridad para qué recaba datos personales, limita su uso a las finalidades previstas y adopta medidas para proteger la información, genera confianza en quienes utilizan sus servicios.

Esa confianza favorece una relación más transparente entre la ciudadanía y quienes tratan datos personales, además de contribuir al cumplimiento de las obligaciones legales y al fortalecimiento de una cultura de respeto por los derechos humanos.

En este sentido, la protección de los datos personales no debe entenderse como un obstáculo para el desarrollo de actividades públicas o privadas, sino como un elemento que promueve la legalidad, la transparencia y la responsabilidad en el tratamiento de la información.

Concepto clave. Los datos personales son importantes porque permiten identificar a las personas, hacer posible el ejercicio de derechos y acceder a numerosos servicios. Su protección garantiza que esa información sea utilizada de manera responsable, respetando la dignidad, la privacidad y los derechos de sus titulares.

Conclusión. Los datos personales acompañan a las personas durante toda su vida y están presentes en una gran variedad de actividades cotidianas. Gracias a ellos es posible acceder a servicios esenciales, acreditar la identidad, ejercer derechos y mantener relaciones con instituciones públicas, empresas y organizaciones. Su importancia radica no solo en el valor de la información que contienen, sino también en las consecuencias que puede tener su tratamiento, cuando los datos personales son utilizados conforme a la ley, contribuyen al funcionamiento eficiente de la sociedad y fortalecen la confianza entre las personas y las instituciones; en cambio, cuando son tratados de manera indebida, pueden



afectar derechos fundamentales y generar diversas consecuencias para sus titulares. Comprender el valor de los datos personales es el primer paso para adoptar una actitud responsable respecto de la información que compartimos y para ejercer, de manera informada, el derecho a su protección.

1.3 Ejemplos cotidianos

Hasta este momento hemos visto que los datos personales forman parte de nuestra identidad y que su tratamiento es indispensable para acceder a numerosos derechos y servicios. Sin embargo, en muchas ocasiones las personas no son conscientes de la cantidad de información que comparten a lo largo del día ni de las diversas situaciones en las que sus datos personales son utilizados.

En la práctica, proporcionar datos personales es una actividad habitual. Ocurre al realizar trámites ante autoridades, utilizar servicios financieros, acudir a una consulta médica, inscribirse en una institución educativa o simplemente al navegar por internet. En la mayoría de los casos, compartir esta información es necesario para recibir un servicio o ejercer un derecho; no obstante, también implica la responsabilidad de quienes la recaban de protegerla y utilizarla conforme a la legislación mexicana vigente en protección de datos personales y demás que resulten aplicables.

A continuación, se presentan algunos ejemplos de situaciones cotidianas en las que los datos personales desempeñan un papel fundamental.

En los servicios de salud

Cuando una persona acude a un hospital, clínica o consultorio médico, generalmente proporciona información como su nombre, edad, domicilio, datos de contacto, antecedentes médicos, alergias y tratamientos previos. Estos datos permiten integrar un expediente clínico, identificar correctamente al paciente y brindar una atención médica adecuada.

En algunos casos también pueden recabarse datos personales sensibles, como información genética, resultados de estudios clínicos o antecedentes familiares relacionados con la salud, los cuales requieren un nivel reforzado de protección debido a la naturaleza de la información que contienen.



En las instituciones educativas

Desde el proceso de inscripción hasta la emisión de un certificado de estudios, las instituciones educativas requieren tratar diversos datos personales de las y los estudiantes. Es común que soliciten información de identificación, domicilio, CURP, datos de contacto de madres, padres o personas tutoras, historial académico e incluso información médica relevante para atender situaciones de emergencia.



El tratamiento de estos datos permite administrar la vida escolar, emitir documentos oficiales y garantizar la seguridad de la comunidad educativa.

En el ámbito laboral

Durante un proceso de contratación o a lo largo de una relación de trabajo, las personas proporcionan información necesaria para cumplir obligaciones legales y administrativas. Entre los datos que habitualmente se solicitan se encuentran la identificación oficial, la CURP, el Registro Federal de Contribuyentes (RFC), el número de seguridad social, el domicilio, los datos bancarios para el pago del salario y la documentación que acredita la preparación académica o la experiencia profesional.



Estos datos permiten formalizar la relación laboral y cumplir con las obligaciones previstas en la legislación correspondiente.

En los trámites y servicios públicos

Las instituciones públicas requieren datos personales para identificar a las personas, integrar expedientes, emitir documentos oficiales y prestar servicios a la ciudadanía. Por ejemplo, al solicitar una licencia de conducir, registrar un nacimiento, tramitar un apoyo social o presentar una solicitud ante una autoridad, es habitual proporcionar documentos que acrediten la identidad y el domicilio de la persona interesada.

El tratamiento de esta información debe realizarse conforme a los principios, deberes y obligaciones previstos en la legislación mexicana vigente en protección de datos personales y demás que resulten aplicables.

En el comercio electrónico

Cada vez es más común que las personas realicen trámites, soliciten servicios o efectúen pagos a través de plataformas digitales de las instituciones públicas. Para ello, puede ser necesario proporcionar información como el nombre, domicilio, correo electrónico, número telefónico, CURP u otros datos necesarios para identificar a la persona, integrar una solicitud o dar seguimiento al trámite.

Por ejemplo, una persona puede utilizar una plataforma digital de una dependencia estatal para solicitar un documento, realizar el pago de un derecho o presentar una solicitud relacionada con algún servicio público. Durante el proceso, podría proporcionar datos personales y adjuntar documentos que contienen información necesaria para atender su solicitud. Estos datos deben ser utilizados únicamente para las finalidades relacionadas con el trámite o servicio y recibir la protección que corresponda conforme a legislación mexicana vigente en protección de datos personales y demás que resulten aplicables.

El uso de herramientas digitales facilita el acceso a los servicios públicos; sin embargo, también implica la responsabilidad de las instituciones de proteger la información personal que recaban y tratarla de manera adecuada.

En el uso de aplicaciones y servicios digitales



Muchas aplicaciones móviles y plataformas digitales requieren ciertos datos personales para funcionar correctamente. Dependiendo del servicio que ofrecen, pueden solicitar acceso a la ubicación del dispositivo, la cámara, el micrófono, los contactos o el almacenamiento de archivos.

En algunos casos, estos permisos son indispensables para prestar el servicio; en otros, pueden ser opcionales. Por ello, resulta recomendable revisar periódicamente los permisos otorgados a las aplicaciones y verificar que correspondan con las funciones que realmente ofrecen.

En las redes sociales

Las redes sociales permiten compartir información, fotografías, videos y opiniones con otras personas. Sin embargo, también implican el tratamiento de una gran cantidad de datos personales. Además del contenido que las personas deciden publicar, estas plataformas pueden gestionar información relacionada con el perfil de usuario, la interacción con otras cuentas, las preferencias de contenido y otros datos derivados del uso del servicio, de conformidad con sus condiciones de uso y avisos de privacidad.

Por esta razón, es recomendable revisar la configuración de privacidad de cada cuenta y reflexionar sobre la información que se comparte de manera pública.

En los servicios financieros

Al realizar un trámite o solicitar un servicio ante una institución pública, las personas pueden proporcionar diversos datos personales, como su nombre, domicilio, teléfono, CURP, documentos de identificación o información relacionada con su situación particular. Estos datos pueden ser necesarios para integrar expedientes, dar seguimiento a solicitudes, acreditar requisitos o brindar el servicio correspondiente.

Debido a la naturaleza de esta información que las instituciones públicas recaban en el ejercicio de sus atribuciones, deben adoptar las medidas necesarias para proteger los datos personales y evitar su acceso, uso, divulgación o tratamiento indebido. Asimismo, las personas tienen derecho a conocer y ejercer control sobre la información que proporcionan.

Por ello, cuando una persona considere que una institución pública ha tratado sus datos personales de manera contraria a las disposiciones aplicables, puede ejercer los derechos y utilizar los mecanismos de protección previstos en la legislación mexicana vigente en protección de datos personales y demás que resulten aplicables.

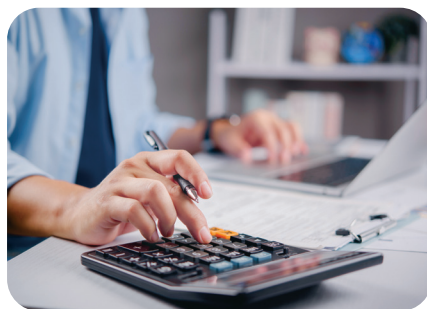


Tabla 1.4 Ejemplos cotidianos del tratamiento de datos personales.

Ámbito de la vida cotidiana	Ejemplos de datos personales que suelen tratarse	Finalidad principal
Servicios de salud	Nombre, expediente clínico, antecedentes médicos, alergias	Brindar atención médica y dar seguimiento a tratamientos.
Educación	Nombre, CURP, domicilio, historial académico	Administrar los servicios educativos y emitir documentos oficiales.
Ámbito laboral	CURP, RFC, número de seguridad social, datos bancarios	Formalizar la relación laboral y cumplir obligaciones legales.
Trámites gubernamentales	Identificación oficial, comprobante de domicilio, firma	Acreditar la identidad y resolver procedimientos administrativos.
Comercio electrónico	Nombre, domicilio, correo electrónico, datos de pago	Procesar compras y entregar bienes o servicios.
Aplicaciones y servicios digitales	Ubicación, correo electrónico, identificadores del dispositivo, permisos del equipo	Proporcionar y personalizar los servicios digitales.
Redes sociales	Nombre de usuario, fotografías, videos, publicaciones e interacciones	Facilitar la comunicación y el uso de la plataforma.
Servicios financieros	Identificación oficial, RFC, domicilio, datos patrimoniales	Verificar la identidad y prestar servicios financieros.

Fuente: Elaboración propia con base en prácticas comunes de tratamiento de datos personales en los sectores público y privado. LPDPPSONL (2019), LGPDPPSO (2025) y LFPDPPP (2025).

Reflexión final. Los ejemplos anteriores muestran que los datos personales acompañan a las personas en prácticamente todas las etapas de su vida. Compartir información no es, por sí mismo, un riesgo; por el contrario, constituye una condición necesaria para ejercer numerosos derechos, y acceder a diversos bienes y servicios. Lo verdaderamente

importante es que el tratamiento de estos datos se realice con respeto a la ley, bajo los Principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad (LPDPPSONL, 2019, art. 16). Así como los deberes de Seguridad y Confidencialidad, y que las personas conozcan los mecanismos disponibles para ejercer control sobre su información. Esta realidad explica por qué la protección de los datos personales se ha consolidado como un derecho humano indispensable en las sociedades contemporáneas.

1.4 Privacidad, protección de datos personales y acceso a la información

Conocer sus diferencias permite comprender mejor los derechos que tienen las personas sobre su información y las obligaciones que deben de cumplir las autoridades y los particulares cuando llevan a cabo tratamiento de datos personales.

En México, estos tres derechos encuentran sustento en la Constitución Política de los Estados Unidos Mexicanos, en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Nuevo León, la Ley Federal de Protección de Datos Personales en Posesión de los Particulares y la Ley de Transparencia y Acceso a la Información Pública del Estado de Nuevo León que regulan el tratamiento de los datos personales y el acceso a la información. Su finalidad es proteger a las personas, fortalecer la transparencia y generar confianza en la actuación de las instituciones.

A continuación, se presentan las principales características de cada uno de estos conceptos.



Privacidad

¿Qué es? La privacidad es el derecho humano a mantener un ámbito de su vida libre de intromisiones indebidas. Comprende aquellos aspectos personales, familiares y sociales que cada individuo decide reservar o compartir únicamente con quienes considere conveniente.

¿Qué protege? Protege ámbitos como las comunicaciones privadas, las relaciones familiares y otros espacios personales en los que las personas pueden desenvolverse sin interferencias injustificadas.



¿Por qué es importante? Porque permite que cada persona conserve un espacio de autonomía para tomar decisiones sobre su vida personal, expresar sus ideas, mantener relaciones de confianza y desarrollar libremente su personalidad.

Ejemplo. Una conversación privada entre familiares, el contenido de un diario personal o las comunicaciones entre una persona y su médico forman parte del ámbito de la privacidad.

Protección de datos personales (PDP)

¿Qué es? Es el derecho que tiene toda persona a decidir sobre el tratamiento de la información que la identifica o la hace identificable. Puede entenderse como una serie de mecanismos o restricciones que se aplican para garantizar el derecho humano autónomo estrechamente relacionado con la autodeterminación informativa y la privacidad. La protección de datos personales permite conocer quién posee los datos personales, para qué se utilizan, cómo se protegen y cuáles son los mecanismos para ejercer control sobre ellos (Constitución Política de los Estados Unidos Mexicanos [CPEUM], 2026, art. 16; Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, 2025).

¿Qué protege? Protege toda información relacionada con una persona física identificada o identificable, como su nombre, domicilio, fotografía, CURP, expediente clínico, datos biométricos o información financiera, entre muchos otros.

¿Por qué es importante? Porque garantiza que los datos personales sean tratados conforme a los principios de licitud, lealtad, consentimiento, información, proporcionalidad, responsabilidad, finalidad y calidad. Así como los deberes de Seguridad y Confidencialidad, evitando usos indebidos o no autorizados.

Ejemplo. Cuando una institución educativa solicita información para inscribir a un estudiante, únicamente pueden utilizar los datos solicitados para las finalidades informadas y debe implementar medidas para protegerlos, adicional a que solo pueden tratar los datos que su marco normativo le permita de acuerdo con sus atribuciones y funciones legales.



Distinción clave entre la privacidad y la Protección de Datos Personales. Mientras la privacidad es el derecho en sí, la protección de datos personales establece los límites concretos sobre lo que otras personas, instituciones públicas o autoridades pueden hacer con nuestra información, las obligaciones para respetarlos y protegerlos. Dicho de otro modo, no se trata de impedir que nuestros datos sean utilizados, sino de establecer reglas para que se utilicen de manera adecuada y respetando nuestros derechos.

Acceso a la información

¿Qué es? Es un derecho humano que comprende solicitar, investigar, difundir, buscar y recibir información. Toda la información generada, obtenida, adquirida, transformada o en posesión de los sujetos obligados es pública y accesible a cualquier persona en los términos y condiciones que se establezcan en la presente Ley, en los tratados internacionales de los que el Estado mexicano sea parte y la Ley General; salvo la información confidencial y la clasificada temporalmente como reservada, por razones de interés público en los términos dispuestos por esta Ley (Ley de Transparencia y Acceso a la Información Pública del Estado de Nuevo León [LTAIPNL], 2016, art. 4).





¿Qué protege? Garantiza el acceso a la información pública relacionada con la actuación gubernamental, el ejercicio de recursos públicos y la toma de decisiones por parte de las autoridades.

¿Por qué es importante? Porque fortalece la transparencia, favorece la rendición de cuentas y permite que la ciudadanía conozca cómo actúan las instituciones públicas.

Ejemplo. Cualquier persona puede solicitar información sobre trámites, servicios, programas o los resultados de un programa gubernamental, siempre que la información sea pública.

¿Cómo se relacionan estos derechos?

Aunque la privacidad, la protección de datos personales y el acceso a la información tienen objetivos distintos, no son derechos que compitan entre sí; por el contrario, se complementan para fortalecer el Estado de derecho y garantizar el respeto a los derechos humanos.

La privacidad protege la esfera personal de cada individuo; la protección de datos personales regula el tratamiento de la información que identifica a las personas; y el acceso a la información permite conocer cómo actúan las instituciones públicas.

En ocasiones, estos derechos coinciden en una misma situación. Por ejemplo, una persona puede solicitar información sobre el gasto público destinado a un hospital, ya que se trata de información de interés público. Sin embargo, esa solicitud no autoriza la entrega de los expedientes clínicos de las y los pacientes, pues contienen datos personales o información sensible cuya protección está expresamente prevista en la ley.

Este equilibrio permite que la sociedad conozca la actuación de las autoridades sin poner en riesgo la privacidad ni los datos personales de las personas.

Concepto clave. La privacidad, la protección de datos personales y el acceso a la información son derechos fundamentales distintos, pero complementarios. Mientras la privacidad protege la vida personal, la protección de datos personales regula el tratamiento de la información que identifica a las personas y el acceso a la información garantiza la transparencia de la actuación pública.

Conclusión. En una sociedad democrática, estos tres derechos cumplen una función esencial. La privacidad protege la esfera personal de cada individuo; la protección de datos personales garantiza que la información relacionada con las personas sea tratada de manera responsable y conforme a la ley; y el acceso a la información fortalece la transparencia, la rendición de cuentas y la participación ciudadana. Comprender sus diferencias ayuda a ejercerlos de manera informada y a reconocer que la transparencia y la protección de los datos personales no son objetivos opuestos, ambos derechos deben coexistir en equilibrio para fortalecer la confianza entre la ciudadanía y las instituciones.

1.5 El derecho a la protección de datos personales en México

La protección de los datos personales es un derecho humano reconocido por la Constitución Política de los Estados Unidos Mexicanos (CPEUM). Esto significa que toda persona tiene la facultad de conocer qué información se recopila sobre ella, para qué se utiliza, quién la posee y cómo puede ejercer control sobre su tratamiento.

Este derecho adquiere especial importancia en una sociedad donde los datos personales forman parte de casi todas las actividades cotidianas. Al realizar un trámite gubernamental, acudir a una consulta médica, abrir una cuenta bancaria, inscribirse en una escuela o utilizar una aplicación digital, las personas proporcionan información que permite identificarlas. Por ello, la ley establece reglas para que esa información sea tratada con responsabilidad, seguridad y respeto a la dignidad humana.

La protección de los datos personales no pretende impedir que las instituciones públicas o las privadas utilicen información cuando exista una finalidad legítima; su objetivo es garantizar que ese tratamiento se realice conforme a la ley, de manera transparente y respetando los derechos de las personas.



Un derecho reconocido por la Constitución

En México, el fundamento principal de este derecho se encuentra en el artículo 16 de la CPEUM, el cual reconoce expresamente que toda persona tiene derecho a la protección de sus datos personales. El segundo párrafo de dicho artículo establece que “toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley” (CPEUM, art. 16, segundo párrafo).

Este reconocimiento constitucional significa que la protección de los datos personales no depende de la voluntad de una institución o de una empresa, sino que constituye un derecho que debe ser respetado por quienes tratan información personal, conforme a las disposiciones legales aplicables.

¿Qué significa este derecho en la vida cotidiana?

El derecho a la protección de los datos personales tiene un impacto directo en la vida de todas las personas. Gracias a este derecho, la ciudadanía puede conocer qué información poseen las instituciones públicas y privadas sobre ellos, así como verificar que dicha información sea utilizada únicamente para los fines que justificaron su obtención.

En términos prácticos, el derecho a la protección de datos personales permite que las personas conozcan y ejerzan control sobre el tratamiento de su información, en los términos previstos por la ley. Entre otras posibilidades, pueden:

- Conocer quién trata sus datos personales y para qué finalidades.
- Saber qué datos personales se tienen sobre ellos y cómo son tratados.
- Solicitar la corrección o actualización de sus datos cuando sean inexactos o estén incompletos.
- Solicitar la cancelación de sus datos personales cuando resulte procedente conforme a la ley.
- Oponerse a determinados tratamientos de sus datos en los supuestos previstos por la legislación.

Estos derechos serán explicados con mayor detalle en el capítulo 8, dedicado al ejercicio de los derechos ARCOP.



Un derecho que también genera obligaciones

Así como las personas tienen derechos respecto de su información personal, quienes recaban y utilizan esos datos también tienen responsabilidades.

Las instituciones públicas y las privadas, así como cualquier persona que trate datos personales deben hacerlo con apego a la legislación vigente, respetando principios y deberes, así como demás obligaciones que se desprenden de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Nuevo León, así como la Ley Federal de Protección de Datos Personales en Posesión de Particulares, esto dependiendo si es una institución pública ya sea federal o estatal, o bien una institución privada.

Entre otras obligaciones, deben:

- Obtener únicamente los datos personales que sean estrictamente necesarios para cumplir una finalidad legítima.
- Informar de manera clara y sencilla cómo serán utilizados.
- Implementar medidas de seguridad para proteger la información.
- Evitar el acceso, uso o divulgación no autorizados.
- Facilitar el ejercicio de los derechos que reconoce la ley.

Estas obligaciones contribuyen a generar confianza entre la ciudadanía y quienes administran información personal.

¿Qué implica el derecho a la protección de los datos personales?

¿Qué reconoce? Que toda persona tiene derecho a mantener el control sobre la información que la identifica o la hace identificable.

¿Qué permite? Conocer cómo se utilizan los datos personales, solicitar su corrección cuando sean inexactos, pedir su cancelación en los casos previstos por la ley y oponerse a determinados tratamientos.

¿Quiénes deben respetarlo? Las autoridades, las instituciones públicas y privadas, así como, cualquier persona física o moral que trate datos personales conforme a la legislación mexicana vigente en protección de datos personales y demás que resulten aplicables.

¿Cuál es su finalidad? Garantizar que la información personal sea tratada de manera lícita, segura, transparente y respetando la dignidad y los derechos de las personas.

Concepto clave. El derecho a la protección de los datos personales garantiza que cada persona conserve el control sobre la información que la identifica. Este derecho obliga a quienes tratan datos personales a hacerlo de manera responsable, transparente y conforme a la Constitución y las leyes mexicanas.

Conclusión. En México, la protección de los datos personales es un derecho humano que permite a las personas mantener el control sobre su información y exigir que esta sea tratada de manera responsable. Su reconocimiento en la Constitución refleja la importancia que tiene la información personal en la vida cotidiana y la necesidad de protegerla frente a

usos indebidos. Más que limitar el intercambio de información, este derecho busca generar confianza entre la ciudadanía, las instituciones públicas y las empresas, estableciendo reglas claras para el tratamiento de los datos personales y mecanismos que permitan a las personas ejercer un control efectivo sobre ellos.



1.6 ¿Qué leyes protegen tus datos personales?

Hasta ahora hemos visto que la protección de los datos personales es un derecho humano reconocido por la Constitución Política de los Estados Unidos Mexicanos. Sin embargo, para que ese derecho pueda ejercerse de manera efectiva, es necesario contar con leyes que establezcan las reglas que deben seguir quienes recaban, utilizan, almacenan o comparten información personal.

En México existe un marco jurídico que regula el tratamiento de los datos personales tanto en el sector público como en el privado. Estas leyes determinan las obligaciones de las instituciones y de las empresas, así como los derechos que tienen las personas respecto de su información.

Conocerlas no significa convertirse en especialista en derecho; basta con identificar cuál es su propósito y en qué situaciones resultan aplicables.



La Constitución como el origen de la protección jurídica

La Constitución Política de los Estados Unidos Mexicanos constituye la norma fundamental del país y es el punto de partida del derecho a la protección de los datos personales.

El artículo 16 reconoce que toda persona tiene derecho a la protección de sus datos personales y establece que la ley regulará la forma en que este derecho debe ejercerse (CPEUM, 2025, art. 16).

A partir del reconocimiento del derecho a la protección de los datos personales en el artículo 16 de la Constitución Política de los Estados Unidos Mexicanos, se desarrollaron diversas disposiciones y leyes reglamentarias que regulan su tratamiento en distintos ámbitos.

Cuando tus datos están en poder de una autoridad

Cuando una institución pública de Nuevo León tiene tus datos personales, no puede utilizarlos de cualquier manera. Debe protegerlos y utilizarlos de acuerdo con las reglas establecidas en la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Nuevo León.

Esta ley se aplica a las autoridades y organismos públicos del Estado y de los municipios, incluidos los Poderes Ejecutivo, Legislativo y Judicial, los órganos autónomos y otros sujetos obligados que señala la propia ley. Su finalidad es garantizar que todas las personas tengan derecho a la protección de sus datos personales y establecer las reglas para su adecuado manejo.

Por ejemplo, cuando entregas tus datos para realizar un trámite, recibir un servicio, solicitar un apoyo o participar en algún procedimiento, la institución que los recibe debe utilizarlos para fines concretos, legales y relacionados con sus funciones.



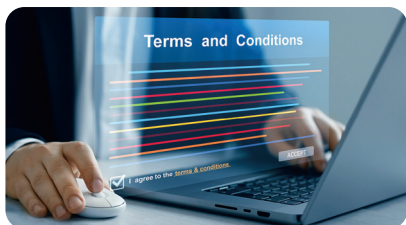
La ley establece, entre otras cosas, que las instituciones públicas deben:

- Informarte para qué utilizarán tus datos personales, mediante un aviso de privacidad.
- Utilizar tus datos para las finalidades que correspondan a sus funciones y atribuciones.

- Solicitar únicamente los datos que sean necesarios para cumplir con la finalidad correspondiente.
- Mantener tus datos correctos y actualizados.
- Proteger tu información mediante medidas de seguridad administrativas, físicas y técnicas.
- Respetar tus derechos de acceso, rectificación, cancelación, oposición y portabilidad (ARCOP) y facilitar los mecanismos para ejercerlos.

En pocas palabras, entregar tus datos a una institución pública no significa que pueda hacer con ellos lo que quiera. La institución tiene la responsabilidad de utilizarlos de manera adecuada, protegerlos y respetar tus derechos.

¿Y cómo puedes saber qué hará una institución con tus datos?



Una de las principales herramientas es el aviso de privacidad, que debe informarte qué datos serán utilizados, para qué se utilizarán, cuál es el fundamento legal para hacerlo y cómo puedes ejercer tus derechos. La ley estatal contempla tanto el aviso de privacidad integral como el simplificado (LPDPPSONL, 2019, art. 1, 2, 16, 17, 18, 24, 29, 30 y 36).

Cuando tus datos están en poder de una Institución Privada

Las empresas, asociaciones, instituciones privadas y cualquier persona física o moral que trate datos personales con fines particulares deben cumplir la LFPDPPP (2025).

Esta ley regula la forma en que los particulares pueden obtener, utilizar, conservar, transferir y, en su caso, eliminar los datos personales. Asimismo, establece obligaciones como elaborar un aviso de privacidad, atender las solicitudes de ejercicio de derechos de las personas y adoptar medidas de seguridad para proteger la información.



En otras palabras, cuando proporcionas tus datos personales a un banco, un hospital privado, una tienda departamental, una universidad particular o una plataforma digital, el tratamiento de esa información debe realizarse conforme a esta ley.

¿Por qué existen tres leyes diferentes?

Una de las preguntas más frecuentes es por qué México cuenta con diferentes leyes en materia de protección de datos personales. La respuesta es sencilla, porque no todas las organizaciones desempeñan las mismas funciones ni el mismo nivel de aplicación.

Las autoridades administran información para cumplir funciones públicas y prestar trámites y servicios a la sociedad, mientras que las instituciones privadas y demás particulares tratan datos personales en el desarrollo de actividades comerciales, profesionales, educativas, financieras o de otra naturaleza privada.

Aunque las leyes tienen diferencias en su ámbito de aplicación, comparten un mismo objetivo, garantizar que los datos personales sean tratados de manera responsable y respetando los derechos de las personas.

¿Qué ley aplica?

Constitución Política de los Estados Unidos Mexicanos

¿Qué establece? Reconoce el derecho humano a la protección de los datos personales.

¿A quién aplica? A todas las personas; sirve de fundamento para el sistema jurídico mexicano.

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

¿Qué regula? El tratamiento de datos personales por parte de autoridades e instituciones públicas.

Ejemplos: secretarías, municipios, organismos constitucionales autónomos, universidades públicas, poderes Legislativo y Judicial, fiscalías y demás sujetos obligados previstos por la ley.



Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Nuevo León

¿Qué regula? Las bases, principios y procedimientos para garantizar el derecho que tiene toda persona a la protección de sus datos personales por parte de autoridades e instituciones públicas estatales y municipales de Nuevo León. Por ejemplo, el poder legislativo estatal, poder judicial estatal, poder ejecutivo estatal, tribunales administrativos, organismos autónomos, instituciones de educación superior públicas autónomas, partidos políticos, ayuntamientos, organismos descentralizados municipales y fideicomisos, todos sujetos obligados previstos por la ley.

Ley Federal de Protección de Datos Personales en Posesión de los Particulares

¿Qué regula? El tratamiento de datos personales realizado por empresas, asociaciones y particulares. *Por ejemplo*, hospitales privados, bancos, escuelas particulares, aseguradoras, comercios, plataformas digitales y prestadores de servicios.

¿Cómo saber qué ley protege mis datos?

En la práctica, identificar la ley aplicable suele ser sencillo. Si los datos personales fueron proporcionados a una institución pública, como un ayuntamiento, una dependencia estatal, una universidad pública o un organismo constitucional autónomo, se aplicará la legislación local y general correspondiente al sector público. Si la información fue entregada a una empresa, un banco, una tienda, una escuela particular, una clínica privada o cualquier otro particular, el tratamiento se registrará por la legislación aplicable al sector privado.

Lo verdaderamente importante es recordar que, independientemente de quién trate los datos personales, las personas conservan sus derechos y pueden exigir que su información sea utilizada conforme a la ley.





Concepto clave. En México, la protección de los datos personales cuenta con un marco jurídico que distingue entre el tratamiento realizado por instituciones públicas y el efectuado por particulares. Aunque las leyes se aplican en ámbitos distintos, todas buscan garantizar el respeto a los derechos de las personas sobre su información personal.

Conclusión. La protección de los datos personales en México no depende únicamente del reconocimiento constitucional de este derecho. También existe un conjunto de leyes que establecen las reglas para el tratamiento de la información personal, las obligaciones de quienes la administran y los derechos que pueden ejercer las personas. Conocer este marco jurídico permite comprender que la protección de los datos personales no es una recomendación o una práctica voluntaria, sino una obligación legal que debe cumplirse tanto en el sector público como en el privado. Este conocimiento será la base para comprender, en los siguientes capítulos, cómo se clasifican los datos personales, quiénes los tratan y cuáles son los mecanismos para protegerlos.

Capítulo 2. Un universo de datos

Introducción

En el capítulo anterior conocimos qué son los datos personales, por qué tienen valor y cuál es el derecho que protege a las personas respecto de su información. Sin embargo, no todos los datos personales revelan el mismo tipo de información ni su tratamiento implica necesariamente los mismos riesgos. Todos están sujetos al régimen de protección que resulte aplicable; no obstante, determinados datos, por su naturaleza o por los riesgos que puede implicar su tratamiento, pueden requerir medidas, requisitos o salvaguardas adicionales.

Algunos datos permiten identificar o distinguir a una persona, como su nombre o su fotografía. Otros revelan aspectos de su esfera más íntima, como su estado de salud, información genética, las creencias religiosas u opiniones políticas. También existen datos relacionados con su entorno familiar, trayectoria académica, actividad laboral o interacción con tecnologías y servicios digitales.



Conocer estas diferencias es importante para comprender que los datos personales pueden clasificarse de acuerdo con la naturaleza de la información que contienen y que algunos de ellos, por los riesgos asociados con su tratamiento, requieren medidas reforzadas de protección digital.

La legislación mexicana distingue, entre otros conceptos relevantes, los datos personales de los datos personales sensibles. Asimismo, en el ámbito jurídico y administrativo se utilizan diversas categorías para identificar la naturaleza de la información tratada, como los datos identificativos, laborales, patrimoniales, académicos, electrónicos y biométricos.

En este capítulo conocerás algunas de las principales categorías utilizadas para clasificar los datos personales en el marco jurídico y administrativo mexicano, así como ejemplos que te ayudarán a identificarlas en situaciones de la vida cotidiana.

2.1 Datos personales de identificación

Los datos personales de identificación también denominados datos identificativos en diversos instrumentos y criterios administrativos comprenden información que permite reconocer, distinguir o acreditar la identidad de



una persona (Davara, Barco & Cervantes, 2019, p. 215). Este tipo de información se solicita con frecuencia al realizar un trámite, contratar un servicio, abrir una cuenta bancaria, inscribirse en una institución educativa o acreditar la identidad ante una autoridad.

En muchas actividades cotidianas, estos son algunos de los primeros datos que una persona proporciona. Su tratamiento permite, entre otras finalidades, verificar la identidad de la persona titular, distinguirla de otras con datos similares y dar certeza jurídica, administrativa o comerciales.

Aunque comúnmente se consideran datos “básicos” de identificación, esto no significa que su protección sea menos importante. Su tratamiento inadecuado o utilización ilícita puede generar riesgos para las personas, entre ellos la suplantación, el fraude o el acceso no autorizado a cuentas, servicios y trámites (Guardia Nacional CERT-MX, 2023) (CONDUSEF, 2021).

Por ello, incluso cuando se trate de información utilizada habitualmente para identificar a una persona, quien la recabe y utilice debe observar las obligaciones y principios aplicables en materia de protección de datos personales.

¿Qué información integra los datos de identificación?

Los datos personales de identificación pueden comprender información que permite reconocer o distinguir de manera directa a una persona o relacionarla con documentos oficiales emitidos por las autoridades competentes.

Tabla 2.1 Ejemplos de datos personales que pueden identificar o hacer identificable a una persona.

- Nombre y apellidos
- Fecha de nacimiento
- Lugar de nacimiento
- Fotografía
- Firma
- CURP
- RFC
- Número de pasaporte
- Datos de una licencia de conducir
- Datos de la Cartilla del Servicio Militar Nacional, cuando corresponda



Nota: Los ejemplos de esta tabla son únicamente ilustrativos. No constituyen una clasificación legal ni una lista cerrada establecida por la legislación. Un dato es personal cuando la información concierne a una persona física identificada o identificable, conforme a la legislación aplicable.

Fuente: LPDPPSONL, 2019, art. 3, fracción X.

¿Por qué son importantes?

Los datos de identificación hacen posible que las personas acrediten su identidad para ejercer sus derechos y acceder a diversos servicios. Por ejemplo, pueden ser necesarios para realizar trámites relacionados con el registro civil, inscribirse en una institución educativa, recibir determinados servicios de salud, celebrar contratos, ejercer derechos político-electorales, abrir una cuenta bancaria o realizar trámites ante autoridades de los distintos órdenes de gobierno.

¿Qué cuidados deben tener?

Aunque los datos de identificación se solicitan con frecuencia, ello no significa que deban compartirse sin precaución.

Antes de proporcionar información personal, es recomendable identificar quién la solicita, para que será utilizada y consultar el aviso de privacidad. Quien trata datos personales debe hacerlo conforme a las finalidades y demás condiciones establecidas en la legislación mexicana vigente en protección de datos personales y demás que resulten aplicables.

También es importante evitar compartir copias de documentos oficiales, fotografías de identificaciones o imágenes que contengan datos personales a través de redes sociales, servicios de mensajería o sitios de internet cuya autenticidad o seguridad no pueda comprobarse.

Una acción tan sencilla como verificar el destinatario antes de enviar una copia de una identificación oficial puede contribuir a reducir el riesgo de un uso indebido de la información.

Datos personales de identificación

¿Qué son? Son los datos que, por su naturaleza o función, permiten identificar, distinguir o acreditar la identidad de una persona.

¿Para qué se utilizan? Para identificar o acreditar la identidad una persona, realizar trámites, acceder a servicios y dar certeza a determinados actos jurídicos o administrativos.

Algunos ejemplos: nombre y apellidos, fotografía, fecha y lugar de nacimiento, CURP, RFC, firma, y números o datos contenidos en documentos oficiales, como el pasaporte o licencia de conducir.



¿Por qué deben protegerse? Porque una utilización indebida puede facilitar la suplantación de identidad, el fraude o el acceso no autorizado a información, cuentas, trámites o servicios.

Concepto clave. Los datos personales de identificación permiten reconocer, distinguir o acreditar la identidad de una persona ante autoridades, instituciones y particulares. Aunque se utilizan de manera habitual, deben ser tratados conforme a la legislación mexicana vigente en protección de datos personales y demás que resulten aplicables, ya que su uso indebido puede generar afectaciones importantes para su titular.

Conclusión. Los datos personales de identificación están presentes en numerosas actividades de la vida cotidiana y son fundamentales para acreditar nuestra identidad ante las autoridades, instituciones y empresas. Su tratamiento responsable facilita el ejercicio de derechos y el acceso a servicios; al mismo tiempo, exige que quienes los recaban los utilicen y protejan conforme a las disposiciones legales aplicables. Las personas también pueden contribuir a su protección evitando compartirlos innecesariamente o a través de medios que no ofrezcan condiciones adecuadas de seguridad. En el siguiente apartado conoceremos otras categorías de información personal que requiere una protección reforzada debido a la naturaleza de los datos que contiene.

2.2 Datos personales patrimoniales, financieros, laborales y académicos

Además de los datos que permiten identificar a una persona, existen otros que describen distintos aspectos de su vida. Algunos reflejan su situación económica; otros se relacionan con su trayectoria laboral, su preparación académica o su experiencia profesional.

Este tipo de información se solicita con frecuencia al realizar trámites, solicitar un crédito, buscar empleo, inscribirse en una institución educativa, contratar determinados servicios o participar en programas públicos.

Aunque estos datos no siempre se consideran sensibles en términos legales, sí requieren un tratamiento responsable, ya que un uso indebido puede afectar el patrimonio, la reputación, las oportunidades laborales o el



desarrollo profesional de una persona. Por ello, quienes los recaban deben utilizarlos únicamente para las finalidades que justificaron su obtención y protegerlos mediante las medidas de seguridad previstas en la legislación.

Datos personales patrimoniales

¿Qué son? Son los datos relacionados con los bienes, derechos y obligaciones económicas que integran o permiten conocer aspectos del patrimonio de una persona.



¿Qué información incluyen? Información sobre bienes inmuebles, vehículos, propiedades, inversiones, participaciones accionarias, deudas y otras obligaciones de carácter patrimonial.

¿Cuándo suelen solicitarse? Al solicitar un crédito, contratar un seguro, realizar operaciones notariales, intervenir en ciertos procedimientos judiciales o cumplir obligaciones fiscales, entre otros supuestos.

¿Por qué deben protegerse? Porque pueden revelar aspectos de la situación patrimonial de una persona y su utilización indebida puede facilitar fraudes, extorsiones o delitos patrimoniales.

Datos personales financieros

¿Qué son? Son los datos relacionados con las operaciones, productos o servicios financieros de una persona y con el manejo de sus recursos económicos.



¿Qué información incluyen? Número de cuenta bancaria, CLABE interbancaria, historial crediticio, información sobre créditos, ingresos, estados de cuenta y datos de tarjetas de débito o crédito.

¿Cuándo suelen solicitarse? Al abrir una cuenta bancaria, solicitar un crédito, realizar inversiones, recibir pagos o efectuar otras operaciones financieras.

¿Por qué deben protegerse? Porque un acceso no autorizado puede generar pérdidas económicas, suplantación de identidad o afectaciones patrimoniales.

Datos personales laborales

¿Qué son? Son los datos relacionados con la actividad profesional, el empleo o la trayectoria laboral de una persona.

¿Qué información incluyen? Puesto desempeñado, antigüedad laboral, nombre del empleador, experiencia profesional, referencias laborales, salario, evaluaciones de desempeño y capacitación recibida.

¿Cuándo suelen solicitarse? Durante procesos de contratación, promociones, evaluaciones de desempeño, prestaciones laborales o trámites de seguridad social.

¿Por qué deben protegerse? Porque pueden influir en oportunidades de empleo y desarrollo profesional, además de contener información confidencial sobre la relación laboral.



Datos personales académicos

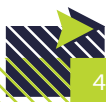
¿Qué son? Son los relacionados con la formación educativa y la trayectoria académica de una persona.

¿Qué información incluyen? Nivel de estudios, certificados, títulos profesionales, cédula profesional, historial académico, calificaciones, constancias y diplomas, entre otros.

¿Cuándo suelen solicitarse? Para ingresar a instituciones educativas, concursar por una plaza, acreditar estudios o participar en procesos de selección de personal.

¿Por qué deben protegerse? Porque forman parte de la trayectoria educativa y profesional de una persona y su tratamiento indebido puede afectar su privacidad o generar consecuencias en determinados procesos académicos o laborales.





¿Qué tienen en común estos datos?

Aunque cada categoría responde a una finalidad distinta, todas contienen información que describe aspectos relevantes de la vida de una persona.

Por esa razón, las instituciones públicas y los particulares únicamente deben solicitar los datos que resulten necesarios para cumplir una finalidad específica y legítima. Además, están obligadas a protegerlos contra el acceso, uso, alteración, pérdida o divulgación no autorizados.

Como regla general, las personas también deben ser cuidadosas al compartir este tipo de información, especialmente cuando utilizan plataformas digitales, redes sociales o realizan trámites por internet.

Conclusión. Los datos personales no solo permiten identificar a una persona; también reflejan parte de su historia, su patrimonio, su desarrollo profesional y su formación académica. Por ello, su protección resulta indispensable para evitar riesgos que puedan afectar la seguridad económica, la estabilidad laboral o las oportunidades educativas de las personas. Conocer estas categorías permite comprender que la protección de los datos personales abarca distintos ámbitos de la vida cotidiana y que toda información debe ser tratada conforme a los principios y obligaciones establecidos por la legislación mexicana vigente en protección de datos personales y demás que resulten aplicables.

2.3 Datos personales sensibles

En la vida cotidiana existen datos personales que, por su naturaleza, requieren una protección mayor. Se trata de información que revela aspectos íntimos de una persona o que, si se utiliza de manera indebida, podría dar lugar a actos de discriminación, exclusión, violencia o afectar gravemente su dignidad y sus derechos.

A este tipo de información la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Nuevo León la denomina datos personales sensibles.

La diferencia con otros datos personales no radica únicamente en su contenido, sino en las posibles consecuencias que podría tener su divulgación, pérdida o uso no autorizado. Mientras que el nombre o el domicilio permiten identificar a una persona, un dato sensible puede revelar información



relacionada con su salud, origen racial o étnico, información genética, convicciones u otros aspectos vinculados con su esfera personal.

Por esa razón, las instituciones públicas y los particulares que tratan este tipo de información tienen la obligación de adoptar medidas de protección reforzadas y utilizarla únicamente cuando exista una finalidad legítima y conforme a la ley.

¿Qué son los datos personales sensibles?

La Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Nuevo León define como datos personales sensibles aquellos que se refieren a la esfera más íntima de una persona o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para ella.

En términos sencillos, son datos que, si llegan a manos equivocadas o se utilizan sin autorización, pueden afectar la integridad, la seguridad, la igualdad de oportunidades o el ejercicio de otros derechos fundamentales.

Por ello, su tratamiento está sujeto a requisitos y exige mayores medidas de seguridad, así como un especial cuidado por parte de quienes los tratan.

¿Qué información se considera un dato personal sensible?

Aquellos que se refieran a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. Se consideran sensibles, de manera enunciativa más no limitativa, los datos personales que puedan revelar aspectos como origen racial o étnico, estado de salud pasado, presente o futuro, datos genéticos o datos biométricos, creencias religiosas, filosóficas y morales, opiniones políticas y preferencia sexual (LPDPPSONL, 2019, art. 3, fracción XI).

Origen racial o étnico. Información que permite conocer la pertenencia a un pueblo o comunidad indígena, adscripción afromexicana, información relacionada con el origen étnico.

Estado de salud. Información que revele el estado de salud física o mental, pasado, presente o futuro (por ejemplo, expediente clínico, diagnósticos médicos, discapacidades, alergias, tratamientos médicos e información genética).



Información genética. Información relacionada con las características genéticas de una persona que, por su contenido y utilización, puede revelar aspectos especialmente vinculados con su salud o identidad biológica.

Características biométricas. Su naturaleza jurídica debe analizarse de acuerdo con la información que revelen, la finalidad y contexto de su tratamiento y, particularmente, con los criterios legales que determinan cuándo un dato afecta la esfera más íntima de una persona o cuándo su utilización indebida puede provocar discriminación o un riesgo grave.

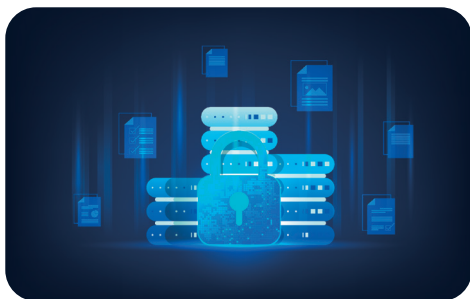
Creencias religiosas, filosóficas o morales. Información relacionada con las convicciones personales, tales como la religión, creencias espirituales, convicciones filosóficas.

Opiniones políticas. Información que revela la afinidad, participación o preferencias políticas de una persona; esto comprende la militancia partidista, preferencias políticas, participación en actividades políticas.

Preferencias sexuales. Información relacionada con la orientación o las preferencias sexuales de una persona.

¿Por qué reciben una protección especial?

Los datos personales sensibles reciben una protección reforzada porque su divulgación o utilización indebida puede afectar gravemente la vida de una persona.



Por ejemplo, la difusión no autorizada de un diagnóstico médico puede vulnerar la privacidad de un paciente; revelar información sobre las creencias religiosas o las opiniones políticas puede dar lugar a actos de discriminación; y la utilización indebida de datos biométricos puede facilitar suplantaciones de identidad difíciles de revertir.

Por ello, la legislación mexicana en protección de datos personales exige que quienes tratan datos personales sensibles adopten medidas de seguridad acordes con el riesgo que representa su tratamiento y limiten su utilización a los casos en que exista una base jurídica y una finalidad legítima.



¿Cuándo puede solicitarse?

Existen situaciones en las que una institución puede necesitar tratar datos personales sensibles para cumplir con las funciones que tiene legalmente encomendadas o para proporcionar un servicio.

Porejemplo, una institución pública de salud puede necesitar información relacionada con el estado de salud de una persona para brindarle atención; una autoridad puede requerir determinados datos para ejercer las atribuciones que la ley le confiere; o una institución educativa puede necesitar información médica para atender una situación relacionada con la salud de sus estudiantes.

En estos casos, el tratamiento de los datos personales sensibles debe sujetarse a las condiciones, principios, obligaciones y demás reglas previstas en la legislación aplicable.

Cuando se trate de sujetos obligados de Nuevo León, el marco principal es la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Nuevo León.

Cuando se trate de particulares, como una institución financiera privada, resulta aplicable la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

¿Cómo proteger tus datos personales sensibles?

- Comparte únicamente la información que sea necesaria.
- Identifica quién solicita tus datos y para qué serán utilizados.
- Verifica que la institución explique claramente para qué la solicita.
- Consulta el aviso de privacidad antes de proporcionar tus datos y revisa las finalidades del tratamiento.
- Evita publicar información médica, biométrica o relacionada con tus creencias en redes sociales sin considerar sus posibles consecuencias.
- Adopta precauciones adicionales al proporcionar información o elementos utilizados para identificación biométrica y verifica la legitimidad del servicio o institución que los solicita.
- Conserva tus documentos personales en lugares seguros y evita compartirlos por medios no confiables.





Concepto clave. Los datos personales sensibles requieren especial cuidado debido a la naturaleza de la información que contienen. En el caso de los sujetos obligados de Nuevo León, su tratamiento debe realizarse conforme a los principios y obligaciones establecidos en la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Nuevo León.

Conclusión. Los datos personales sensibles requieren un nivel de protección mayor debido a la información que contienen y a las consecuencias que podría tener su uso indebido. Su tratamiento implica una responsabilidad especial para las instituciones públicas y los particulares, quienes deben garantizar que esta información sea utilizada únicamente para las finalidades autorizadas y con las medidas de seguridad necesarias.

Para las personas, conocer qué información puede tener esta naturaleza permite tomar decisiones más informadas al compartirla y comprender que la protección de los datos personales también contribuye a salvaguardar la proteger la dignidad, la privacidad y el ejercicio de otros derechos fundamentales.

2.4 Datos que obran en registros de seguridad, procuración y administración de justicia

Existen datos personales que, por la institución que los resguarda y la finalidad para la que fueron obtenidos, requieren un tratamiento especial. Este es el caso de la información que forma parte de los registros de las autoridades encargadas de la seguridad pública, la procuración de justicia y la administración de justicia.

Estos datos pueden encontrarse, entre otros, en denuncias, carpetas de investigación (es importante precisar que el Código Nacional de Procedimientos Penales también contiene reglas específicas sobre los registros de investigación y su acceso), expedientes y procesos judiciales, registros de detención, sistemas penitenciarios, registros relacionados con personas desaparecidas, y otros sistemas de información administrados por las autoridades competentes.

Aunque esta información puede ser necesaria para la prevención o persecución de delitos y para el ejercicio de las funciones de seguridad, procuración y administración de justicia, su tratamiento está sujeto a reglas específicas. La legislación de Nuevo León establece que los datos personales utilizados por estas instituciones deben ser los necesarios y proporcionales para cumplir con sus funciones, además de estar protegidos mediante medidas de seguridad de nivel alto. (LPDPPSONL, 2019, art. 94, 95 y 96).

Las autoridades deben tratar los datos personales conforme al marco jurídico aplicable y adoptar las medidas necesarias para protegerlos contra el daño, pérdida, alteración, destrucción, uso, acceso o tratamiento no autorizado. Asimismo, el acceso público a la información contenida en estos registros debe determinarse de acuerdo con las disposiciones aplicables en materia de protección de datos personales, transparencia y acceso a la información, así como con las normas especiales que regulen cada procedimiento o sistema de información.

Esta protección adquiere especial relevancia cuando la divulgación de los datos puede afectar la privacidad, la seguridad, la dignidad, el debido proceso, la presunción de inocencia u otros derechos de las personas involucradas.

¿Qué información puede formar parte de estos registros?

Los registros relacionados con la seguridad pública, la procuración y la administración de justicia pueden contener datos personales de distintas personas que intervienen o se encuentran relacionadas con investigaciones, o actuaciones de las autoridades competentes, entre ellas:

- Personas denunciantes
- Víctimas u ofendidos
- Personas testigos
- Personas imputadas o sujetas a investigación
- Personas detenidas
- Personas procesadas o sentenciadas

- Personas privadas de la libertad
- Personas desaparecidas o no localizadas, así como, cuando corresponda, sus familiares
- Servidores públicos que participan en investigaciones o procedimientos
- Personas buscadas o localizadas en cumplimiento de una resolución judicial



Además de los datos de identificación, estos registros pueden contener información sobre hechos investigados o denunciados, declaraciones, entrevistas, informes, dictámenes periciales, fotografías, datos biométricos, documentos oficiales y otras actuaciones o elementos incorporados a una investigación, procedimiento, expediente, registro o sistema de información.

¿Por qué reciben una protección especial?

La información contenida en estos registros puede tener un impacto directo en los derechos de las personas.

Su divulgación indebida podría poner en riesgo una investigación, afectar el debido proceso, vulnerar la presunción de inocencia, comprometer la seguridad de víctimas o testigos, o incluso generar daños a la reputación y a la vida privada de quienes intervienen en un procedimiento.

Por ello, las autoridades deben proteger esta información mediante las medidas de seguridad previstas en la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Nuevo León, específicamente en sus artículos 36 y 96, al restringir su acceso a las personas autorizadas, de acuerdo con las funciones que desempeñan.

¿Qué tipo de información contienen? Datos personales relacionados con investigaciones, actuaciones de procuración de justicia, procesos judiciales, ejecución de sentencias y actividades vinculadas con la seguridad pública, entre otros supuestos previstos en la legislación aplicable.

¿Quiénes pueden aparecer en estos registros? Personas denunciantes, víctimas, testigos, personas imputadas, personas sentenciadas, personas privadas de la libertad y servidores públicos relacionados con el procedimiento.

¿Por qué debe protegerse? Porque el tratamiento o divulgación indebida de esta información pueden afectar la privacidad y la seguridad de las personas, comprometer una investigación o procedimiento, dependiendo del caso, incidir en derechos como el debido proceso y la presunción de inocencia.

¿Puede cualquier persona consultar esta información?

No. Aunque en México existe el derecho de acceso a la información pública, ello no significa que toda la información en poder de las autoridades sea pública.

Cuando un expediente o un registro contiene datos personales, las autoridades deben analizar cada caso conforme a la legislación mexicana vigente en protección de datos personales y demás que resulten aplicables para determinar qué información puede hacerse pública y cuál debe permanecer protegida.

Asimismo, existen procedimientos en los que la información puede mantenerse reservada mientras continúan las investigaciones o hasta que desaparezcan las causas que justificaron esa reserva, siempre de conformidad con la ley.

¿Qué derechos tienen las personas?

Las personas cuyos datos personales se encuentran en registros utilizados por instituciones de seguridad, procuración o administración de justicia tienen derecho a la protección de sus datos personales, de acuerdo con la legislación aplicable.



Esto significa que el hecho de que una institución utilice información personal para cumplir funciones de seguridad, prevención o persecución de delitos no elimina la obligación de proteger esos datos. La Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Nuevo León establece que las bases de datos utilizadas para estas funciones deben sujetarse a los principios previstos en la ley y contar con medidas de seguridad de nivel alto.

Asimismo, las personas pueden ejercer los derechos que la legislación reconoce respecto de sus datos personales, en los términos y bajo las condiciones que establece la propia ley.

En este tipo de registros, el ejercicio de estos derechos debe analizarse de acuerdo con la naturaleza de la información y con las funciones que realiza la institución responsable. Por ello, una solicitud relacionada con estos datos debe ser atendida conforme a las disposiciones específicas que resulten aplicables (LPDPPSONL, 2019, art. 94, 95 y 96).

Conclusión. Los registros de seguridad, procuración y administración de justicia contienen información indispensable para el funcionamiento de las instituciones encargadas de proteger a la sociedad y garantizar el acceso a la justicia. Sin embargo, también concentran datos personales cuya divulgación indebida puede afectar derechos fundamentales como la privacidad, la presunción de inocencia, el debido proceso y la seguridad de las personas. Por ello, la Ley de *Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Nuevo León* establece principios y obligaciones para que las instituciones públicas traten los datos personales de manera lícita y responsable, únicamente para finalidades concretas, lícitas, explícitas y legítimas relacionadas con sus atribuciones, y solo respecto de los datos que sean adecuados, relevantes y estrictamente necesarios para cumplir con esas finalidades.



2.5 Ejemplos ilustrativos

A lo largo de este capítulo conocimos que los datos personales pueden clasificarse de distintas maneras según la información que contienen. Sin embargo, en la vida cotidiana no solemos pensar en esas categorías cuando realizamos un trámite o contratamos un servicio.

Los siguientes casos muestran situaciones comunes en las que compartimos datos personales. Te invitamos a identificar qué tipo de información proporcionan y por qué es importante protegerla.



Caso 1. Inscripción en una universidad

Sofía fue aceptada en una universidad pública. Para concluir su inscripción, la institución le solicita diversos documentos e información, entre los que figuran el acta de nacimiento, CURP, fotografía, comprobante de domicilio, certificado de bachillerato, número telefónico, correo electrónico e información sobre alergias o alguna condición médica relevante.

Tabla 2.2 ¿Qué tipo de datos está proporcionando Sofía?

Información	Tipo de dato
Acta de nacimiento, CURP y fotografía	Datos de identificación
Certificado de estudios	Datos académicos
Domicilio, teléfono y correo electrónico	Datos de contacto
Información médica	Datos personales sensibles

¿Por qué los solicita la universidad? Para integrar el expediente escolar, verificar la identidad de la estudiante, mantener comunicación con ella y brindarle atención adecuada cuando sea necesario.

Recuerda. La universidad solo debe solicitar los datos que sean necesarios para cumplir con las finalidades relacionadas con la prestación del servicio educativo.

Caso 2. Solicitud de un crédito bancario

Miguel desea adquirir un automóvil mediante un crédito bancario. Antes de autorizar el financiamiento, la institución le solicita información relacionada con su identidad y su situación económica, tales como la identificación oficial, RFC, comprobante de domicilio, comprobantes de ingresos, estados de cuenta e historial crediticio.

Tabla 2.3 ¿Qué tipo de datos está proporcionando Miguel?

Información	Tipo de dato
Identificación oficial y RFC	Datos de identificación
Comprobante de domicilio	Datos de contacto
Estados de cuenta e historial crediticio	Datos financieros
Comprobantes de ingresos	Datos patrimoniales y financieros

¿Por qué los solicita el banco? Para verificar la identidad del solicitante, evaluar su capacidad de pago y cumplir con las disposiciones legales aplicables al otorgamiento de créditos.

Recuerda. Antes de entregar información financiera, verifica que la institución sea legítima y revisa su aviso de privacidad.

Caso 3. Consulta médica

Laura acude a un hospital para recibir atención médica. Como parte de su expediente clínico, el personal de salud solicita información relacionada con su estado de salud, tales como nombre, CURP, fecha de nacimiento, antecedentes médicos, alergias, estudios de laboratorio y diagnóstico médico.

Tabla 2.4 ¿Qué tipo de datos está proporcionando Laura?

Información	Tipo de dato
Nombre y CURP	Datos de identificación
Antecedentes médicos, alergias, estudios y diagnóstico	Datos personales sensibles

¿Por qué los solicita el hospital? Para brindar un diagnóstico adecuado, proporcionar el tratamiento correspondiente y dar seguimiento a la atención médica.

Recuerda. La información sobre tu estado de salud merece una protección reforzada. Solo debe ser utilizada para las finalidades autorizadas por la ley.

Caso 4. Solicitud de empleo

Alejandro participa en un proceso de selección de personal. La empresa le solicita documentos para acreditar su preparación y experiencia, entre ellos se encuentran: el currículum vitae, título profesional, cédula profesional, referencias laborales, constancias de capacitación y número de seguridad social.



Tabla 2.5 ¿Qué tipo de datos está proporcionando Alejandro?

Información	Tipo de dato
Currículum y referencias	Datos laborales
Título y cédula profesional	Datos académicos
Número de seguridad social	Datos de identificación

¿Por qué los solicita la empresa? Para verificar que el candidato cumple con el perfil del puesto y acreditar su experiencia profesional.

Recuerda. Una empresa no debe solicitar información que no tenga relación con el puesto de trabajo que estás solicitando.

Caso 5. Presentación de una denuncia

Daniel acude ante la autoridad competente para denunciar el robo de su vehículo. Durante el procedimiento proporciona información personal y documentación relacionada con los hechos, como nombre, domicilio, teléfono, identificación oficial, narración de los hechos y documentos del vehículo.





Tabla 2.6 ¿Qué tipo de datos está proporcionando Daniel?

Información	Tipo de dato
Nombre e identificación	Datos de identificación
Domicilio y teléfono	Datos de contacto
Información contenida en la denuncia	Datos que obran en registros de seguridad y procuración de justicia

¿Por qué los solicita la autoridad? Para integrar la investigación correspondiente y dar seguimiento al procedimiento previsto por la ley.

Recuerda. La información contenida en una investigación debe protegerse para salvaguardar los derechos de las personas involucradas y el adecuado desarrollo del procedimiento.

¿Qué aprendimos?

Aunque cada situación es diferente, todas tienen un punto de encuentro, ya que las personas proporcionan datos personales para acceder a un servicio, ejercer un derecho o cumplir una obligación.

Antes de compartir tu información, recuerda hacerte preguntas tales como ¿Quién me solicita mis datos? ¿Para qué los necesita? ¿Son realmente necesarios? ¿Cómo serán protegidos?

Concepto clave. Identificar el tipo de datos personales que compartimos en cada situación cotidiana nos ayuda a ejercer nuestros derechos y a tomar decisiones informadas sobre nuestra información personal. Cuando entregas tus datos a una institución pública no pierdes tus derechos sobre ellos, la autoridad los recibe para cumplir una función pública y debe tratarlos conforme a las reglas que protegen tu información.

Una idea para recordar. Antes de entregar tus datos, pregunta quién los solicita, para qué los necesita y dónde puedes consultar el aviso de privacidad. Si después quieres saber qué información tiene una institución sobre ti, corregirla, solicitar su cancelación u oponerte a determinado tratamiento, puedes ejercer los derechos que correspondan.



¿Qué deben hacer las instituciones con tus datos personales?

Cuando realizas un trámite, recibes un servicio o ejerces un derecho ante una institución pública, puede ser necesario proporcionar datos personales. Dependiendo del trámite o servicio, pueden solicitarte, por ejemplo, tu nombre, domicilio, CURP, teléfono, correo electrónico, documentos de identidad u otra información necesaria para atender tu solicitud.

¿Para qué pueden necesitar esta información? Las instituciones públicas tratan datos personales para cumplir las funciones que la ley les atribuye y prestar servicios a la ciudadanía. Por ejemplo, un municipio puede requerir determinados datos para realizar un trámite; una escuela pública, para gestionar una inscripción y el expediente escolar; una institución de salud, para brindar atención; y una autoridad de seguridad o justicia, para ejercer cumplir las funciones que legalmente le corresponden.

Al tratar tus datos personales, la institución debe informarte sobre las características principales de su tratamiento mediante el aviso de privacidad. Además, debe utilizar la información para las finalidades que correspondan, tratar únicamente los datos adecuados, relevantes y necesarios, adoptar las medidas de seguridad aplicables y garantizar los mecanismos para que puedas ejercer tus derechos.

Puede utilizarlos para realizar las funciones que legalmente tiene encomendadas, prestar servicios, integrar expedientes, cumplir obligaciones, atender procedimientos o ejercer atribuciones. En determinados casos, tus datos también pueden ser transferidos a otras instituciones o terceros, siempre que exista un fundamento jurídico o se cumplan los requisitos previstos en la ley de la materia.

En otras palabras, que una autoridad tenga tus datos no significa que pueda utilizarlos para cualquier propósito. Su tratamiento debe estar relacionado con sus atribuciones y responder a finalidades determinadas, concretas, además de cumplir con los principios, deberes y demás obligaciones previstas en materia de protección de datos personales. Cuando quien trata tus datos es una institución estatal pública, será la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Nuevo León; y si es una Institución Pública Federal, será la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.



¿Qué ley aplica a tus datos personales cuando están en posesión de una institución pública de Nuevo León?

Si tus datos personales son tratados por una institución pública estatal o municipal de Nuevo León, por ejemplo, una dependencia o entidad del Gobierno del Estado, un municipio, alguno de los Poderes Ejecutivo, Legislativo o Judicial, una universidad pública o un partido político, entre otros sujetos obligados, su tratamiento debe realizarse conforme al marco jurídico vigente en materia de protección de datos personales.

Actualmente, este marco comprende la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y, en el ámbito local, la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Nuevo León.

Capítulo 3. ¿Quién tiene tus datos y por qué los quiere?

3.1 El sector público

Cuando realizas un trámite ante una institución pública, solicitas un servicio gubernamental, acudes a una escuela pública, recibes atención médica o participas en algún programa gubernamental, puede ser necesario que proporciones determinados datos personales.

Dependiendo del trámite o servicio que realices, pueden solicitarte diversos datos personales, como tu nombre, domicilio, teléfono, correo electrónico, fecha de nacimiento, identificación oficial o información contenida en documentos de identificación. Cuando resulte necesario, pueden tratarse datos personales sensibles, como aquellos relacionados con estado de salud, los cuales requieren una protección reforzada.

Sin embargo, que una institución pública tenga tus datos personales no significa que pueda utilizarlos para cualquier propósito. Su tratamiento debe estar relacionado con las atribuciones que legalmente le corresponden, responder a finalidades determinadas y cumplir con los principios, deberes y demás obligaciones establecidas en la normativa aplicable.





¿Qué instituciones públicas pueden tratar tus datos personales?

En Nuevo León, distintas instituciones públicas pueden tratar datos personales para cumplir las funciones y atribuciones encomendadas. Entre ellos se encuentran los Poderes Ejecutivo, Legislativo y Judicial; los municipios, órganos constitucionales autónomos, partidos políticos, así como los fideicomisos y fondos públicos, entre otros sujetos obligados previstos por la legislación estatal de la materia.

En la práctica, esto significa que tus datos pueden ser tratados por estar en manos de instituciones muy distintas, por ejemplo:

- Una dependencia del Gobierno del Estado;
- Un municipio;
- Una escuela pública;
- Un hospital o institución pública de salud;
- Un tribunal;
- El Congreso del Estado;
- Un Organismo Constitucional Autónomo;
- Una institución pública de educación superior;
- O alguna otra institución incluida en el padrón de sujetos obligados en materia de Protección de Datos Personales.

El Instituto Estatal de Transparencia, Acceso a la Información y Protección de Datos Personales, cuenta con un padrón de sujetos obligados responsables en materia de protección de datos personales, que permite identificar las instituciones públicas sujetas a las obligaciones previstas en la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Nuevo León, y demás normativa aplicable (INFONL, 2026).

¿Por qué una institución pública necesita tus datos?

Las instituciones públicas tratan datos personales cuando los necesitan para ejercer sus atribuciones, cumplir obligaciones legales y/o prestar los servicios que tienen a su cargo. La información necesaria dependerá de la finalidad y de las características de cada trámite, servicio o procedimiento.



Por ejemplo:

- Para realizar un trámite. Una institución pública puede necesitar determinados datos para identificarte, verificar que cumples con los requisitos aplicables y, cuando corresponda, para expedir un documento o prestar un servicio.
- Para brindarte atención médica. Una institución pública de salud puede tratar datos de identificación e información relacionada con tu estado de salud para brindarte atención y dar seguimiento a tu tratamiento adecuado.
- Para inscribirte en una escuela pública. La institución puede requerir información de la o el estudiante y, cuando corresponda, de su madre, padre, persona tutora o responsable.
- Para recibir un beneficio o participar en un programa público. Puede ser necesario proporcionar datos personales para verificar el cumplimiento de los requisitos establecidos y condiciones establecidas para recibirlo.
- Para cumplir una obligación legal. En algunos casos, hay situaciones en las que una institución debe recabar, utilizar o conservar determinada información porque una disposición jurídica así lo establece.



En todos estos casos, debe existir una razón que justifique el tratamiento de tus datos personales y que esté relacionada con las atribuciones de la Institución. Esto significa que una autoridad no puede pedirte información simplemente porque pueda resultarte útil, los datos que trate deben guardar relación con las finalidades y funciones que legalmente le corresponden.

¿La institución puede pedir cualquier dato?

No. Una institución pública no debe solicitar información personal de manera indiscriminada. La información que recaba debe guardar relación con sus atribuciones y con las finalidades para las que será tratada, de conformidad con la normativa aplicable en la materia.

Por ello, cuando te soliciten un dato, puedes preguntarte por qué necesitan dicha información. En algunos casos, un dato que a primera vista

puede parecer innecesario puede ser requerido para cumplir una obligación legal o atender las características particulares de un trámite o servicio, no significa que la institución esté actuando de forma incorrecta.

En cualquier caso, tienes el derecho a conocer cómo serán tratados tus datos de acuerdo con la ley de la materia.

¿Qué debe hacer una institución pública con tus datos?

Las instituciones que tratan datos personales bajo su responsabilidad deben cumplir con los principios, deberes y obligaciones que derivan de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Nuevo León, y demás normativa aplicable. Entre otras medidas, deben procurar que la información sea:

- Tratada para las finalidades que correspondan;
- Exacta, completa, correcta y actualizada;
- Protegida contra accesos, o usos, modificaciones o divulgaciones no autorizados;
- Accesible únicamente para quienes estén autorizados y necesiten tratarla en el ejercicio de sus funciones y;
- Conservada durante los plazos que correspondan conforme a las disposiciones legales aplicables.

Además, las instituciones deben adoptar medidas administrativas, físicas y técnicas para proteger los datos personales frente a posibles riesgos.



¿Y si una institución necesita compartir mis datos?

En determinadas circunstancias, una institución pública puede necesitar comunicar datos personales a otra autoridad, institución o tercero. A esta comunicación, en los supuestos previstos por la normativa en materia de datos personales, se le denomina transferencia de datos personales.

Sin embargo, esto no significa que tus datos puedan circular libremente de una institución a otra. Su transferencia debe realizarse conforme a las condiciones y requisitos establecidos en la ley estatal de protección de datos personales.

Por ejemplo, una disposición jurídica puede establecer que determinada información sea comunicada a otra autoridad para que esta pueda ejercer las atribuciones que legalmente le corresponden de acuerdo con su marco normativo.

Por ello, la institución pública tiene la obligación de informar a las personas sobre el tratamiento de sus datos personales, en cumplimiento al principio de información. Para ello, debe poner a disposición el aviso de privacidad, documento que permite conocer, entre otros aspectos, las finalidades del tratamiento, y, cuando corresponda, las transferencias de datos personales que puedan realizarse.

¿Cómo saber quién tiene tus datos?

Un primer paso es identificar las instituciones con las que has realizado trámites o ante las que has recibido algún servicio. Puedes preguntarte:

- ¿En qué dependencia realicé mi trámite?
- ¿En qué escuela pública entregué mis documentos?
- ¿En qué institución pública recibí atención?
- ¿A qué municipio proporcioné mis datos?
- ¿Qué organismo público me solicitó información?

Además, puedes consultar el padrón de sujetos obligados del Instituto de Transparencia, Acceso a la Información, y Protección de Datos Personales de Nuevo León (INFONL, 2026a) para identificar a las instituciones sujetas al régimen local.

Si quieres saber específicamente qué datos personales tiene una institución sobre ti y conocer información relacionada con su tratamiento, puedes ejercer tu derecho de acceso a tus datos personales. Más adelante te explicaremos cómo hacerlo.

Tus datos siguen siendo tuyos

Cuando proporcionas tus datos personales a una institución pública, conservas los derechos que la legislación en la materia te reconoce respecto de su tratamiento.

La Constitución Política del Estado Libre y Soberano de Nuevo León reconoce el derecho de las personas a la protección de sus datos personales. Asimismo, establece las bases legales para garantizar su protección cuando se encuentran en posesión de los sujetos obligados del ámbito estatal y municipal.

En consecuencia, puedes ejercer los derechos que la legislación reconoce para conocer y, cuando corresponda, solicitar la rectificación, cancelación, oposición y/o portabilidad al tratamiento de tus datos personales, es importante mencionar que el ejercicio de estos derechos se puede hacer de forma simultánea, ya que ninguno se contrapone al ejercicio del otro.

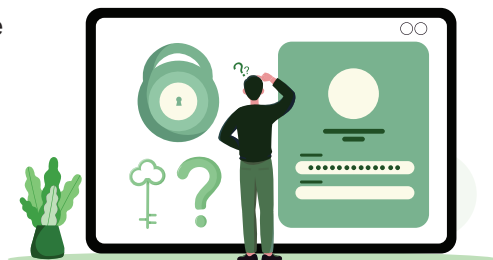
Además, si consideras que una institución pública de Nuevo León no está tratando adecuadamente tus datos o no respetó tus derechos, existen mecanismos para solicitar su protección ante el Instituto Estatal de Transparencia, Acceso a la Información y Protección de Datos Personales (INFONL). En los capítulos siguientes te explicaremos cuáles son y cómo utilizarlos.

Un ejemplo de la vida cotidiana

Imagina que realizas un trámite ante una institución pública del Estado de Nuevo León. Te solicitan tu nombre, identificación, domicilio y teléfono. La institución utiliza esos datos para integrar tu expediente y atender el trámite.

Meses después te surgen dudas sobre qué información tienen de ti, para qué la utilizan o quién puede verla. Estas son preguntas legítimas.

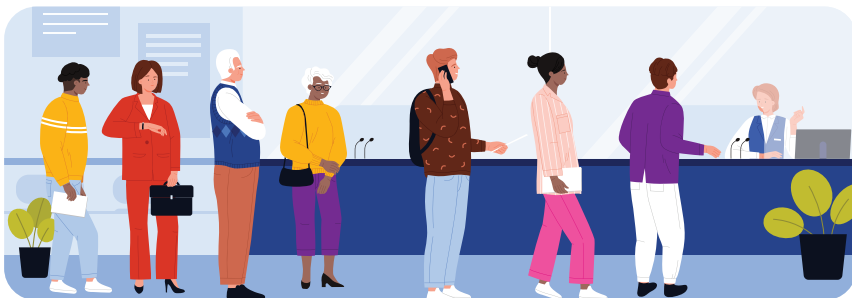
La protección de datos personales busca precisamente que las instituciones públicas no solo recaben y utilicen información de la ciudadanía, sino que también sean responsables de protegerla y de tratarla conforme a la normativa aplicable. Además, las personas cuentan con derechos que les permiten conocer y, cuando corresponda, ejercer control sobre el tratamiento de su información.



3.2 El sector privado

Además de las instituciones públicas, empresas, profesionistas y otras personas u organizaciones del sector privado tratan datos personales para desarrollar sus actividades, prestar servicios o mantener relaciones con sus clientes y usuarios.

Así, cada vez que abrimos una cuenta bancaria, compramos un producto por internet, acudimos a un hospital privado, contratamos un servicio de telefonía, nos inscribimos en un gimnasio o participamos en un programa de fidelidad, pueden recabarse o generar datos personales relacionados con nosotros.



Dependiendo del servicio o de la relación de que se trate, puede ser necesario proporcionar determinados datos personales. Sin embargo, ello no significa que los particulares puedan recabar cualquier información o utilizarla para cualquier finalidad.

En México, el tratamiento de datos personales por parte de los particulares se encuentra regulado por la Ley Federal de Protección de Datos Personales en Posesión de Particulares (LFPDPPP, 2025). Esta ley establece los principios, deberes y obligaciones para quienes tratan datos personales, así como los derechos, recursos y procedimientos que pueden ejercer sus titulares, ante el tratamiento de sus datos personales.

¿Quiénes pueden tratar tus datos en el sector privado?

Distintos tipos de profesionistas y organizaciones privadas pueden tratar datos personales como parte de sus actividades. Por ejemplo:

- Instituciones bancarias y financieras
- Hospitales, clínicas y laboratorios privados
- Escuelas y universidades particulares
- Compañías de seguros
- Comercios electrónicos
- Empresas de telefonía e internet
- Empresas de mensajería y paquetería
- Despachos profesionales y consultorías
- Tiendas departamentales y supermercados
- Hoteles y agencias de viajes
- Plataformas digitales
- Gimnasios y clubes deportivos

La información que pueden tratar dependerá de la naturaleza del servicio que presta, de las finalidades correspondientes y de las obligaciones legales aplicables.

¿Para qué utilizan tus datos personales?

Los particulares pueden tratar datos personales para distintas finalidades relacionadas con los servicios que prestan, las relaciones que mantienen con las personas y el cumplimiento de sus obligaciones. Algunos ejemplos son:



Tabla 3.1 Finalidades comunes del tratamiento de datos en el sector privado.

Finalidad	Ejemplo
Identificar a los clientes	Apertura de cuentas, contratación de servicios o celebración de contratos.
Prestar un servicio	Atención médica, servicios educativos, telecomunicaciones o transporte.
Procesar pagos	Facturación, cobros electrónicos y administración de cuentas.
Mantener comunicación	Confirmación de compras, envío de estados de cuenta o atención al cliente.
Cumplir obligaciones legales	Cumplimiento de obligaciones fiscales, financieras o de otra naturaleza previstas en la normativa que sea aplicable.

En todos los casos, el sector privado debe informar las características principales del tratamiento mediante el aviso de privacidad y tratar los datos personales conforme a las finalidades y condiciones previstas en la Ley Federal de Protección de Datos Personales en Posesión de Particulares (LFPDPPP, 2025).

El aviso de privacidad como una obligación para quien trata tus datos

Cuando un particular trata datos personales, tiene la obligación de informarte sobre las características principales de ese tratamiento mediante el aviso de privacidad. Este documento te permite conocer, entre otros aspectos:

- Quién es responsable del tratamiento de tus datos, y el domicilio donde se encuentra;
- Qué datos personales serán tratados;
- Para qué finalidades serán utilizados;
- Qué opciones y medios existen para limitar su uso o divulgación;
- Cómo puedes ejercer tus derechos de Acceso, Rectificación, Cancelación, y Oposición;
- Cómo puedes conocer los cambios al aviso de privacidad;
- Los medios de contacto para resolver dudas o presentar solicitudes relacionadas con el tratamiento de los datos personales.



Leer el aviso de privacidad te permite conocer el destino que tendrá la información antes de proporcionarla.

¿Puede una empresa pedir cualquier dato?

No. Los datos que se soliciten deben ser adecuados, relevantes, pertinentes y necesarios en relación con las finalidades para las que serán tratados.

Por ejemplo, una tienda en línea puede necesitar tu domicilio para entregar un producto; sin embargo, no debería solicitar información que no guarde relación con esa la compra o con alguna otra finalidad legítima y debidamente informada.

Además, cuando una empresa u otro particular trate datos personales sensibles, deberá observar medidas reforzadas de protección. Entre otras

obligaciones, debe justificar la necesidad de su tratamiento para finalidades legítimas y concretas y, cuando corresponda, obtener el consentimiento expreso y por escrito de la persona titular, además de adoptar las medidas necesarias para proteger esta información.

La Ley Federal de Protección de Datos Personales en Posesión de los Particulares establece expresamente dos reglas particularmente importantes para los datos sensibles:

1. Consentimiento expreso y por escrito. Como regla aplicable al tratamiento de datos personales sensibles, el responsable debe obtener el consentimiento expreso y por escrito de la persona titular, mediante firma autógrafa, firma electrónica u otro mecanismo de autenticación, sin perjuicio de las excepciones legales en las que no es necesario recabar consentimiento.
2. Justificación de las bases de datos sensibles. No pueden crearse bases de datos que contengan datos personales sensibles si su creación no se justifica para finalidades legítimas, concretas y acordes con las actividades o fines del responsable.



A ello se suman los principios generales de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad.

¿Qué obligaciones tiene quien trata tus datos personales?

Cuando una persona entrega sus datos personales a una empresa, espera que esta actúe con responsabilidad y proteja su información. Por ello, quienes tratan datos personales en el sector privado tienen, entre otras, las siguientes obligaciones:

- Informar de manera clara cómo utilizarán los datos personales.
- Tratar datos adecuados, relevantes y necesarios para las finalidades correspondientes.
- Implementar medidas de seguridad para proteger la información.
- Evitar el acceso, uso o divulgación no autorizados.

- Contar con mecanismos para atender el ejercicio de los derechos reconocidos por la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

Al cumplirse estas obligaciones fortalecen la confianza entre las personas consumidoras y las empresas, favoreciendo relaciones transparentes y responsables.

Un ejemplo de la vida cotidiana

Imagina que decides comprar un teléfono celular a través de una tienda en línea. Para completar la compra, la empresa solicita tu nombre, domicilio, número telefónico, correo electrónico y los datos necesarios para procesar el pago.

Cada uno de estos datos cumple una finalidad específica; en particular, identificar a la persona compradora, enviar el producto al domicilio correcto, mantener comunicación durante el proceso de pago y dar seguimiento a la operación comercial.

La empresa debe tratar esos datos conforme a las finalidades informadas en el aviso de privacidad y a las demás condiciones previstas en la legislación aplicable. Si pretende utilizarlos para una finalidad distinta, deberá observar los requisitos que la ley establece para ello.

Concepto clave. Las empresas y organizaciones privadas que traten datos personales deben hacerlo conforme a los principios, deberes y obligaciones establecidos por la Ley Federal de Protección de datos personales y demás normativa aplicable. Esto significa que no pueden utilizar la información de manera arbitraria y deben respetar los derechos de las personas titulares.

Conclusión. El sector privado trata datos personales en numerosas actividades de nuestra vida cotidiana, desde una compra por internet hasta la contratación de servicios financieros, educativos o de salud. Sin embargo, que una empresa tenga tus datos no significa que pueda utilizarlos libremente. Como ya lo hemos mencionado anteriormente, su tratamiento debe realizarse conforme a las finalidades, principios, deberes y demás obligaciones establecidas en el marco normativo aplicable.

Por ello, conocer quién trata tus datos personales, para qué los utiliza y qué derechos puedes ejercer te permite tomar decisiones más informadas al contratar un servicio, realizar una compra o relacionarte con una empresa u organización privada.

3.3 Diferencias entre el régimen público y el privado

Hasta ahora hemos visto que tanto las instituciones públicas como las empresas privadas pueden tratar datos personales. Sin embargo, no todas lo hacen bajo las mismas reglas.

En México, el tratamiento de datos personales se encuentra sujeto a regímenes jurídicos distintos según quién sea responsable de la información, es decir, uno aplicable a los sujetos obligados del sector público y otro a las personas físicas o morales de carácter privado. Aunque ambos buscan proteger los datos personales y garantizar los derechos de sus titulares, existen diferencias en las reglas, obligaciones, procedimientos y autoridades competentes.

Conocer esta diferencia permite comprender por qué los procedimientos, las obligaciones e incluso las autoridades competentes pueden variar dependiendo de quién trate nuestros datos personales.



¿Qué es el régimen público?

El régimen público regula el tratamiento de datos personales realizado por las instituciones públicas del Estado en el ejercicio de sus atribuciones y funciones.

Esto significa que una institución pública no puede tratar datos personales de manera arbitraria, el tratamiento debe estar relacionado con las atribuciones que legalmente le corresponden, responder a finalidades concretas, lícitas, explícitas y legítimas, y cumplir con los principios, deberes y demás obligaciones previstas en la normativa aplicable.

Por ejemplo, una institución pública puede necesitar determinados datos personales para expedir un documento oficial, prestar un servicio público, o integrar un expediente o atender un procedimiento.

¿Qué es el régimen privado?

El régimen privado regula el tratamiento de los datos personales realizado por personas físicas o morales de carácter privado, como empresas, profesionistas y organizaciones particulares. Por ejemplo, una institución



bancaria, una escuela particular, un hospital privado, una aseguradora o una tienda en línea pueden tratar datos personales para prestar servicios, mantener una relación con sus clientes, celebrar contratos o cumplir las obligaciones legales que les corresponden.

En ambos regímenes, las personas cuentan con derechos para proteger sus datos personales y ejercer control sobre su tratamiento en los términos previstos por la legislación aplicable.

¿En qué se parecen?

Aunque se trata de regímenes distintos, ambos establecen principios, deberes y obligaciones destinados a proteger los datos personales y los derechos de sus titulares. En términos generales, quienes tratan datos personales deben hacerlo conforme a la legislación aplicable:

- Tratar los datos personales para finalidades determinadas y legítimas;
- Tratar únicamente la información adecuada y necesaria de acuerdo con las finalidades correspondientes;
- Adoptar medidas físicas, técnicas y administrativas para proteger los datos frente a accesos, usos o divulgaciones no autorizados; y
- Garantizar el ejercicio de los derechos reconocidos a las personas titulares.

En otras palabras, aunque las reglas específicas pueden variar, tanto las instituciones públicas como los particulares tienen obligaciones respecto de la protección de los datos personales que tratan.

¿En qué son diferentes?

Una de las principales diferencias se encuentra en la naturaleza de quien realiza el tratamiento de los datos personales y en el marco jurídico que regula sus actividades. De ello derivan diferencias en las bases y condiciones del tratamiento, las obligaciones, los procedimientos y recursos para ejercer sus derechos y las autoridades garantes competentes.

Tabla 3.2 Régimen público y régimen privado.

Aspecto	Sector público	Sector privado
¿Quién trata los datos?	Autoridades, entidades, órganos y demás sujetos obligados.	Empresas, profesionistas y personas físicas o morales de carácter privado sujetas a la legislación correspondiente.
¿Para qué pueden tratarlos?	Para ejercer atribuciones, cumplir obligaciones y prestar servicios o realizar funciones públicas.	Para prestar servicios, mantener relaciones jurídicas, celebrar contratos, desarrollar sus actividades y cumplir obligaciones.
¿Qué legislación aplica?	LPDPPSONL, LGPDPPSO y demás disposiciones aplicables.	LFPDPPP y demás disposiciones aplicables.
¿El consentimiento siempre es necesario?	No. Existen tratamientos relacionados con atribuciones y obligaciones legales en los que el consentimiento no constituye la base para tratar los datos.	Como regla general, el tratamiento está sujeto al consentimiento, salvo las excepciones previstas por la ley.
¿Qué deben hacer?	Cumplir los principios, deberes y obligaciones previstos en el régimen aplicable y garantizar los derechos de las personas.	Cumplir los principios, deberes y obligaciones previstos en la LFPDPPP y garantizar los derechos de las personas.
¿Quién protege tus datos personales?	Las autoridades garantes competentes, de acuerdo con el ámbito federal o local. En Nuevo León, el Instituto Estatal de Transparencia, Acceso a la Información y Protección de Datos Personales (INFONL) es el organismo autónomo encargado de garantizar el derecho a la protección de datos personales en posesión de los sujetos obligados.	Unidad de Protección de Datos Personales, la cual está adscrita a la Secretaría Anticorrupción y Buen Gobierno a través de su órgano desconcentrado Transparencia para el Pueblo.

Un ejemplo de la vida cotidiana

Imagina que proporcionas tu nombre, domicilio y CURP en dos situaciones distintas. En la primera, acudes a un hospital público para recibir atención médica. En la segunda, contratas un seguro de gastos médicos con una empresa privada.

En ambos casos se tratan datos personales; sin embargo, las reglas aplicables son distintas. El hospital público trata la información en el ejercicio de sus funciones y conforme al régimen aplicable al sector público. Por su parte, la aseguradora trata los datos en el marco de una relación de carácter privado y conforme a la legislación aplicable al sector privado.

A pesar de estas diferencias, ambos deben cumplir las obligaciones que les correspondan para proteger tus datos personales y respetar tus derechos.

¿Por qué es importante conocer esta diferencia?

Identificar quién trata tus datos personales es uno de los primeros pasos para saber qué reglas se aplican, qué derechos puedes ejercer, cómo debes presentar una solicitud y ante qué autoridad puedes acudir si consideras que tus datos fueron tratados indebidamente.

Por ello, antes de iniciar cualquier procedimiento relacionado con la protección de tus datos, conviene preguntarte y determinar si una institución pública o un particular tiene tus datos; esto te permitirá identificar la ruta que debes seguir para ejercer tus derechos.

Concepto clave. En México existen reglas distintas para el tratamiento de datos personales dependiendo de quién los trata. Si se encuentran en posesión de una institución pública, se aplica el régimen correspondiente a las autoridades; si los trata una empresa, profesionista u otro particular, se aplica el régimen previsto para el sector privado. Identificar quién tiene tus datos es fundamental para saber qué derechos puedes ejercer, cómo hacerlo y ante qué autoridad acudir.

Conclusión. Ahora que conoces quién puede tratar tus datos personales y qué régimen le corresponde, surge la importante duda sobre si puede compartírlas con alguien más.



3.4 ¿Cuándo pueden compartir tus datos con terceros?

Cuando proporcionamos datos personales para realizar un trámite, contratar un servicio o ejercer un derecho, es natural preguntarnos qué puede ocurrir con esa información y si puede ser comunicada a otras personas, instituciones o empresas.

La respuesta es que los datos personales no pueden compartirse libremente. Su comunicación debe cumplir las condiciones establecidas en la legislación aplicable.

En México, la legislación establece que los datos personales deben utilizarse para las finalidades que justificaron su obtención y que cualquier comunicación de esa información debe realizarse conforme a la ley, respetando los derechos de las personas y aplicando las medidas necesarias para protegerla.

Esto significa que tanto las instituciones públicas como las organizaciones privadas deben actuar con responsabilidad cuando exista la necesidad de compartir datos personales con otra autoridad o con otra entidad.



¿Qué significa compartir datos personales?

En términos sencillos, significa comunicar datos personales a otra persona, institución u organización. Cuando esa comunicación se realiza a un tercero distinto de la persona titular, del responsable o de quien trata los datos personales por cuenta de este, puede constituir una transferencia de datos personales en los términos previstos por la legislación aplicable. Las transferencias pueden realizarse, por ejemplo:

- Entre instituciones públicas;
- entre particulares;
- de una institución pública a un particular;
- o de un particular a una autoridad competente.

Siempre que se cumplan los requisitos previstos en la normativa aplicable.



No toda comunicación de datos es una transferencia

En ocasiones, una institución o empresa necesita que otra persona u organización trate datos personales por su cuenta y siguiendo sus instrucciones, por ejemplo, para prestar un servicio. En estos casos puede existir una relación entre un responsable y una persona encargada del tratamiento.

A esta comunicación se le denomina remisión y tiene reglas distintas de una transferencia.

En términos sencillos, en una transferencia los datos se comunican a otro responsable o tercero en los términos previstos por la ley; en una remisión, una persona encargada trata los datos por cuenta y siguiendo las instrucciones del responsable.

¿Por qué puede ser necesario compartir información?

Existen distintas circunstancias en las que puede ser necesario comunicar datos personales. Por ejemplo, una transferencia puede estar prevista en una disposición jurídica, ser necesaria para el ejercicio de determinadas atribuciones o resultar indispensable para atender alguno de los supuestos establecidos por la legislación.

En el sector público, la Ley General y la Estatal en materia de datos personales, contempla expresamente diversos supuestos en los que puede realizarse una transferencia sin consentimiento, incluyendo transferencias previstas en leyes o tratados; entre responsables para facultades compatibles o análogas; para investigación y persecución de delitos y procuración o administración de justicia; para reconocimiento, ejercicio o defensa de derechos; y otros casos legalmente establecidos.

En todos estos casos, la comunicación de datos debe responder a una finalidad legítima y encontrarse prevista en el marco jurídico correspondiente.



¿Existen límites para compartir datos personales?

Sí. Que una institución o empresa tenga tus datos personales no significa que pueda comunicarlos libremente a cualquier persona o utilizarlos para cualquier finalidad.

Como regla general, las transferencias deben realizarse conforme a las finalidades del tratamiento y cumplir con los requisitos establecidos por la legislación aplicable. Dependiendo del régimen y de las circunstancias, puede requerirse el consentimiento de la persona titular o actualizarse alguna de las excepciones previstas por la ley de la materia.

Cuando la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Nuevo León y Ley Federal de Protección de Datos Personales en Posesión de los Particulares, permiten comunicar datos personales, esa comunicación debe realizarse respetando principios como la licitud, la finalidad, la proporcionalidad y la responsabilidad, además de aplicar medidas de seguridad para evitar accesos o divulgaciones no autorizadas.

Ejemplos de situaciones en las que pueden comunicarse datos personales

Aunque cada situación debe analizarse conforme a la legislación mexicana vigente de protección de datos personales y demás que resulten aplicables, algunos ejemplos son los siguientes:

Tabla 3.3 Casos en los que puede estar prevista la comunicación de datos personales.

Situación	¿Cuál puede ser la finalidad?
Atención médica	Para dar continuidad al tratamiento del paciente o cumplir obligaciones sanitarias previstas por la ley.
Procedimientos administrativos	Cuando una autoridad debe remitir un expediente a otra institución competente.
Procesos judiciales	Cuando una autoridad jurisdiccional o ministerial requiere información conforme a sus atribuciones legales.
Contratación de servicios	Cuando es necesario comunicar datos a proveedores que participan en la prestación del servicio, siempre bajo las obligaciones legales correspondientes.



Estos ejemplos muestran que la comunicación de datos personales no depende de la voluntad de quien posee la información, sino de las condiciones establecidas por la legislación aplicable.

¿Cómo puedes saber si tus datos podrían transferirse?

Tanto las instituciones públicas como las organizaciones privadas deben informar a las personas sobre el tratamiento que recibirán sus datos personales.

Una de las principales fuentes de esa información es el aviso de privacidad, en el que se explica, entre otros aspectos:

- Qué datos personales serán recabados.
- Para qué serán utilizados.
- Si existe la posibilidad de transferir la información en los casos previstos por la legislación.
- Los medios para ejercer los derechos que reconoce la ley.

Leer este documento permite conocer con mayor claridad el destino que tendrá la información proporcionada.

Un ejemplo de la vida cotidiana

Imagina que compras un producto en una tienda en línea. La empresa recibe tu nombre, domicilio y número telefónico para procesar la compra y, posteriormente, comparte esos datos con la empresa de paquetería encargada de realizar la entrega.

En este caso, la comunicación de los datos tiene una finalidad específica, la cual es hacer llegar el producto al domicilio correcto. Sin embargo, esa información no puede utilizarse para fines distintos de aquellos para los que fue compartida, salvo en los casos permitidos por la legislación.

Concepto clave. Transferir (Comunicar) datos personales no es una decisión discrecional. Tanto las instituciones públicas como las organizaciones privadas solo pueden comunicar información personal cuando existe una base jurídica que lo permita y siempre respetando los derechos de las personas y las obligaciones previstas por la legislación.

Conclusión. En ocasiones, transferir datos personales entre instituciones o con terceros es necesario para prestar un servicio, cumplir una obligación legal o garantizar el ejercicio de un derecho. Sin embargo, esa posibilidad no elimina el deber de proteger la información ni autoriza un uso indiscriminado de los datos personales. La legislación mexicana establece reglas claras para que estas comunicaciones se realicen únicamente cuando exista una justificación legal, una finalidad legítima y las medidas de seguridad necesarias para proteger la información. Conocer estas reglas permite a la ciudadanía comprender mejor cómo circulan sus datos personales y fortalecer la confianza en las instituciones y organizaciones que los tratan.

3.5 ¿Qué autoridad puede ayudarte?

Cuando consideras que tus datos personales no fueron tratados correctamente, no estás solo. Existen autoridades a las que puedes acudir para recibir orientación y, cuando corresponda, solicitar la protección de tus derechos. Dependiendo de su ámbito de competencia, estas auto-



ridades pueden orientar a las personas, conocer procedimientos para protección de datos personales, vigilar el cumplimiento de la normativa y desarrollar otras funciones previstas en la legislación aplicable en materia de protección de datos personales.

Dependiendo de su ámbito de competencia, estas autoridades pueden orientar a las personas, conocer procedimientos para la protección de sus derechos, vigilar el cumplimiento de la normativa y desarrollar otras funciones previstas en la legislación aplicable.

La autoridad competente dependerá, principalmente de quién tenga tus datos personales, una institución pública federal, una institución pública estatal o municipal, o bien, un particular.

Por ello, el primer paso es identificar quién es el responsable del tratamiento de tus datos personales.

¿En qué pueden ayudarte?

Dependiendo del caso y de sus atribuciones, las autoridades competentes pueden:

- Orientarte sobre los derechos que tienes respecto de tus datos personales;
- Explicarte cómo ejercer tus derechos de acceso, rectificación, cancelación, oposición y, cuando corresponda, portabilidad;
- Informarte sobre los procedimientos disponibles cuando consideres que tus derechos no fueron respetados;
- Conocer y resolver los medios de impugnación o procedimientos que correspondan conforme a la legislación aplicable; y
- Recibir o atender, en los casos previstos por la ley, denuncias relacionadas con posibles incumplimientos en materia de protección de datos personales.

En muchos casos, una orientación oportuna puede ayudarte a resolver el problema sin necesidad de iniciar un procedimiento más complejo.



¿Qué autoridad puede ayudarte, según el caso?

Tabla 3.4 Autoridades en materia de protección de datos personales.

Si el problema es con...	¿Quién puede ayudarte?	¿Qué puede hacer?
Una institución pública federal	Unidad de Protección de Datos Personales, la cual está adscrita a la Secretaría Anticorrupción y Buen Gobierno del Poder Ejecutivo Federal.	Orientarte sobre tus derechos y conocer y substanciar los procedimientos relacionados con el tratamiento de datos personales por autoridades federales, conforme a la legislación vigente.

Si el problema es con...	¿Quién puede ayudarte?	¿Qué puede hacer?
Una institución pública estatal o municipal de Nuevo León.	INFONL, dentro del ámbito de sus atribuciones.	Brindar orientación, evaluar, conocer y substanciar los medios de impugnación previstos por la ley y promover el cumplimiento de las obligaciones en materia de protección de datos personales por parte de las instituciones públicas estatales y municipales.
Una empresa u otro particular	Unidad de Protección de Datos Personales, la cual está adscrita a la Secretaría Anticorrupción y Buen Gobierno del Poder Ejecutivo Federal.	Orientarte, recibir los procedimientos previstos en la ley y vigilar el cumplimiento de las obligaciones de quienes tratan datos personales en el sector privado.

Antes de presentar un recurso

¿Qué puedes hacer antes de acudir a la autoridad?

Dependiendo del problema, el primer paso puede consistir en ejercer directamente tus derechos ante la institución pública, ya sea estatal o federal, así como ante alguna institución privada. Por ejemplo, si un dato es incorrecto, puedes presentar una solicitud de rectificación.

Por ello, es importante:

1. Identificar quién tiene tus datos personales;
2. Determinar qué derechos deseas ejercer;
3. Presentar la solicitud correspondiente;
4. Conservar la solicitud, respuesta y demás documentos relacionados; y
5. Verificar los plazos establecidos por la legislación competente.

Si la respuesta no resuelve la situación o no se recibe en el tiempo previsto, entonces puedes acudir ante la autoridad competente para iniciar un procedimiento para proteger tu información de carácter personal.

Un ejemplo de la vida cotidiana

María detectó que una empresa de telefonía tenía registrado un domicilio incorrecto, ya que aparecía una dirección que no correspondía con la suya. Por ello, ejerció su derecho de rectificación y solicitó que la información fuera corregida.

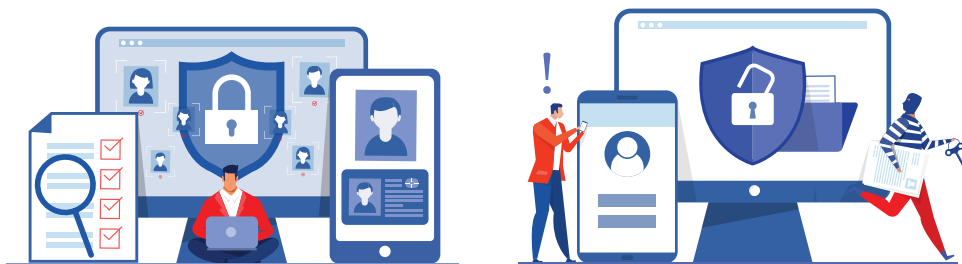
La empresa rechazó su solicitud sin explicar claramente las razones.

Ante esta situación, María buscó información sobre los mecanismos disponibles para inconformarse y acudir a la autoridad competente para recibir orientación sobre el procedimiento aplicable.

Este caso muestra la importancia de identificar primero quién tiene los datos, qué derecho se quiere ejercer y qué autoridad es competente cuando la respuesta no resulta satisfactoria.

Concepto clave. Identificar quién tiene tus datos personales es fundamental para saber que legislación aplica, ante quién debes ejercer tus derechos y qué autoridad puede intervenir si surge una inconformidad o un posible incumplimiento. Las autoridades en materia de protección de datos personales no solo resuelven controversias. También orientan a la ciudadanía, promueven el ejercicio de los derechos y vigilan que las instituciones públicas y las organizaciones privadas traten los datos personales conforme a la ley.

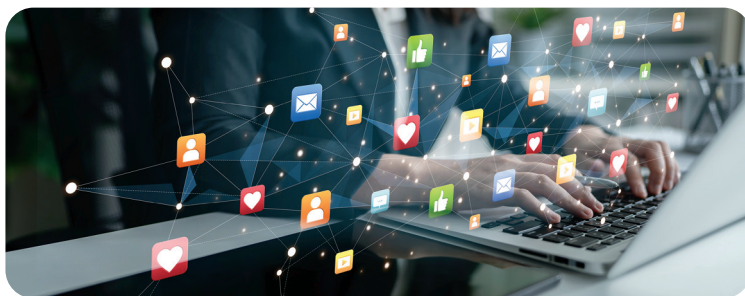
Conclusión. La protección de los datos personales no depende únicamente de las obligaciones que tienen las instituciones públicas y las empresas. También existen autoridades cuya función es orientar, proteger y garantizar el ejercicio de este derecho. Conocer a qué autoridad acudir y qué tipo de apoyo puede brindar, permite actuar con mayor seguridad cuando surge un problema relacionado con el tratamiento de los datos personales y fortalece la confianza de la ciudadanía en los mecanismos de protección previstos por la legislación.



Capítulo 4. Protege tus datos en el mundo digital

4.1 Situaciones que pueden comprometer la protección de tus datos personales

Vivimos en una época en la que gran parte de nuestras actividades se realizan por medios digitales. Consultamos información desde el teléfono celular, enviamos mensajes, realizamos compras, pagamos servicios, estudiamos, trabajamos y compartimos fotografías o videos con familiares y amistades.



Cada una de estas acciones implica el uso de datos personales. En ocasiones proporcionamos nuestro nombre, correo electrónico o número telefónico para crear una cuenta; en otras, compartimos información que puede requerir mayores precauciones por los riesgos asociados a su uso indebido, como datos financieros, documentos de identificación o información relacionada con nuestra salud.

La tecnología ha facilitado muchas actividades de la vida cotidiana; sin embargo, también ha incrementado las situaciones en las que nuestros datos personales pueden quedar expuestos si no actuamos con precaución.

En la mayoría de los casos, los riesgos no provienen de la tecnología en sí misma, sino de la manera en que utilizamos los dispositivos, las aplicaciones o los servicios digitales. Una decisión aparentemente sencilla, como compartir una fotografía de un documento oficial o aceptar los permisos de una aplicación sin leerlos, puede tener consecuencias que no siempre advertimos en ese momento.

Por ello, aunque las instituciones públicas y privadas tienen la responsabilidad de proteger los datos personales que tratan, las personas también podemos adoptar medidas preventivas para reducir algunos riesgos en nuestra vida digital, conocer las situaciones que pueden comprometer la protección de nuestros datos personales es una de las mejores herramientas para prevenir problemas y ejercer un mayor control sobre nuestra información.

Las situaciones más comunes

Muchos riesgos relacionados con los datos personales pueden presentarse durante actividades digitales cotidianas. Identificarlos permite adoptar medidas sencillas para reducirlos.

Compartir demasiada información en redes sociales. Las redes sociales permiten mantener contacto con familiares, amistades y comunidades de interés. Sin embargo, publicar información personal sin considerar quién puede acceder a ella puede revelar aspectos de nuestra vida privada. Además, una vez publicada la información puede ser copiada, descargada o compartida con otras personas, aun cuando posteriormente eliminemos la publicación, por ejemplo, compartir fotografías de identificaciones oficiales, boletos de viaje, comprobantes de domicilio o documentos escolares puede exponer datos que podrían ser utilizados de manera indebida.

Antes de publicar, pregúntate si es realmente necesario compartir esa información.

Aceptar permisos sin leerlos. Muchas aplicaciones solicitan autorización para acceder a la cámara, el micrófono, la ubicación, la lista de



contactos o la galería de fotografías. En algunos casos estos permisos son indispensables para que la aplicación funcione correctamente; en otros, no guardan relación con el servicio que ofrece. Leer qué permisos solicita una aplicación y decidir cuáles autorizar es una forma sencilla de proteger la información personal. Antes de

concederlos, revisa si guardan relación con las funciones de la aplicación. También es recomendable revisar periódicamente los permisos que ya otorgaste y retirar aquellos que dejaron de ser necesarios.

Utilizar contraseñas fáciles de adivinar o repetirlas en distintas cuentas.

Las contraseñas siguen siendo una de las principales barreras para proteger nuestras cuentas. Utilizar fechas de nacimiento, nombres de familiares o secuencias numéricas sencillas puede facilitar el acceso no autorizado a la información. Una contraseña robusta, diferente para cada cuenta importante y acompañada, cuando sea posible, de la autenticación en dos pasos (también conocida como verificación de dos pasos), incrementa significativamente la protección de los datos personales.

Conectarse a redes públicas para realizar trámites o pagos.

Las redes inalámbricas disponibles en lugares públicos son útiles para navegar por internet, pero no siempre ofrecen las mismas condiciones de seguridad que una red privada. Si se realizan operaciones bancarias, compras o trámites que implican el intercambio de datos personales, es recomendable utilizar una conexión segura o la red móvil del dispositivo.



Responder mensajes, correos o llamadas sin verificar su origen. Cada vez es más común recibir mensajes, correos electrónicos o llamadas en las que alguien solicita datos personales argumentando que existe un problema con una cuenta, un paquete pendiente de entrega o un supuesto beneficio.

Antes de proporcionar cualquier información, es importante verificar que la comunicación provenga realmente de la institución o empresa correspondiente. Las instituciones públicas y privadas (profesionistas y empresas u otros particulares) formalmente establecidas cuentan con canales oficiales para atender a las personas usuarias.

Algunas personas intentan obtener información personal haciéndose pasar por bancos, empresas, autoridades o personas conocidas. Pueden hacerlo mediante correos electrónicos (*phishing*), mensajes de texto (*smishing*) o llamadas telefónicas (*vishing*).

Estos mensajes suelen buscar que actúes rápidamente, ya que pueden advertir sobre el bloqueo de una cuenta, un cargo desconocido, un paquete pendiente o un supuesto premio.

No proporciones información ni ingreses a enlaces únicamente porque el mensaje parece auténtico. Si tienes dudas, contacta directamente a la institución utilizando sus canales oficiales.

Tabla 4.1 Situaciones cotidianas y cómo prevenirlas.

Situación	¿Qué puede ocurrir?	¿Qué puedes hacer?
Publicar fotografías de documentos oficiales en redes sociales.	Otras personas podrían conocer información que permite identificarte.	Evita compartir imágenes de documentos personales o datos sensibles.
Instalar aplicaciones sin revisar los permisos.	La aplicación podría acceder a información que no necesita para funcionar.	Lee los permisos antes de aceptarlos y descarga aplicaciones de fuentes confiables.
Utilizar la misma contraseña en varias cuentas.	Si una cuenta se ve comprometida, las demás también podrían estar en riesgo.	Utiliza contraseñas diferentes y activa la verificación en dos pasos cuando esté disponible.
Conectarte a una red Wi-Fi pública para realizar pagos o consultar información bancaria.	Tu información podría quedar más expuesta durante la conexión.	Utiliza una red privada o los datos móviles de tu teléfono.
Proporcionar datos personales por llamada, mensaje o correo sin verificar quién los solicita.	Podrías entregar información a personas que buscan obtenerla de forma indebida.	Confirma siempre la identidad de quien solicita tus datos antes de compartirlos.
Compartir códigos de verificación.	Otra persona podría intentar acceder a una de tus cuentas.	Nunca compartas códigos de acceso o verificación que recibas para autenticarte.

Un ejemplo de la vida cotidiana

Ana descargó una aplicación para editar fotografías. Durante la instalación, la aplicación solicita acceso permanente a su ubicación, a sus contactos y al micrófono.

Antes de aceptar, Ana revisó los permisos y observó que varios de ellos no eran necesarios para editar imágenes. Decidió negar aquellos que no guardaban relación con la función de la aplicación y continuar únicamente con los permisos indispensables.

Con una acción tan sencilla, protegió parte de su información personal sin dejar de utilizar la aplicación.

Concepto clave. Proteger tus datos personales en el entorno digital no significa en dejar de utilizar la tecnología, sino en conocer que información proporcionas o se genera durante su uso, tomar decisiones informadas y adoptar medidas que reduzcan los riesgos para tu privacidad y tus datos personales.

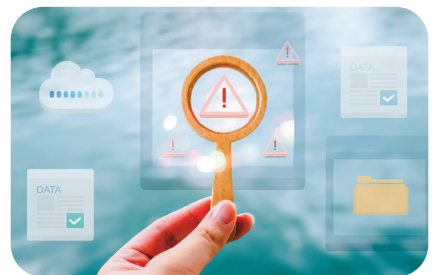
Conclusión. El uso de herramientas digitales forma parte de nuestra vida diaria y continuará creciendo en los próximos años. Por ello, aprender a identificar las situaciones que pueden comprometer nuestros datos personales es una habilidad cada vez más importante. Pequeñas acciones, como revisar los permisos de una aplicación, utilizar contraseñas seguras, evitar compartir documentos en redes sociales o verificar quién solicita nuestra información, pueden marcar una gran diferencia en la protección de nuestra privacidad. Cuidar los datos personales no requiere conocimientos especializados; requiere desarrollar hábitos responsables que permitan aprovechar los beneficios de la tecnología con mayor seguridad.

4.2 Riesgos al utilizar redes sociales e internet

Las redes sociales e internet han transformado la manera en que nos comunicamos, aprendemos, trabajamos y realizamos muchas actividades cotidianas. Hoy es posible hacer una videollamada con familiares, comprar un producto, realizar un trámite gubernamental o consultar información desde un teléfono celular en cuestión de minutos.

Sin embargo, así como estas herramientas ofrecen grandes beneficios, también pueden representar riesgos para la protección de los datos personales cuando no se utilizan con precaución.

En muchas ocasiones, la información que compartimos en internet permanece disponible durante mucho tiempo y puede llegar a personas distintas de aquellas para quienes originalmente estaba destinada. Por



ello, cada fotografía, comentario, publicación o dato que hacemos público puede contribuir a formar un perfil sobre quiénes somos, dónde vivimos, cuáles son nuestros hábitos e incluso cuáles son nuestros intereses.

Consulta el material en:



<https://infonl.mx/>

Proteger los datos personales en internet no significa dejar de utilizar las redes sociales, sino aprender a compartir únicamente la información necesaria y aprovechar las herramientas de privacidad que ofrecen las plataformas digitales.

El INFONL, a través de su Dirección de Capacitación, pone a disposición el material “Datos personales en riesgo. El costo de compartir en línea”, donde podrás conocer más sobre la importancia de proteger tus datos personales en internet y los riesgos asociados con compartir información en línea.

¿Qué información compartimos sin darnos cuenta?

Muchas veces pensamos que solo proporcionamos datos personales cuando llenamos un formulario o realizamos un trámite. Sin embargo, también compartimos información cuando:

- Publicamos fotografías o videos.
- Indicamos nuestra ubicación.
- Comentamos dónde trabajamos o estudiamos.
- Compartimos fechas importantes, como cumpleaños o aniversarios.
- Publicamos información sobre viajes o vacaciones.
- Participamos en concursos o dinámicas en redes sociales.
- Respondemos cuestionarios o encuestas en línea.

Cada uno de estos datos, por separado, puede parecer inofensivo. Sin embargo, al reunirse, permiten conocer aspectos muy específicos de nuestra vida cotidiana.



Riesgos más comunes en redes sociales e internet

Exponer más información de la necesaria. Compartir datos personales de manera pública facilita que personas desconocidas obtengan información sobre nosotros. Por ejemplo, publicar una fotografía de una credencial oficial, un comprobante de domicilio o un boleto de viaje puede revelar datos que deberían mantenerse reservados.



Aceptar solicitudes de personas desconocidas. No todas las personas que interactúan en internet son quienes dicen ser. Aceptar solicitudes de amistad o mantener comunicación con perfiles desconocidos puede facilitar el acceso a información personal, fotografías o publicaciones que estaban destinadas únicamente a familiares y amistades. Antes de aceptar una solicitud, conviene revisar si realmente conocemos a esa persona.

Compartir la ubicación en tiempo real. Informar que nos encontramos de vacaciones o que nuestra vivienda permanecerá desocupada durante varios días puede representar un riesgo para nuestra seguridad y privacidad. Si deseas compartir una experiencia de viaje, una buena práctica es hacerlo una vez que hayas regresado.

Participar en cuestionarios o juegos que solicitan información personal. En internet es frecuente encontrar cuestionarios o dinámicas que preguntan, por ejemplo, cuál fue el nombre de tu primera mascota, cómo se llamaba tu escuela primaria o cuál es tu comida favorita. Aunque parecen juegos inofensivos, algunas de estas preguntas coinciden con la información utilizada como preguntas de recuperación de cuentas o forman parte de los datos que muchas personas comparten públicamente. Antes de responder, reflexiona si realmente vale la pena proporcionar esa información.



Hacer clic en enlaces sin verificar su origen. No todos los enlaces que circulan en internet son seguros. Si recibes un mensaje con promociones, premios, supuestas actualizaciones de cuentas o solicitudes urgentes para ingresar a un sitio web, verifica primero que provenga de una fuente oficial. Cuando tengas dudas, ingresa directamente a la página oficial de la institución o empresa en lugar de utilizar el enlace recibido.

Tabla 4.2 Buenas prácticas para proteger tus datos en redes sociales e internet.

Si haces esto...	Podría ocurrir que...	Una buena práctica es...
Publicar información personal de manera pública.	Personas desconocidas pueden acceder a esa información.	Comparte únicamente lo necesario y revisa la configuración de privacidad de tus cuentas.
Aceptar solicitudes de perfiles desconocidos.	Otras personas pueden acceder a tus publicaciones y datos personales.	Acepta únicamente a personas que realmente conozcas.
Compartir tu ubicación en tiempo real.	Se puede conocer dónde te encuentras o si tu domicilio está desocupado.	Comparte esa información solo cuando sea necesario o después de regresar del lugar.
Participar en cuestionarios que solicitan datos personales.	Puedes revelar información que ayude a identificarte o a responder preguntas de seguridad.	Evita compartir información personal en juegos o dinámicas en línea.
Abrir enlaces recibidos por mensajes inesperados.	Podrías ingresar a sitios falsos o proporcionar información personal.	Verifica siempre el remitente y accede a los sitios oficiales escribiendo la dirección directamente en tu navegador.

Un ejemplo de la vida cotidiana

Luis realizó un trámite mediante una plataforma digital de una institución pública. Para pedir ayuda, publicó en redes sociales una captura de pantalla del sistema. Sin embargo, la imagen mostraba su nombre completo, número de folio y otros datos relacionados con su solicitud.

Aunque su intención era únicamente explicar el problema que estaba enfrentando, la publicación permitió que esa información quedará expuesta a cualquier persona que pudiera acceder a ella. Luis comprendió entonces la importancia de revisar las capturas de pantalla antes de compartirlas y ocultar aquellos datos que no sea necesario hacer públicos.

Concepto clave. Cada publicación, fotografía o comentario en internet puede contener datos personales. Antes de compartir información, pregúntate quién podrá verla, cuánto tiempo permanecerá disponible y si realmente es necesario hacerla pública.

Conclusión. Las redes sociales e internet forman parte de nuestra vida diaria y ofrecen múltiples beneficios para comunicarnos, aprender y acceder a servicios. Sin embargo, también requieren que actuemos con responsabilidad al compartir información personal. Adoptar hábitos sencillos, como revisar la privacidad de nuestras cuentas, aceptar únicamente contactos conocidos, evitar publicar datos sensibles y verificar el origen de los enlaces que recibimos, contribuye a reducir riesgos y fortalece la protección de nuestros datos personales. La mejor herramienta para disfrutar del entorno digital es combinar sus ventajas con un uso informado y responsable.

4.3 Buenas prácticas para proteger tu información personal

Proteger los datos personales no depende únicamente de las instituciones públicas o de las empresas que los tratan. Cada persona también desempeña un papel importante al decidir cómo comparte su información y qué medidas adopta para mantenerla segura.

En la vida diaria realizamos muchas actividades que implican el uso de datos personales, tales como crear cuentas en internet, realizar compras, utilizar aplicaciones, hacer trámites, consultar servicios de salud o efectuar operaciones bancarias. En todas ellas es posible reducir los riesgos mediante hábitos sencillos.

No se trata de dejar de utilizar la tecnología, sino de hacerlo de forma informada y responsable.

Piensa antes de compartir tus datos

Antes de proporcionar información personal, pregúntate:

- ¿Realmente necesitan este dato para brindarme el servicio?
- ¿Conozco quién está solicitando mi información?
- ¿Comprendo para qué utilizarán mis datos personales?
- ¿Existe un aviso de privacidad que explique cómo serán tratados?

Responder estas preguntas puede ayudarte a decidir si es conveniente compartir determinada información.

Utiliza contraseñas seguras



Las contraseñas son la primera barrera para proteger nuestras cuentas. Una contraseña segura debe ser difícil de adivinar y diferente para cada servicio importante.

También es recomendable activar la verificación en dos pasos, cuando esté disponible, ya que agrega una capa adicional de protección al solicitar un segundo método de verificación para acceder a la cuenta.

Mantén actualizados tus dispositivos

Los teléfonos celulares, computadoras y tabletas reciben actualizaciones que corrigen errores, incorporan mejoras y pueden solucionar vulnerabilidades de seguridad. Instalar oportunamente esas actualizaciones contribuye a mantener protegidos los dispositivos y la información que almacenan.



También es recomendable contar con herramientas de seguridad que ayuden a detectar y prevenir amenazas. En las computadoras, pueden utilizarse las funciones de protección que incorpora el propio sistema operativo o, si la persona usuaria lo consi-

dera necesario, instalar un software antivirus de una fuente confiable.

Recuerda: antes de instalar un antivirus u otro programa de seguridad, verifica que provenga del sitio oficial del proveedor y evita descargarlo desde páginas, anuncios o enlaces de procedencia desconocida.

Descarga aplicaciones únicamente de fuentes confiables

Antes de instalar una aplicación:

- Verifica quién la desarrolló.
- Revisa la calificación y los comentarios de otras personas usuarias.
- Comprueba qué permisos solicita.
- Descárgala únicamente desde las tiendas oficiales de aplicaciones.

Si una aplicación solicita permisos que no son necesarios para funcionar, analiza si realmente deseas instalarlos.



Protege tus documentos personales

Las credenciales oficiales, pasaportes, actas, comprobantes de domicilio y demás documentos contienen información que permite identificarte.

Evita compartir fotografías de estos documentos en redes sociales o enviarlas por medios no seguros, salvo cuando sea estrictamente necesario y conozcas quién las recibirá.

Asimismo, cuando ya no necesites documentos impresos que contengan datos personales, destrúyelos antes de desecharlos para evitar que sean recuperados por otras personas.

Verifica la identidad de quien solicita información

Si recibes una llamada, un mensaje o un correo electrónico en el que te solicitan datos personales, contraseñas o códigos de verificación:

- No proporciones información de inmediato.
- Verifica que la comunicación provenga realmente de la institución o empresa correspondiente.
- Utiliza los números telefónicos o sitios oficiales para confirmar la información.

Recuerda que las instituciones financieras y muchas autoridades nunca solicitan contraseñas, NIP o códigos de seguridad por teléfono, mensaje o correo electrónico.



Revisa la configuración de privacidad

La mayoría de las redes sociales y aplicaciones permiten decidir quién puede ver la información que compartimos. Dedicar unos minutos a revisar estas opciones puede ayudarte a controlar mejor quién tiene acceso a tus publicaciones, fotografías y datos personales.

Es recomendable revisar esta configuración periódicamente, ya que las plataformas pueden actualizar sus funciones o modificar algunas opciones.

Tabla 4.3 Hábitos sencillos para proteger tus datos personales.

Hábito	¿Por qué es importante?
Utilizar contraseñas diferentes para cada cuenta importante.	Reduce el riesgo de que varias cuentas se vean comprometidas si una contraseña es conocida por terceros.
Activar la verificación en dos pasos.	Agrega una medida adicional de seguridad para acceder a tus cuentas.
Leer el aviso de privacidad antes de proporcionar información personal.	Permite conocer quién utilizará tus datos y con qué finalidad.
Revisar los permisos de las aplicaciones.	Evita compartir información que no es necesaria para el funcionamiento de la aplicación.
Mantener actualizados los dispositivos.	Ayuda a corregir vulnerabilidades y mejorar la seguridad.
Verificar la identidad de quien solicita información.	Reduce el riesgo de entregar datos personales a personas que buscan obtenerlos de forma indebida.
Configurar la privacidad de las redes sociales.	Permite controlar quién puede ver tus publicaciones y datos personales.
Destruir documentos con datos personales antes de desecharlos.	Evita que otras personas recuperen información que podría utilizarse de manera indebida.

Un ejemplo de la vida cotidiana

Roberto recibió un correo electrónico en el que se le pedía actualizar los datos de su cuenta bancaria mediante un enlace. Antes de ingresar, revisó cuidadosamente el remitente y observó que la dirección no correspondía al banco.

En lugar de acceder al enlace, abrió la aplicación oficial de su institución financiera y confirmó que no existía ninguna solicitud de actualización.

Gracias a este hábito, evitó proporcionar sus datos personales en un sitio que no era auténtico.

Concepto clave. La protección de los datos personales comienza con decisiones cotidianas. Adoptar hábitos sencillos, como verificar quién solicita la información, utilizar contraseñas seguras y revisar la configuración de privacidad de nuestras cuentas, reduce significativamente los riesgos y fortalece el control sobre nuestros datos.

Conclusión. Proteger la información personal no requiere conocimientos especializados ni herramientas complejas. En la mayoría de los casos, basta con desarrollar hábitos responsables y mantener una actitud preventiva al utilizar servicios digitales. Cada vez que decidimos qué información compartir, revisamos un aviso de privacidad, verificamos la identidad de quien solicita nuestros datos o configuramos la privacidad de nuestras cuentas, estamos fortaleciendo la protección de nuestra información personal. La mejor estrategia para cuidar nuestros datos personales es combinar el uso de la tecnología con decisiones informadas y responsables.

Para recordar. Antes de compartir tus datos personales, detente un momento y pregúntate si es realmente necesario proporcionar esta información, si sabes quién la recibirá y si conoces para qué será utilizada. Hacer estas preguntas puede ayudarte a prevenir riesgos y a ejercer un mayor control sobre tu información personal.



4.4 Casos ilustrativos para aprender

A veces, la mejor forma de comprender la importancia de proteger los datos personales es observar cómo determinadas decisiones o situaciones cotidianas pueden generar riesgos para nuestros datos personales y tener consecuencias inesperadas.

Los siguientes ejemplos muestran situaciones que cualquier persona podría enfrentar al utilizar internet, las redes sociales o los servicios digitales. Su propósito es ayudar a identificar riesgos y reflexionar sobre las acciones que pueden prevenirlos.

Nota editorial: los casos presentados en este apartado son ejemplos elaborados con fines didácticos para facilitar la comprensión de los temas abordados en este capítulo.

Caso 1. La fotografía que reveló más información de la necesaria

Sofía terminó un trámite importante y, emocionada por el resultado, publicó en sus redes sociales una fotografía de su nueva credencial.

Aunque cubrió parcialmente algunos datos, la imagen permitía observar su nombre completo, una parte de la Clave Única de Registro de Población (CURP), la fotografía y el código QR del documento.

Horas después, una amistad le comentó que esa información podía facilitar que terceros conocieran más datos sobre ella o intentaran utilizarla de manera indebida.

Sofía eliminó la publicación y comprendió que no todo lo que parece inofensivo debe compartirse en internet.

¿Qué podemos aprender? Los documentos oficiales contienen datos personales en una sola imagen, no deben difundirse públicamente. Antes de publicar una fotografía, conviene revisar cuidadosamente la información que aparece en ella.

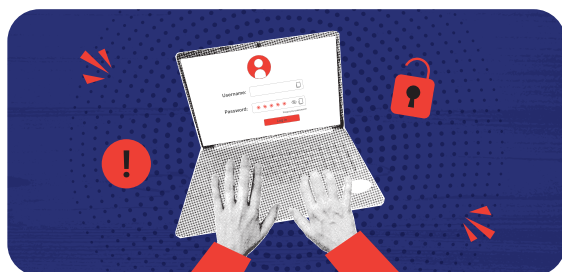
Caso 2. Una contraseña para todas las cuentas

Miguel utilizaba la misma contraseña para su correo electrónico, sus redes sociales y su banca digital porque le resultaba más fácil recordarla.

Un día perdió el acceso a una de sus cuentas. Al poco tiempo descubrió que también habían intentado ingresar a otros servicios donde utilizaba la misma contraseña.

Después de recuperar sus cuentas, decidió establecer una contraseña distinta para cada una de ellas y activar la verificación en dos pasos.

¿Qué podemos aprender? Reutilizar contraseñas incrementa el riesgo de que varias cuentas se vean comprometidas. Utilizar contraseñas diferentes fortalece la protección de la información personal.



Caso 3. Una aplicación con más permisos de los necesarios

Daniel descargó una aplicación para editar fotografías. Durante la instalación observó que la aplicación solicitaba acceso permanente a su ubicación, lista de contactos y micrófono.

Antes de aceptar, revisó para qué servía cada permiso y decidió autorizar únicamente aquellos indispensables para utilizar la aplicación.

¿Qué podemos aprender? No todas las aplicaciones necesitan acceder a toda la información del dispositivo. Revisar los permisos antes de aceptarlos ayuda a proteger los datos personales.



Caso 4. Un mensaje inesperado

Laura recibió un mensaje de texto donde le informaban que existía un problema con la entrega de un paquete y que debía ingresar a un enlace para confirmar su domicilio.

Antes de abrir el vínculo, recordó que no había realizado ninguna compra reciente.

Días después supo que otras personas habían recibido mensajes similares con el propósito de obtener información personal.

¿Qué podemos aprender? No todos los mensajes que recibimos son auténticos. Es recomendable verificar la información directamente con la empresa o institución correspondiente.



Lo más importante de estos ejemplos

Aunque las situaciones son diferentes, todas tienen algo en común, ya que las personas actuaron en un entorno cotidiano y utilizaron herramientas digitales que forman parte de su vida diaria. La diferencia estuvo en las decisiones que tomaron antes de compartir información.

En muchas ocasiones, detenerse unos segundos para analizar una situación puede evitar problemas relacionados con la protección de los datos personales.

Concepto clave. La mayoría de los riesgos relacionados con los datos personales pueden prevenirse cuando aprendemos a reconocer las situaciones que los generan y actuamos con precaución antes de compartir información, conceder permisos o responder a solicitudes inesperadas.

Conclusión. Cada experiencia representa una oportunidad para fortalecer nuestros hábitos de protección de datos personales. No es necesario esperar a enfrentar un problema para adoptar medidas de prevención. Revisar la información que compartimos, verificar quién la solicita y utilizar responsablemente las herramientas digitales son acciones sencillas que contribuyen a proteger nuestra privacidad y a ejercer un mayor control sobre nuestros datos personales.

Sin embargo, la protección de los datos personales no depende únicamente de las decisiones de las personas usuarias. Las instituciones, empresas y demás responsables también deben cumplir con las obligaciones de seguridad y tratamiento adecuado que establece la legislación aplicable.



BLOQUE II.

GUÍA DE SUPERVIVENCIA: CASOS PRÁCTICOS

Capítulo 5. Tus datos personales en la vida cotidiana

5.1 Tus datos personales al realizar trámites y servicios públicos

Al realizar trámites o solicitar servicios públicos, es necesario proporcionar determinados datos personales para que las instituciones puedan llevar a cabo sus funciones. La información que se solicita puede variar según el trámite, el servicio y la finalidad para la que será utilizada.

Esto no significa que nuestros datos puedan utilizarse de cualquier manera. Las instituciones públicas necesitan determinada información para cumplir con sus funciones, como para identificar correctamente a una persona, integrar un expediente, entregar un documento o prestar un servicio. Sin embargo, el hecho de que una institución tenga nuestros datos personales también implica una responsabilidad, es decir, debe protegerlos y utilizarlos para las finalidades que correspondan.

La legislación mexicana vigente de protección de datos personales establece reglas para el tratamiento de los datos personales que se encuentran en posesión de las instituciones públicas, así como bases para proteger esta información y garantizar los derechos de las personas.



¿Qué datos pueden pedirte?

Dependiendo del trámite o servicio, una institución pública puede necesitar diferentes tipos de información.

Tabla 5.1 Datos que pueden solicitarse según el trámite.

Trámite o servicio	Algunos datos que pueden solicitarse
Obtener un documento oficial	Nombre, fecha de nacimiento, CURP y otros datos necesarios para identificarte.
Solicitar atención médica	Nombre, fecha de nacimiento, datos de contacto e información relacionada con tu estado de salud.
Tramitar una licencia para conducir	Datos de identificación, fotografía, firma y, según corresponda, información relacionada con el trámite.
Realizar un trámite fiscal	Nombre, RFC, domicilio y demás información necesaria para cumplir con las obligaciones correspondientes.
Solicitar un apoyo o programa público	Datos de identificación, domicilio y, dependiendo del programa, información que permita determinar si cumples con los requisitos.

Los datos que pueden solicitarte dependen del trámite. No todas las instituciones necesitan la misma información ni pueden pedirla sin una razón relacionada con sus funciones.

¿Por qué una institución pública necesita mis datos?

En términos sencillos, una institución pública solicita datos personales porque necesita identificarte, realizar un trámite, prestarte un servicio o cumplir alguna función que tiene encomendada. Por ejemplo, si acudes a una institución para solicitar un documento a tu nombre, necesita saber quién eres y contar con información suficiente para evitar errores o confusiones.

Lo importante es entender que entregar tus datos para realizar un trámite no significa perder el control sobre ellos. Las instituciones públicas tienen obligaciones respecto de la información que reciben y deben adoptar medidas para protegerla.



¿Qué puedes hacer antes de entregar tus datos?

No es necesario desconfiar de todos los trámites públicos. Sin embargo, sí es recomendable mantener una actitud informada. Antes de proporcionar información personal, puedes:

1. **Preguntar por qué necesitan el dato.** Si no entiendes por qué te solicitan determinada información, pregunta cuál es su finalidad.
2. **Revisar el aviso de privacidad.** Las instituciones públicas deben informar a las personas sobre el tratamiento que darán a sus datos personales.
3. **Entregar la información por los medios oficiales.** Cuando realices un trámite por internet, asegúrate de estar utilizando el sitio oficial de la institución.
4. **Evitar entregar información adicional que no sea necesaria.** Si un trámite requiere determinados datos, proporciona los que correspondan y evita compartir información personal por canales informales.
5. **Conservar tus comprobantes.** Guarda solicitudes, acuses, folios o documentos relacionados con el trámite. Pueden ser útiles si posteriormente necesitas aclarar alguna situación.

¿Y qué pasa con los documentos que entregas?

En muchos trámites públicos se solicitan copias de documentos que contienen información personal, como identificación oficial, comprobante de domicilio, CURP, actas, certificados, entre otros. Antes de entregar una copia, verifica que:

- El trámite sea auténtico.
- La institución sea la responsable del servicio.
- El documento solicitado corresponda al trámite.
- Estés entregándolo por un medio oficial.

Si realizas el trámite de manera digital, evita enviar documentos personales a correos electrónicos o números de mensajería que no hayas podido verificar.



Un ejemplo de la vida cotidiana

Imagina que una persona acude a una oficina pública para realizar un trámite. Le solicitan una identificación oficial y un comprobante de domicilio. La persona entrega los documentos porque son necesarios para continuar con el procedimiento.

Hasta aquí, todo parece normal. Sin embargo, después recibe un mensaje de una persona que afirma trabajar en esa oficina y le solicita que envíe por WhatsApp una fotografía de su tarjeta bancaria “para completar el trámite”. Aquí existe una señal de alerta.

Una cosa es entregar los documentos solicitados mediante los canales oficiales y otra muy distinta proporcionar información adicional a una persona cuya identidad y función no han sido verificadas. La lección es sencilla, el hecho de que una persona tenga acceso a un trámite público no significa que pueda solicitarte cualquier dato personal.



¿Qué pasa con tus datos después del trámite?

Esta es una pregunta que pocas veces nos hacemos. Cuando entregamos información personal, podemos pensar únicamente en el momento en que realizamos el trámite. Sin embargo, los datos pueden formar parte de expedientes, sistemas o registros institucionales.



Por eso, las instituciones públicas tienen la responsabilidad de establecer medidas para proteger la información que se encuentra bajo su resguardo. La protección no termina cuando concluye el trámite.

Tabla 5.2 Antes de entregar tus datos personales.

Pregúntate	¿Por qué hacerlo?
¿Quién me está solicitando la información?	Para confirmar que se trata de una institución pública legítima.
¿Para qué necesitan mis datos?	Para comprender la finalidad del tratamiento.
¿Dónde puedo consultar el aviso de privacidad?	Para conocer cómo serán tratados tus datos.
¿Estoy utilizando un canal oficial?	Para evitar enviar información a personas o sitios que no corresponden a la institución.
¿Estoy proporcionando únicamente la información necesaria?	Para evitar compartir datos personales que no sean necesarios para el trámite.

Tus datos también tienen derechos

Una de las ideas que debemos conservar a lo largo de esta obra es que tus datos personales no dejan de ser tuyos porque los hayas proporcionado a una institución pública. En Nuevo León la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Nuevo León reconoce derechos que permiten a las personas tener mayor control sobre su información personal.

Por eso, si tienes dudas sobre el tratamiento de tus datos, si encuentras un error en tu información o consideras que una institución no los está protegiendo adecuadamente, existen mecanismos para ejercer tus derechos y, cuando corresponda, acudir ante las autoridades competentes. Estos derechos serán explicados con mayor detalle en los capítulos posteriores de esta obra.

Concepto clave. Cuando realizas un trámite público, proporcionar tus datos personales puede ser necesario. Pero la institución que los recibe tiene la responsabilidad de protegerlos y utilizarlos de acuerdo con las reglas aplicables.

Para recordar. Antes de entregar tus datos personales en un trámite público, identifica quién los solicita, pregunta para qué los necesitan, revisa el aviso de privacidad, utiliza canales oficiales, comparte únicamente la información necesaria y conserva tus comprobantes. Son acciones sencillas, pero ayudan a mantener un mayor control sobre nuestra información personal.

5.2 La protección de tus datos en escuelas y servicios de salud

Las escuelas y los servicios de salud forman parte de nuestra vida cotidiana. En ambos espacios es necesario proporcionar información personal para recibir un servicio, pero la cantidad y el tipo de datos que se solicitan pueden ser muy distintos.

Una escuela puede necesitar conocer el nombre, domicilio, teléfono, fecha de nacimiento o información de contacto de una persona estudiante y de sus familiares. En determinadas situaciones también puede tratar información sobre su salud, desempeño académico, situación familiar o necesidades específicas.



En un hospital o centro de salud, además de los datos que permiten identificar al paciente, se recopila información relacionada con su estado de salud, antecedentes médicos, estudios, tratamientos y medicamentos.

Esta información merece especial cuidado. No todos los datos personales tienen el mismo nivel de sensibilidad, y los relacionados con la salud requieren medidas de protección particularmente cuidadosas.

En las escuelas y la información que pueden tener de ti

Para prestar servicios educativos, las escuelas necesitan contar con determinada información de sus estudiantes y, en algunos casos, de sus madres, padres o tutores. Entre los datos que pueden formar parte de un expediente escolar se encuentran los siguientes.

Tabla 5.3 Datos personales en un expediente escolar.

Tipo de información	Ejemplos
Identificación	Nombre, fecha de nacimiento, CURP y fotografía.
Contacto	Domicilio, teléfono y correo electrónico.
Información familiar	Nombre y datos de contacto de madres, padres o tutores.
Académica	Calificaciones, evaluaciones, asistencia y trayectoria escolar.
Salud	Información necesaria para atender determinadas situaciones de salud o emergencias.
Imagen y voz	Fotografías, videos o grabaciones realizadas en actividades escolares, cuando corresponda.

No significa que todas las escuelas recopilen todos estos datos. La información que se solicite debe estar relacionada con las actividades y servicios que presta la institución.

¿Qué debes cuidar como estudiante o como madre, padre o tutor?

También debemos tener cuidado con la información que compartimos dentro y fuera de la escuela. Por ejemplo, publicar en redes sociales una fotografía de un grupo escolar puede revelar los nombres, rostros, uniforme, escuela a la que asisten o incluso la ubicación de niñas, niños y adolescentes.

Por ello, antes de publicar fotografías de actividades escolares, es recomendable pensar si realmente es necesario hacerlas públicas y quién podrá verlas. Cuando se trata de niñas, niños y adolescentes, la protección debe ser especialmente cuidadosa, pues se encuentran en una etapa de desarrollo que requiere mayor protección de sus derechos.





En los servicios de salud

La información relacionada con nuestra salud puede revelar aspectos muy personales de nuestra vida. Cuando acudimos a una consulta médica, un hospital, un laboratorio o una farmacia, podemos proporcionar información como:

- Nombre y fecha de nacimiento
- Datos de contacto
- Antecedentes médicos
- Enfermedades o padecimientos
- Resultados de estudios
- Tratamientos y medicamentos
- Información genética, cuando corresponda

Estos datos deben manejarse con especial cuidado y utilizarse para las finalidades relacionadas con la atención y los servicios correspondientes.

¿Por qué debemos cuidar especialmente los datos de salud?

Imagina que una persona comparte públicamente una fotografía de su expediente médico. En una sola imagen podrían aparecer su nombre, diagnóstico, resultados de estudios, medicamentos y otros datos personales. Esa información podría revelar aspectos de su vida que no desea hacer públicos. Por eso, un expediente médico no es simplemente un documento, contiene información personal que merece protección.

Un ejemplo de la vida cotidiana

Mariana llevó a su hijo a una consulta médica en una institución de salud. Después de la consulta, recibió por mensaje una copia digital de los resultados de unos estudios.

Mariana quería pedir una segunda opinión y pensó en publicar los resultados en un grupo de redes sociales. Antes de hacerlo, revisó el documento y se dio cuenta de que aparecían el nombre completo de su hijo, su fecha de nacimiento y otros datos personales.

Decidió no publicar el documento completo. En su lugar, consultó directamente con el médico y, si fuera necesario compartir determinada información, procuraría eliminar los datos que permitieran identificar al menor.



¿Qué podemos aprender? No siempre es necesario publicar un documento completo para obtener ayuda. Antes de compartir información médica, conviene preguntarnos quién necesita verla y qué datos realmente necesita conocer.

¿Qué ocurre cuando una escuela o un servicio de salud comparte información?

En determinadas circunstancias puede ser necesario comunicar información a otras personas o instituciones para prestar adecuadamente un servicio, atender una emergencia o cumplir una obligación. Sin embargo, esto no significa que los datos puedan compartirse sin límites.

La institución debe respetar las reglas aplicables al tratamiento de datos personales y adoptar medidas para evitar que la información llegue a personas que no necesitan conocerla. Por ejemplo, si una institución educativa necesita informar a una persona autorizada sobre una situación relacionada con un estudiante, debe hacerlo utilizando mecanismos adecuados y evitando divulgar información innecesaria. De igual manera, en los servicios de salud, el acceso a la información médica debe realizarse de acuerdo con las reglas aplicables y respetando la privacidad del paciente.

Tabla 5.4 ¿Cómo proteger tus datos en escuelas y servicios de salud?

Situación	Recomendación
Te solicitan información para inscribirte en una escuela.	Pregunta qué datos necesitan y revisa el aviso de privacidad.
La escuela toma fotografías durante una actividad.	Pregunta cómo serán utilizadas y dónde podrían publicarse.
Recibes documentos escolares por medios digitales.	Evita reenviarlos a personas que no necesitan conocer su contenido.
Recibes resultados de estudios médicos.	No los publiques completos en redes sociales; revisa primero qué información contienen.
Una persona te solicita información médica de otra persona.	No la compartas sin verificar que tenga autorización o que exista una razón válida para hacerlo.
Utilizas una aplicación o plataforma escolar o médica.	Revisa qué información solicita y utiliza únicamente aplicaciones y sitios oficiales.

Una regla sencilla



Cuando se trate de información escolar o de salud, podemos utilizar una regla muy sencilla (compartir la información únicamente con quien realmente la necesita y por el medio adecuado). No se trata de ocultar información que una escuela, médico u hospital necesita para cumplir con su función; se trata de evitar que esa información circule sin necesidad.

Algo especialmente importante para niñas, niños y adolescentes

Cuando los datos pertenecen a niñas, niños o adolescentes, debemos ser todavía más cuidadosos. La información sobre su escuela, domicilio, fotografías, actividades, estado de salud o ubicación puede revelar aspectos importantes de su vida.

Madres, padres, tutores, escuelas, instituciones de salud y demás personas que intervienen en su atención deben procurar que esta información sea tratada de manera responsable y respetuosa de sus derechos. La protección comienza también con algo muy sencillo, pensar antes de publicar.

Concepto clave. Las escuelas y los servicios de salud necesitan determinados datos personales para cumplir con sus funciones, pero eso no significa que puedan utilizar o compartir toda la información sin límites. Los datos deben recibir el cuidado que corresponde a su naturaleza y finalidad.

Para recordar. Antes de entregar o compartir información escolar o de salud, debes preguntar para qué necesitan los datos, revisar el aviso de privacidad, cuidar especialmente la información de salud, evitar publicar documentos completos en redes sociales, proteger la información de niñas, niños y adolescentes, y compartir únicamente lo necesario y con las personas adecuadas.





5.3 Tus datos personales en instituciones financieras

Abrir una cuenta bancaria, solicitar un crédito, contratar un seguro, realizar una transferencia o utilizar una aplicación financiera son actividades que requieren el tratamiento de datos personales.

Para prestar estos servicios, las instituciones financieras pueden necesitar conocer la identidad de sus clientes, mantener medios de contacto, verificar determinada información, evaluar solicitudes, ejecutar operaciones y cumplir las obligaciones jurídicas que les resulten aplicables.

Esto puede implicar el tratamiento de información como nombre, domicilio, teléfono, correo, entre otros datos personales.



Tabla 5.5 Información que puede solicitar una institución financiera.

Servicio	Información que puede ser necesaria
Abrir una cuenta	Datos de identificación, domicilio y datos de contacto.
Solicitar una tarjeta	Datos de identificación, información de contacto y aquella necesaria para evaluar y formalizar el servicio.
Solicitar un crédito	Datos de identificación, información financiera y aquella necesaria para determinar las condiciones del crédito.
Contratar un seguro	Datos de identificación y la información necesaria para contratar y administrar el seguro.
Realizar operaciones bancarias	Información relacionada con la cuenta, tarjeta u operación correspondiente.
Utilizar una aplicación financiera	Datos necesarios para identificarte, autenticarte y proporcionarte el servicio.

Fuente: elaboración propia con fines ilustrativos. Los datos efectivamente tratados dependerán del servicio, de la institución financiera y de las disposiciones jurídicas que resulten aplicables. Que una institución financiera solicite información no significa que pueda pedir cualquier dato sin relación con el servicio.

El hecho de que determinada información pueda resultar útil para una institución financiera no significa que pueda solicitarse sin justificación; al igual que en otros tratamientos, debe existir una finalidad que explique por qué se recaban determinados datos.



Tus datos y tu dinero están relacionados

Cuando una persona comparte información financiera, no solamente está proporcionando datos personales. En muchos casos, también está proporcionando información que puede permitir conocer aspectos de su situación económica. Por ejemplo, una cuenta bancaria puede mostrar cuánto dinero recibe una persona, con qué frecuencia realiza determinadas operaciones, dónde realiza compras, qué servicios utiliza y a quién realiza transferencias.

Por ello, esta información debe manejarse con especial cuidado. Una fotografía de una tarjeta bancaria, por ejemplo, puede contener información que nunca debería publicarse en redes sociales o enviarse a personas desconocidas.



Nunca compartas tus datos confidenciales

Uno de los principales hábitos para proteger nuestra información financiera es no compartir contraseñas, NIP, códigos de seguridad o códigos de verificación con otras personas.

Si recibes una llamada o mensaje en el que alguien afirma trabajar para tu banco y te solicita esta información, detente, aunque la persona conozca tu nombre o algunos datos tuyos, eso no demuestra que realmente pertenezca a la institución. La CONDUSEF ha alertado sobre comunicaciones falsas que utilizan el nombre de instituciones financieras para obtener datos como contraseñas, NIP, números de cuenta o información de tarjetas.

Cuidado con las instituciones financieras falsas

Este riesgo merece especial atención. En abril de 2026, la CONDUSEF informó que diez instituciones financieras habían sido suplantadas (CONDUSEF, 2026). En estos casos, personas o empresas utilizan indebidamente el nombre, logotipo o denominación de una institución financiera para engañar a quienes buscan obtener un crédito u otro servicio.

Por ejemplo, alguien puede contactarte por internet y ofrecerte un crédito inmediato a cambio de tu identificación y un depósito para “comenzar el trámite”. Antes de entregar documentos o realizar un pago, verifica que la institución exista y que se encuentre registrada. La CONDUSEF cuenta con el Sistema de Registro de Prestadores de Servicios Financieros (SIPRES), que permite consultar información sobre instituciones financieras registradas.

Las solicitudes de acceso a tu teléfono como señal de alerta

No todas las solicitudes de información tienen la misma justificación. La CONDUSEF ha advertido sobre entidades que condicionan créditos o tarjetas a que las personas permitan el acceso a información de sus dispositivos, como la lista de contactos, fotografías, cámara, micrófono, redes sociales o información íntima, y ha señalado que este tipo de información puede no tener relación con el servicio financiero solicitado.

Por eso, antes de aceptar los permisos de una aplicación financiera, revisa qué información solicita y para qué la necesita. Si una solicitud te parece excesiva o no guarda relación con el servicio que estás contratando, pregunta antes de aceptar.



¿Qué puedes hacer para proteger tus datos financieros?

Algunas medidas son muy sencillas:

1. **No compartas tus contraseñas.** Tus contraseñas son personales; no las compartas por teléfono, mensajes, correo electrónico o redes sociales.
2. **Nunca proporciones códigos de verificación.** Si recibes un código para confirmar una operación o ingresar a una cuenta, no lo compartas con otra persona.
3. **Revisa tus movimientos.** Consultar periódicamente tus cuentas permite detectar operaciones que no reconozcas y actuar oportunamente.
4. **Utiliza únicamente aplicaciones y sitios oficiales.** Evita ingresar información financiera desde enlaces que recibas en mensajes inesperados.
5. **Revisa el aviso de privacidad.** Antes de contratar un servicio, conoce qué información recopilará la institución y para qué será utilizada.
6. **Verifica la institución.** Si vas a contratar un crédito, especialmente si te contactaron por internet o redes sociales, verifica que la institución financiera sea auténtica y esté registrada.

Tabla 5.6 Antes de proporcionar información financiera.

Si te solicitan...	Antes de hacerlo...
Una fotografía de tu identificación	Verifica quién la solicita y para qué trámite la necesita.
Datos de tu tarjeta	Confirma que estás utilizando un canal oficial.
Tu contraseña	No la compartas.
Un NIP	No lo proporciones a terceros.
Un código recibido por mensaje	No lo compartas y verifica qué operación estás autorizando.
Acceso a tus contactos, fotografías o micrófono	Revisa si realmente es necesario para el servicio.
Un depósito para otorgarte un crédito	Verifica primero que la institución sea legítima y esté registrada.



Un ejemplo de la vida cotidiana

Jorge encontró en redes sociales un anuncio que ofrecía créditos personales “sin revisar historial y con autorización inmediata”. Una persona se comunicó con él y le pidió una fotografía de su identificación, acceso a sus contactos y un depósito para “activar” el crédito.

Jorge estuvo a punto de proporcionar la información, pero decidió verificar primero la institución. Al consultar los registros correspondientes descubrió que la empresa que lo había contactado no correspondía a la institución financiera que decía representar. Decidió no continuar con el trámite.

¿Qué podemos aprender? Una oferta atractiva no necesariamente es una oferta segura. Cuando se trata de dinero y datos personales, verificar antes de proporcionar información puede evitar pérdidas económicas y problemas relacionados con nuestra identidad.

¿A quién acudir si tienes un problema?

Si tienes un problema relacionado con un servicio financiero, como un crédito, una tarjeta, una cuenta o una institución financiera, puedes acudir a la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (CONDUSEF), que brinda asesoría y atención a las personas usuarias de servicios financieros. Actualmente cuenta con unidades de atención en distintas partes del país y servicios a distancia.

Es importante distinguir, sin embargo, si el problema es con una autoridad financiera relacionado específicamente con la protección de datos personales. La autoridad competente dependerá de la naturaleza del asunto y del tipo de institución involucrada. Esta distinción será explicada con mayor detalle en los capítulos dedicados al ejercicio de los derechos y a las autoridades que pueden ayudarte.

Concepto clave. Tus datos financieros pueden decir mucho sobre ti y, en algunos casos, permitir el acceso a tu patrimonio. Por eso, protegerlos es también una forma de proteger tu identidad y tu dinero.

Para recordar. Antes de proporcionar información a una institución financiera, verifica quién te está contactando, revisa el aviso de privacidad, utiliza canales oficiales, no compartas contraseñas, NIP ni códigos de seguridad, desconfía de créditos demasiado fáciles o solicitudes inesperadas, y consulta a la CONDUSEF cuando tengas dudas sobre una institución financiera.

5.4 Lo que compartes al utilizar aplicaciones móviles

Hoy utilizamos aplicaciones móviles prácticamente para todo, comunicarnos, pedir comida, trasladarnos, comprar, estudiar, realizar operaciones bancarias, consultar información, hacer ejercicio o simplemente entretenernos. Para funcionar, algunas de estas aplicaciones necesitan acceder a determinados datos o funciones del teléfono, pero eso no significa que debamos compartir toda nuestra información sin revisar antes para qué será utilizada.

Cada vez que instalas una aplicación, creas una cuenta o utilizas alguno de sus servicios, puedes proporcionar información como tu nombre, número telefónico, correo electrónico, fotografías, ubicación o datos relacionados con la actividad que realizas dentro de la aplicación. También puedes autorizar el acceso a determinadas funciones de tu teléfono, como la cámara, el micrófono, los contactos, los archivos o la ubicación. Por eso, antes de aceptar, conviene preguntarse qué estás compartiendo y por qué.

Cinco recomendaciones para usar aplicaciones con mayor seguridad



Una aplicación no necesita saber todo sobre ti para funcionar.

Comparte únicamente la información que tenga una relación razonable con el servicio que estás utilizando. En particular, conviene:

- Revisar los permisos antes de aceptarlos y volver a revisarlos periódicamente.
- Descargar aplicaciones desde tiendas y sitios oficiales.
- Mantener actualizado el sistema operativo y las aplicaciones.
- Evitar introducir información sensible en aplicaciones que no necesiten o cuya legitimidad no puedas verificar.
- Eliminar las aplicaciones que dejen de ser útiles y revisar los permisos que tenían concedidos.

¿Qué información puedes estar compartiendo?

Dependiendo de la aplicación y del servicio que ofrece, pueden solicitarse diferentes tipos de datos personales, por ejemplo:

- **Datos de identificación:** nombre, edad o fecha de nacimiento.
- **Datos de contacto:** número telefónico y correo electrónico.
- **Ubicación:** dónde te encuentras o los lugares que visitas.
- **Fotografías y videos:** cuando permites el acceso a la cámara o a tus archivos.
- **Información de contactos:** cuando autorizas el acceso a la agenda de tu teléfono.
- **Información sobre tus actividades:** búsquedas, compras, preferencias o servicios que utilizas.
- **Datos relacionados con el dispositivo:** información técnica que permite identificar o reconocer el dispositivo utilizado.

No todas las aplicaciones necesitan los mismos datos. Lo importante es que exista una relación razonable entre la información que solicita la aplicación y el servicio que quieres utilizar.

Los permisos también son importantes

Cuando una aplicación pregunta si puede acceder a tu ubicación, a la cámara o al micrófono, no se trata simplemente de presionar “aceptar” para continuar. Detente un momento y piensa si la aplicación realmente necesita ese permiso para hacer lo que quieres.

Por ejemplo, una aplicación de mapas puede necesitar conocer tu ubicación para indicar una ruta, y una aplicación para realizar videollamadas puede necesitar la cámara y el micrófono. Pero si una aplicación que solamente utilizas para consultar información solicita acceso a tus contactos, fotografías y ubicación permanente, es razonable preguntarse si todos esos permisos son necesarios.



Antes de aceptar, revisa el aviso de privacidad

El aviso de privacidad es una herramienta importante para conocer qué sucede con tus datos personales. La legislación federal vigente de protección de datos personales lo define como el documento que debe ponerse a disposición de la persona titular para informarle sobre los propósitos del tratamiento de sus datos personales.

Por eso, antes de registrarse o proporcionar información, procura revisar quién está recopilando tus datos, qué datos personales solicita, para qué los va a utilizar, con quién puede compartirlos, cómo puedes ejercer tus derechos y dónde puedes consultar el aviso de privacidad completo. No siempre será necesario leer documentos extensos de principio a fin; lo importante es identificar la información esencial antes de entregar tus datos.

Cinco preguntas antes de dar permiso

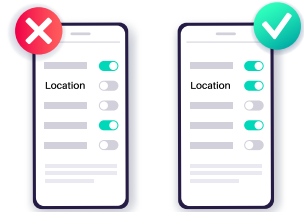
Antes de aceptar una solicitud de una aplicación, puedes hacerte estas cinco preguntas:

1. **¿Qué información me están solicitando?** Identifica si se trata de tu ubicación, fotografías, contactos, teléfono, correo electrónico u otro dato.
2. **¿Para qué la necesitan?** Busca una explicación clara sobre la finalidad.
3. **¿Es necesario para utilizar el servicio?** No todos los permisos son indispensables para todas las funciones.
4. **¿Puedo utilizar la aplicación sin proporcionar ese dato?** En algunos casos puedes negar un permiso y continuar utilizando determinadas funciones.
5. **¿Sé quién tendrá mis datos y qué puedo hacer si tengo un problema?** Identificar al responsable te permitirá saber dónde acudir si posteriormente necesitas ejercer algún derecho.



Un ejemplo de la vida cotidiana

Imagina que descargas una aplicación para consultar el clima. La aplicación solicita tu ubicación para mostrarte el pronóstico correspondiente al lugar donde te encuentras; esa solicitud puede tener una relación directa con el servicio que quieres utilizar. Pero además te solicita acceso a tus contactos, fotografías y micrófono.



En ese momento puedes preguntarte para qué necesita una aplicación del clima tus contactos o tu micrófono. Si no encuentras una razón relacionada con el servicio, puedes revisar los permisos y decidir cuáles deseas autorizar. Este pequeño ejercicio puede ayudarte a evitar que compartas información que no necesitas proporcionar.

¿Qué pasa cuando utilizas una aplicación de una institución pública?

Si utilizas una aplicación desarrollada u operada por una institución pública del Estado de Nuevo León y, mediante ella, se recaban tus datos personales, dicha institución debe observar el marco jurídico aplicable a los sujetos obligados en materia de protección de datos personales.

Antes de recabar tus datos personales, la institución debe poner a tu disposición el aviso de privacidad, en el que se informa, entre otros aspectos, qué datos serán recabados, para qué finalidades serán utilizados, y cuáles son las condiciones aplicables para su tratamiento. De esta manera, puedes conocer cómo será tratada tu información antes de proporcionarla.



Esto es particularmente importante cuando utilizas aplicaciones para realizar trámites o recibir servicios públicos, ya que pueden involucrar datos de identificación, domicilio, situación laboral, datos patrimoniales o, en determinados casos, datos personales sensibles.

No se trata de dejar de utilizar las aplicaciones

La protección de datos personales no significa tener miedo a la tecnología ni dejar de utilizar las aplicaciones; significa aprender a utilizarlas con mayor cuidado. Antes de compartir información, detente, revisa, pregunta y

decide. No todos los datos tienen el mismo valor ni todos los permisos son necesarios. Compartir únicamente la información que sea necesaria para utilizar un servicio puede ayudarte a mantener un mayor control sobre tus datos personales.

Para recordar. Una aplicación puede pedir muchos permisos, pero antes de aceptarlos pregúntate si realmente los necesita. Tus datos personales son tuyos y tienes derecho a saber para qué se utilizan.

5.5 ¿Cómo identificar cuándo te solicitan más datos de los necesarios?

En nuestra vida diaria es común que una institución, empresa, escuela, servicio médico, aplicación o establecimiento nos solicite información personal. Algunas veces se trata de datos indispensables para recibir un servicio; otras, pueden pedirnos información adicional que no parece tener relación clara con lo que estamos realizando.

Esto puede generar una pregunta muy sencilla, relacionada con si realmente necesitan todos estos datos para hacer el trámite o prestarme el servicio. No siempre es fácil saberlo. Por eso, una buena práctica es detenernos unos momentos antes de proporcionar información y tratar de entender qué dato nos están solicitando, para qué lo necesitan y qué relación tiene con el servicio que queremos recibir.

La protección de los datos personales parte, entre otros aspectos, de que la información debe utilizarse para una finalidad determinada y que no deben solicitarse datos que no sean necesarios para cumplirla. En el ámbito de los sujetos obligados, la legislación nacional de protección de datos personales establece que deben tratarse únicamente los datos adecuados, relevantes y estrictamente necesarios para la finalidad que justifica su tratamiento. En Nuevo León, la legislación estatal de protección de datos personales establece las bases para la protección de los datos personales que se encuentran en poder de los sujetos obligados estatales y municipales.

Una pregunta que puede ayudarte

Antes de entregar un dato personal, piensa qué tiene que ver ese dato con lo que estás solicitando. Por ejemplo, si vas a realizar un trámite para obtener un documento, es razonable que te soliciten información para identificarte.

Pero si además te piden información que aparentemente no tiene relación con el trámite, puedes preguntar para qué la necesitan. No significa que la solicitud sea necesariamente incorrecta, simplemente tienes derecho a comprender por qué se solicita determinada información.

Cinco señales para estar atento

No existe una lista que permita afirmar automáticamente que una solicitud es indebida. Sin embargo, hay situaciones que deberían llevarte a preguntar antes de proporcionar información.

Tabla 5.7 Señales para estar atento antes de compartir un dato personal.

Señal	¿Qué puedes hacer?
Te solicitan información que no parece relacionada con el trámite.	Pregunta para qué la necesitan.
No te explican qué harán con tus datos.	Solicita información sobre el aviso de privacidad.
Te piden datos muy personales para un servicio sencillo.	Pregunta si son indispensables y cuál es su finalidad.
Te solicitan documentos adicionales sin explicar por qué.	Pregunta cuál es la razón de la solicitud.
Te piden enviar información por un medio que no reconoces como oficial.	Verifica primero que el canal sea legítimo.

Fuente: Elaboración propia con base en los principios y deberes establecidos en la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Nuevo León, (2019).

No todos los datos tienen la misma importancia

Una de las ideas que queremos que el lector conserve de este libro es que un dato personal puede parecer pequeño, pero al combinarse con otros puede revelar mucho sobre una persona. Por ejemplo, el nombre, el teléfono, el domicilio y la fecha de nacimiento, juntos, pueden proporcionar mucha más información que cualquiera de esos datos por separado. Por eso, no



debemos pensar únicamente “no pasa nada, solo me están pidiendo mi teléfono”; es mejor preguntarnos por qué necesitan ese dato y para qué lo van a utilizar.

Un ejemplo de la vida cotidiana

Cuando realizas una compra de un producto en una tienda y, para elaborar el comprobante de compra, te solicitan determinados datos. Hasta ahí puede existir una razón relacionada con la operación. Pero después te preguntan cuál es tu fecha de nacimiento, dónde trabajas, cuántas personas viven contigo, cuál es tu ingreso mensual y qué otros productos utilizas.

En ese momento es razonable preguntar si todos esos datos son necesarios para realizar tu compra. Algunos podrían tener una finalidad determinada, por ejemplo, para un programa de beneficios o para ofrecerte algún servicio adicional; pero si ese fuera el caso, la persona debe poder conocer para qué se utilizarán sus datos y qué está aceptando.

El aviso de privacidad puede darte la respuesta

Una de las herramientas más importantes para saber qué sucederá con nuestros datos es el aviso de privacidad. No es necesario leerlo como si fuera un documento jurídico complicado; para efectos prácticos, basta con buscar tres cosas, las cuales son quién tendrá tus datos (identifica a la persona, empresa, institución o autoridad responsable), qué datos van a utilizar (observa qué información personal será recopilada) y para qué la van a utilizar, que es una de las preguntas más importantes.

La Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Nuevo León establece que, antes del tratamiento de sus datos personales, la persona titular debe conocer las características principales de ese tratamiento, a fin de que pueda tomar decisiones informadas sobre el uso de su información.

Para ello, el responsable debe poner a su disposición un aviso de privacidad, cuyo propósito es informar sobre los alcances y condiciones generales del tratamiento de los datos personales. Además, la ley establece que el aviso de privacidad debe estar redactado y estructurado de manera



clara y sencilla, para que cumpla adecuadamente su función de informar (LPDPPSONL, 2019, art. 27 y 28).

¿Qué pasa si no entiendo por qué me solicitan un dato?

Pregunta. No necesitas utilizar palabras jurídicas, por lo que puedes decir “¿para qué necesitan este dato?”, “¿es obligatorio proporcionarlo para realizar el trámite?” o “¿dónde puedo consultar el aviso de privacidad?”. Son preguntas sencillas que pueden ayudarte a tomar una decisión informada.

Un ejemplo relacionado con una aplicación

Supongamos que descargas una aplicación para consultar horarios de transporte público. La aplicación solicita acceso a tu ubicación para mostrarte las rutas cercanas. En este caso, existe una relación evidente entre el dato solicitado y la función que deseas utilizar.

Ahora imagina que la misma aplicación solicita acceso permanente a tus fotografías, contactos y micrófono. No necesariamente significa que esté actuando de manera incorrecta, pero sí es razonable que te preguntes para qué necesita una aplicación de transporte todos esos permisos. Antes de aceptarlos, revisa la información que proporciona la aplicación y decide qué permisos son realmente necesarios.

¿Qué puedes hacer cuando consideras que te piden demasiado?

No siempre podrás negarte a proporcionar un dato. En algunos trámites o servicios existen datos que deben solicitarse porque una ley o una disposición aplicable así lo establece. Por eso, la pregunta no debe ser simplemente “¿me pueden pedir este dato?”, sino “¿por qué necesitan este dato y cuál es la finalidad para la que será utilizado?”.

Si se trata de una institución pública, puedes consultar su aviso de privacidad y, si tienes dudas sobre el tratamiento de tus datos, acudir a su Unidad de Transparencia o buscar orientación ante la autoridad competente. En el caso de sujetos obligados de Nuevo León, el marco estatal es particularmente importante para comprender estas obligaciones.



Tabla 5.8 Antes de entregar un dato personal.

Pregunta	¿Qué buscas saber?
¿Quién?	¿Quién solicita mis datos y quién será el responsable de ellos?
¿Para qué?	¿Cuál es la finalidad para la que se utilizarán mis datos?
¿Cuáles?	¿Qué datos personales me están solicitando?
¿Es necesario?	¿Tiene relación con el trámite o servicio?
¿Dónde?	¿Dónde puedo consultar el aviso de privacidad?
¿Cómo?	¿Estoy entregando mis datos por un medio oficial y seguro?

Una regla fácil de recordar. Si no sabes para qué quieren tu dato, pregunta antes de entregarlo. No se trata de desconfiar de todas las instituciones o empresas, sino de conocer qué información compartimos y tomar decisiones informadas sobre nuestros datos personales.

Concepto clave. Que alguien solicite un dato personal no significa automáticamente que esté pidiendo demasiado. La mejor forma de saberlo es conocer la finalidad para la que se solicita y verificar que exista una relación entre esa información y el trámite o servicio que queremos recibir.

Para recordar. No entregues información por costumbre. Antes de compartirla, recuerda preguntar, leer, verificar, comprender y decidir. Tus datos personales tienen valor y tú tienes derecho a conocer cómo serán utilizados.

5.6 ¿Cuándo es necesario entregar una copia de tu identificación oficial?

La identificación oficial es uno de los documentos que más utilizamos para acreditar nuestra personalidad, dicho de otro modo, para demostrar quiénes somos. La presentamos al realizar trámites, contratar servicios, recoger documentos, abrir cuentas o llevar a cabo determinadas gestiones.

Sin embargo, entregar una copia de nuestra identificación también significa proporcionar varios datos personales en un solo documento, tales como nombre, fotografía, firma, domicilio, fecha de nacimiento, CURP u otros datos que permiten identificarnos, entre otros elementos.



Por eso, antes de entregar una copia, vale la pena detenernos y preguntarnos si realmente necesitan una copia completa de nuestra identificación para realizar ese trámite. La respuesta dependerá del trámite y de las reglas que le sean aplicables.

¿Por qué pueden pedirte una identificación?

En algunos trámites es necesario comprobar que la persona que realiza la gestión es realmente quien dice ser. Por ejemplo, una institución puede necesitar verificar tu identidad para entregarte un documento a tu nombre, realizar un trámite en el que eres la persona interesada, permitir el acceso a determinada información personal, acreditar que eres titular de un servicio, o llevar a cabo determinados procedimientos en los que la identificación esté prevista como requisito.

En el caso de los sujetos obligados de Nuevo León, la legislación estatal contempla la identificación oficial como uno de los medios mediante los cuales una persona puede acreditar su identidad para ejercer determinados derechos relacionados con sus datos personales.

Pero existe una diferencia importante, que una institución necesite comprobar tu identidad no significa automáticamente que necesite conservar una copia completa de tu identificación. Por eso es válido preguntar.

Antes de entregar una copia, pregunta

Puedes utilizar preguntas muy sencillas, como ¿para qué necesitan la copia?, ¿es un requisito del trámite?, ¿dónde se establece ese requisito?, ¿qué harán con la copia?, ¿cuánto tiempo la conservarán? y ¿puedo consultar su aviso de privacidad? Estas preguntas no significan que estés rechazando realizar el trámite; simplemente te ayudan a conocer qué sucederá con tus datos.



No es lo mismo mostrar que entregar una copia

Esta diferencia puede parecer pequeña, pero es importante, por ejemplo, mostrar una identificación oficial permite acreditar o verificar la identidad de una persona, mediante el cotejo de la información contenida en dicho documento, por lo tanto, entregar una copia significa que otra persona o institución tendrá un documento que contiene diversos datos personales y podrá conservarlo de acuerdo con las reglas aplicables.

Por eso, cuando solamente necesitas comprobar tu identidad, puedes preguntar si basta con mostrar el documento original en lugar de entregar una copia. Esto dependerá del trámite y de sus requisitos.

¿Qué puedes hacer para proteger la copia?

Si después de verificar que la copia es necesaria tienes que entregarla, puedes tomar algunas precauciones:

1. **Verifica quién la recibirá.** Asegúrate de que estás entregando el documento a la institución, empresa o persona que realmente realiza el trámite.
2. **Utiliza un medio oficial.** Si debes enviarla de manera digital, utiliza el correo, plataforma o sistema oficial indicado para el trámite. Evita enviar documentos personales a números de teléfono o cuentas personales que no puedas verificar.
3. **Pregunta para qué será utilizada.** La persona o institución debe poder explicarte la finalidad relacionada con la recopilación de tus datos.
4. **Revisa el aviso de privacidad.** Te permite conocer quién tratará tus datos y para qué finalidad.
5. **Evita compartir copias innecesariamente.** No entregues una copia simplemente porque alguien te la pidió; primero verifica si realmente es necesaria.

¿Puedo poner una leyenda en la copia?

En determinadas situaciones puede ser útil colocar sobre la copia una leyenda que indique para qué se entrega (por ejemplo, "Copia entregada exclusivamente para el trámite de _____, ante _____, con fecha

_____.”). Esto puede ayudar a dejar claro el propósito para el cual se proporcionó el documento.

Es importante señalar que esta medida no sustituye las obligaciones legales de quien recibe los datos ni garantiza por sí sola que la copia no pueda utilizarse de otra manera; es simplemente una medida preventiva que puede ayudar a identificar el propósito de la copia.

Un ejemplo de la vida cotidiana

Carlos acudió a una institución para realizar un trámite. La persona que lo atendió le pidió una copia de su identificación oficial. Carlos preguntó para qué la necesitaban, y la persona le explicó que debía integrar su expediente y le indicó dónde podía consultar el aviso de privacidad. Carlos verificó que el trámite fuera oficial y entregó la copia por el medio indicado.

En otro momento, una persona le pidió una fotografía de su identificación mediante una aplicación de mensajería personal, pero no pudo explicar para qué la necesitaba. Carlos decidió no enviarla hasta confirmar la identidad de la persona y la finalidad de la solicitud.

¿Qué podemos aprender? No todas las solicitudes de una copia de identificación deben aceptarse automáticamente. Antes de entregarla, conviene conocer quién la solicita, para qué la necesita y cómo será protegida.

¿Y si me dicen que es requisito?

Si te dicen que la copia es obligatoria, puedes preguntar dónde está establecido ese requisito. En algunos trámites efectivamente existe una disposición que exige acreditar la identidad mediante determinados documentos. La pregunta no busca impedir el trámite, sino ayudarte a distinguir entre un requisito necesario y una solicitud adicional que no está claramente justificada.



Tabla 5.9 Antes de entregar una copia de tu identificación.

Situación	Pregúntate
Te solicitan una copia.	¿Realmente es necesaria?
Te dicen que es requisito.	¿Dónde está establecido?
Te piden enviarla por internet.	¿El sitio o medio es oficial?
No te explican para qué la quieren.	¿Cuál es la finalidad?
No conoces cómo tratarán la información.	¿Dónde puedo consultar el aviso de privacidad?
Solo necesitan comprobar quién eres.	¿Es suficiente mostrar el original?
Ya no necesitas realizar el trámite.	¿Qué sucederá con la copia que entregué?

Una regla fácil de recordar. Antes de entregar una copia de tu identificación, verifica que sea necesaria, conoce para qué será utilizada y asegúrate de entregarla por un medio confiable. No se trata de negarnos a entregar nuestra identificación cuando realmente es necesaria, sino de evitar entregar copias de documentos personales sin saber quién las tendrá, para qué las utilizará y cómo serán protegidas.

Concepto clave. Tu identificación oficial contiene varios datos personales en un solo documento. Por eso, antes de entregar una copia, verifica que sea necesaria para el trámite y pregunta cuál será su finalidad.

Para recordar. No entregues una copia por costumbre. Antes, pregunta para qué la necesitan, verifica quién la solicita, confirma si es un requisito, revisa el aviso de privacidad, utiliza medios oficiales y conserva comprobantes del trámite cuando sea posible. Y recuerda, mostrar tu identificación y entregar una copia no son necesariamente lo mismo.



5.7 Cámaras de seguridad, fotografías y videograbaciones

Es posible que, sin darnos cuenta, aparezcamos en una fotografía o en una grabación varias veces durante el día. Una cámara puede encontrarse en la entrada de una institución pública, en una escuela, en un hospital, en un edificio, en un establecimiento comercial o en un espacio destinado a brindar seguridad. También podemos aparecer en fotografías o videos realizados durante un evento, una actividad escolar, una reunión de trabajo o una celebración.



Esto nos lleva a una pregunta importante, la cual es si una fotografía o una videograbación también puede ser un dato personal. La respuesta es sí, cuando permite identificar o hacer identificable a una persona. La imagen de una persona puede ser un dato personal porque permite reconocerla; lo mismo puede ocurrir con una grabación de voz cuando permite identificar a quien habla. Por ello, tomar, almacenar, utilizar o compartir fotografías y videograbaciones puede implicar un tratamiento de datos personales.

¿Todas las imágenes son datos personales?

No necesariamente. La clave está en saber si la información permite identificar o hacer identificable a una persona. Por ejemplo, una fotografía de un paisaje sin personas identificables no contiene, por sí misma, información que permita identificar a una persona; en cambio, una fotografía en la que aparece claramente una persona identificable sí puede involucrar un dato personal. Lo mismo puede suceder con una grabación de una cámara de seguridad en la que una persona puede ser reconocida.

¿Para qué se utilizan las cámaras de seguridad?

Las cámaras pueden utilizarse para diferentes finalidades, como proteger instalaciones, prevenir determinados incidentes, vigilar accesos, controlar entradas y salidas, proteger a las personas que se encuentran en un lugar, o investigar un incidente cuando corresponda.



Sin embargo, que una cámara tenga una finalidad de seguridad no significa que las imágenes puedan utilizarse para cualquier otro propósito. La información debe manejarse de acuerdo con la finalidad para la que fue obtenida y con las obligaciones aplicables a quien la trata.

¿Quién puede tener cámaras de seguridad?

En nuestra vida cotidiana podemos encontrarnos con cámaras instaladas por distintos responsables, según el lugar de que se trate.

Tabla 5.10 Lugares con cámaras de seguridad y posibles responsables.

Lugar	¿Quién podría utilizarlas?
Oficinas de gobierno	Dependencias y entidades públicas.
Escuelas	Instituciones educativas públicas o particulares.
Hospitales	Instituciones y prestadores de servicios de salud.
Bancos	Instituciones financieras.
Comercios	Empresas o establecimientos privados.
Edificios	Administraciones o responsables del inmueble.
Espacios públicos	Autoridades competentes, conforme a sus atribuciones.

La forma en que deben tratarse las imágenes dependerá de quién sea responsable de ellas y de la finalidad para la que fueron obtenidas. En el caso de las instituciones públicas de Nuevo León, debe considerarse la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Nuevo León y las demás disposiciones aplicables.

¿Pueden grabarte sin que lo sepas?

La presencia de una cámara no significa necesariamente que exista una violación a la protección de datos personales. En determinados lugares puede ser necesario utilizar sistemas de videovigilancia para cumplir una función de seguridad o prestar un servicio.



Lo importante es que las personas puedan conocer, cuando corresponda, quién utiliza las cámaras, para qué finalidad y cómo se tratará la información obtenida. Por eso es frecuente encontrar avisos colocados en los accesos o zonas videovigiladas con frases como “área videovigilada” “Sonríe estas siendo grabado” o “este establecimiento cuenta con cámaras de seguridad”, que ayudan a informar que existe un sistema de videovigilancia.

No obstante, a lo anterior, colocar únicamente una imagen de una cámara acompañada cualquiera de las frases referidas en el párrafo anterior, no debe entenderse automáticamente como el cumplimiento de todas las obligaciones en materia de protección de datos personales; motivo por el cual, el responsable deberá proporcionar la información que corresponda mediante el aviso de privacidad y conforme a las leyes y regulaciones que resulten aplicable.

¿Pueden compartir una grabación?

No debe entenderse que una grabación puede compartirse libremente simplemente porque fue obtenida por una cámara de seguridad. Por ejemplo, una grabación puede contener la imagen de varias personas que no tienen relación con un incidente; compartirla públicamente en redes sociales puede exponer información personal de personas que aparecen en ella.

Por eso, antes de publicar o enviar una grabación debemos preguntarnos para qué se obtuvo, quién necesita verla, si existe una razón válida para compartirla y si la persona responsable tiene autorización o fundamento para hacerlo.

Un ejemplo de la vida cotidiana

Una tienda cuenta con cámaras de seguridad para proteger sus instalaciones. Un día ocurre un incidente y una persona aparece en una de las grabaciones. El encargado obtiene el vídeo y decide publicarlo en redes sociales para pedir ayuda a la ciudadanía.

Aunque la intención pueda ser localizar a una persona, la grabación contiene imágenes de otras personas que se encontraban en el lugar y que quizá no tienen ninguna relación con el incidente. Antes de hacer pública una grabación, deben analizarse las reglas aplicables y la necesidad de proteger los datos de las personas que aparecen en ella.

¿Qué podemos aprender? Una grabación de seguridad no debe convertirse automáticamente en contenido para redes sociales. Las imágenes deben manejarse con responsabilidad y de acuerdo con la finalidad para la que fueron obtenidas.

¿Y las fotografías de eventos?

No todas las fotografías requieren el mismo tratamiento. Por ejemplo, si una persona toma una fotografía familiar para conservarla en su álbum personal, estamos ante una situación diferente de cuando una institución fotografía a cientos de personas durante un evento y posteriormente publica las imágenes en su sitio web o redes sociales.



Cuando una institución toma fotografías para después utilizarlas públicamente, es importante que informe a las personas sobre esa finalidad y cumpla con las obligaciones que correspondan. Esto adquiere especial importancia cuando aparecen niñas, niños y adolescentes, ya que su imagen y otros elementos que permitan identificarlos pueden revelar información sobre ellos y exponerlos a riesgos que deben ser considerados de manera reforzada al decidir si las fotografías serán difundidas. Por ello, las instituciones deben prestar especial atención a la protección de su privacidad y al cumplimiento de las disposiciones aplicables antes de publicar este tipo de imágenes.



Tabla 5.11 Antes de publicar una fotografía, piensa.

Pregunta	¿Por qué importa?
¿Quién aparece en la fotografía?	Puede contener datos personales de varias personas.
¿Se puede identificar a las personas?	Si pueden reconocerse, la imagen puede constituir un dato personal.
¿Dónde fue tomada?	Puede revelar información sobre la ubicación o actividades de una persona.
¿La fotografía incluye niñas, niños o adolescentes?	Su información merece especial cuidado.
¿Tengo una razón para hacerla pública?	Publicar no siempre es necesario.
¿Quién podrá verla?	Una publicación en internet puede alcanzar a muchas personas.

Observa una fotografía aparentemente sencilla, puede mostrar el rostro de una persona, su escuela, su domicilio, su ubicación y las personas con las que se encuentra. Por eso, una fotografía no debe analizarse únicamente como una imagen; también debemos pensar en la información que puede revelar.

¿Qué pasa si una cámara está en una institución pública?

Cuando una institución pública de Nuevo León utiliza cámaras de video-vigilancia, el tratamiento de las imágenes debe sujetarse a las obligaciones establecidas en la legislación aplicable en materia de protección de datos personales. La ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Nuevo León establece principios y obligaciones para quienes tratan datos personales bajo su responsabilidad.

Entre otras cuestiones, deberá determinar para que serán utilizadas las imágenes, e implementar mecanismos de seguridad para evitar que terceros accedan a dichas imágenes o realicen tratamiento no autorizados.

No debe pasar desapercibido que la videovigilancia es una herramienta, sin embargo, su utilización no elimina las obligaciones del responsable respecto a los datos personales que obtiene mediante ella.

Esto significa que las imágenes obtenidas mediante sistemas de videovigilancia no deben considerarse información sin dueño, son datos que deben protegerse cuando permiten identificar a una persona.

¿Puedo ejercer derechos respecto de una videograbación en la que aparezco?

Cuando una institución pública trata datos personales relacionados contigo, puedes ejercer los derechos que la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Nuevo León reconoce respecto de esa información, siempre que se cumplan los requisitos establecidos en dicha norma.

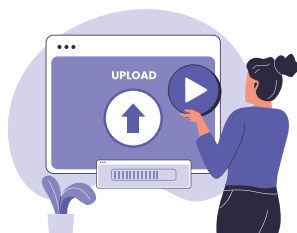
Esto puede incluir información contenida en fotografías o videograbaciones cuando permita identificarte, no obstante, la existencia de una grabación no significa que necesariamente deba entregarse una copia íntegra en todos los casos.

Lo anterior, debido a que existen situaciones en las que una grabación puede estar relacionada con investigaciones, seguridad pública, procedimientos o derechos de otras personas. En esos casos, el acceso puede estar sujeto a determinadas reglas y restricciones. Por eso, no toda grabación puede entregarse automáticamente a cualquier persona que la solicite.

Concepto clave. Una fotografía o videograbación (tu imagen) puede ser un dato personal cuando permite identificarte. Por eso, las fotografías y videograbaciones deben utilizarse y compartirse de manera responsable, respetando la finalidad para la que fueron obtenidas y las reglas de protección de datos que correspondan.

Para recordar. Cuando aparezcas en una fotografía o videograbación, recuerda que tu imagen puede ser un dato personal, pregunta para qué se utilizará. Cuando corresponda, pregunta para qué será utilizada y cómo será difundida. Si compartes fotografías o videos de otras personas, considera las posibles consecuencias y presta especial atención cuando

aparezcan niños, niñas y adolescentes. Su imagen y sus datos personales requieren consideraciones particulares de protección, que conoceremos con mayor detalle en el siguiente capítulo. Antes de publicar con fotografía o videograbación en redes sociales, piensa en quién podrá verla y por cuánto tiempo podría permanecer disponible.



Capítulo 6. Protección de datos para grupos de atención prioritaria

6.1 ¿Cómo cuidar la información de niñas, niños y adolescentes?

Niñas, niños y adolescentes forman parte de una sociedad en la que gran parte de las actividades ocurren también en internet. Estudian, juegan, se comunican, realizan actividades deportivas, utilizan aplicaciones, ven videos y comparten fotografías. En ese camino van dejando información sobre ellos, como su nombre, edad, escuela, fotografías, voz, ubicación, gustos, actividades e incluso información sobre su familia.



Por eso, cuidar sus datos personales no significa alejarlos de la tecnología. Significa enseñarles a utilizarla sin poner en riesgo información que puede revelar demasiado sobre su vida.

En Nuevo León, este cuidado no es solamente una recomendación. La Ley de los Derechos de Niñas, Niños y Adolescentes para el Estado de Nuevo León reconoce que niñas, niños y adolescentes tienen derecho a la protección de sus datos personales y a la vida privada, y establece que, cuando una autoridad trata sus datos, debe privilegiar su interés superior (Ley de los Derechos de Niñas, Niños y Adolescentes para el Estado de Nuevo León, 2025, art. 97).

¿Qué información debemos cuidar?

Tabla 6.1 Información de niñas, niños y adolescentes que merece especial cuidado.

Información	¿Por qué debemos cuidarla?
Nombre completo	Permite identificar al menor.
Fotografía	Puede revelar su identidad y apariencia.
Nombre de la escuela	Permite conocer dónde estudia.
Domicilio	Puede revelar dónde vive.
Número telefónico	Puede facilitar contactos no deseados.
Ubicación	Puede revelar dónde se encuentra o los lugares que frecuenta.
Voz	Puede permitir identificarlo.
Información médica	Puede revelar aspectos de su salud.
Calificaciones	Forma parte de su información personal y escolar.
Fotografías y videos	Pueden mostrar su identidad, actividades, relaciones y ubicación.

Fuente: elaboración propia con fines ilustrativos. La naturaleza y clasificación jurídica de cada dato dependerá de la información y del contexto en el que sea tratado.

No todos estos datos tienen la misma naturaleza ni generan necesariamente el mismo nivel de riesgo, sin embargo, cuando permiten identificar o hacer identificable a una niña, niño o adolescente, deben ser tratados considerando las disposiciones que protegen sus derechos y en especial al interés superior del menor.

La idea no es enseñar a niñas, niños y adolescentes a tener miedo de compartir información, sino enseñarles a reconocer qué información es privada y cuándo deben pedir ayuda antes de compartirla.



¿Por qué necesita especial protección la información de carácter personal de las niñas, niños y adolescentes?

Una persona adulta puede tener mayor experiencia para reconocer cuando alguien intenta obtener información que no debería proporcionar; una niña, un niño o un adolescente todavía está desarrollando esas habilidades. Por eso, una solicitud aparentemente sencilla puede pasar desapercibida, preguntas como “¿en qué escuela estudias?”, “¿dónde vives?”, “¿a qué hora sales de clases?”, “mándame una fotografía” o “dime dónde estás” pueden parecer, cada una por separado, poco importantes. Pero si alguien reúne todas esas respuestas, puede obtener una imagen mucho más completa de la vida de un menor. Por eso es importante enseñarles a pensar antes de compartir.

La protección especial de niñas, niños y adolescentes no debe entenderse únicamente como una consecuencia de que puedan tener menos experiencia utilizando internet, existe una razón jurídica más profunda.

En todas las decisiones y actuaciones que les conciernan debe considerarse el interés superior de la niñez, principio que exige que la protección y garantía de sus derechos ocupe una consideración primordial. Esto cobra real importancia debido a que la Suprema Corte de Justicia de la Nación ha sostenido que el interés superior de la niñez constituye un principio rector y una consideración primordial que debe orientar las decisiones de las autoridades cuando puedan afectar los derechos de niñas, niños y adolescentes; en particular, la Primera Sala ha señalado que este principio exige realizar un análisis específico de las circunstancias del caso y no una aplicación automática o abstracta de la norma, esta idea tiene su sustento, en la tesis de rubro: **“INTERÉS SUPERIOR DEL MENOR. SU CONFIGURACIÓN COMO CONCEPTO JURÍDICO INDETERMINADO Y CRITERIOS PARA SU APLICACIÓN A CASOS CONCRETOS”¹**.



¹ Época: Décima Época; Registro: 2006593; Instancia: Primera Sala, Tipo de Tesis: Jurisprudencia; Fuente: Gaceta del Semanario Judicial de la Federación. Libro 7, Junio de 2014, Tomo I, página 270; Materia(s): Constitucional; Tesis: 1a./J. 44/2014 (10a.).



Así pues, aplicado a la protección de datos personales, lo anterior significa que no basta con afirmar que la información será utilizada para una finalidad institucional, educativa, médica o administrativa, también debe analizarse si los datos solicitados son necesarios, qué riesgos puede generar su tratamiento, quién tendrá acceso a ellos, durante cuánto tiempo se conservarán y qué medidas se adoptarán para evitar un uso indebido, ya que esto también alcanza su privacidad y sus datos personales.

Adicionalmente, es que se debe tener presente que las niñas, niños y adolescentes se encuentran en un proceso de desarrollo y adquisición progresiva de capacidades, por tal motivo la manera en que participan en las decisiones relacionadas con sus datos debe considerar su edad, madurez y desarrollo; en resumidas cuentas *“protegerlos no significa ignorar su opinión, sino acompañarlos en el ejercicio de sus derechos de acuerdo con su desarrollo progresivo”*.

El interés superior de la niñez también importa cuando hablamos de datos

Para una mayor comprensión a lo antes señalado, imaginemos que una institución de gobierno quiere implementar una nueva plataforma digital para estudiantes, dicha plataforma permite registrar asistencia, entregar tareas y consultar calificaciones, pero además solicita fotografías, ubicación permanente y acceso a determinada información del dispositivo.

Cuando el tratamiento involucra datos de niñas, niños o adolescentes no basta con argumentar que la tecnología puede resultar útil; es necesario que la institución analice qué información resulta necesaria, para qué será utilizada, qué riesgos pueden existir y qué medidas son adecuadas para proteger los derechos de las personas menores de edad; el interés superior de la niñez debe formar parte de las decisiones que puedan afectar sus derechos.

Protección no significa excluirlos de las decisiones

Con frecuencia se piensa que cualquier decisión relacionada con los datos personales de una persona menor de edad corresponde exclusivamente a los adultos, sin embargo, la realidad requiere un análisis que merece más

atención, puesto que niñas, niños y adolescentes son titulares de derechos y desarrollan progresivamente la capacidad para comprender y participar en las decisiones que les afectan.

Por ello, de acuerdo con su edad y grado de madurez, resulta importante explicarles de manera comprensible los siguientes cuestionamientos que se indican a título orientativo:

- a) qué información se está solicitando;
- b) quién la utilizará;
- c) para qué será utilizada;
- d) si será compartida o publicada;
- e) qué consecuencias puede tener determinada decisión; y
- f) qué pueden hacer si algo les genera dudas o incomodidad.

Esto permite que la protección de datos personales se convierta también en un proceso de educación y participación, y no solamente en una serie de prohibiciones impuestas por personas adultas.

Una fotografía puede contar mucho

Las fotografías son una de las formas más comunes de compartir información sobre niñas, niños y adolescentes. Una fotografía del primer día de clases puede mostrar su rostro, su uniforme, el nombre de la escuela y el lugar donde se encuentra; una fotografía durante un viaje puede mostrar su rostro, su ubicación, las personas con las que está y el momento en que se encuentra fuera de casa.

Por eso, antes de publicar una fotografía conviene hacer una pausa y preguntarse qué información se está mostrando además de la fotografía misma. No se trata de prohibir que las familias compartan momentos importantes, sino de hacerlo de manera responsable.

¿Qué deben enseñar las personas adultas?

La protección comienza en casa, pero no termina ahí. Madres, padres, tutores, familiares, docentes y personas responsables pueden ayudar enseñando reglas sencillas:



1. **No compartir contraseñas.** Las contraseñas son personales y no deben compartirse con amistades ni con personas desconocidas.
2. **No publicar la ubicación en tiempo real.** Es preferible evitar publicaciones que permitan conocer dónde se encuentra el menor en ese momento.
3. **No proporcionar información a desconocidos.** Si alguien solicita datos personales, fotografías o información sobre la familia, es mejor no responder y acudir a una persona adulta de confianza.
4. **Preguntar antes de descargar una aplicación.** Algunas aplicaciones solicitan información o permisos que deben revisarse antes de aceptarlos.
5. **Avisar cuando algo resulte incómodo.** Un menor debe saber que puede contarle a una persona adulta si alguien le pide fotografías, información personal o le hace sentir incómodo.

Enseñarles a decir “no”



Una de las herramientas más sencillas de protección es enseñarles que no están obligados a responder todas las preguntas que les hagan en internet. Pueden aprender frases como “no quiero compartir esa información”, “voy a preguntarle primero a mi mamá, papá o persona responsable”, “no conozco a esa persona” o “no voy a compartir dónde estoy”. Son respuestas sencillas, pero ayudan a que niñas, niños y adolescentes comprendan que poner límites también es una forma de protegerse.

Las escuelas también manejan datos personales

Las escuelas tienen información importante de sus estudiantes, como expedientes escolares, calificaciones, datos de contacto, información médica, registros de asistencia, fotografías, información de madres, padres o tutores y datos relacionados con actividades escolares.

Cuando se trata de una institución pública sujeta a la legislación de Nuevo León, el tratamiento de esa información debe cumplir con las obligaciones establecidas en la LPDPPSONL, que establece, entre otros aspectos, que los sujetos obligados deben utilizar los datos para finalidades concretas y relacionadas con sus atribuciones.



Por eso, las familias pueden preguntar qué datos tienen de su hija o hijo, para qué los utilizan, quién puede tener acceso a ellos y dónde pueden consultar el aviso de privacidad. Estas preguntas son parte de una cultura de protección de datos.

¿Qué pasa con las fotografías de actividades escolares?

Imaginemos que una escuela organiza un festival y toma fotografías de los estudiantes. Posteriormente, alguien propone publicar todas las fotografías en las redes sociales de la institución. Antes de hacerlo, es necesario considerar las obligaciones aplicables al tratamiento de esas imágenes y, especialmente, el derecho a la privacidad y protección de datos de niñas, niños y adolescentes.

La legislación de Nuevo León establece que no deben realizarse divulgaciones o difusiones ilícitas de información o datos personales de niñas, niños y adolescentes que permitan identificarlos y que afecten sus derechos, honra, imagen o reputación (Ley de los Derechos de Niñas, Niños y Adolescentes para el Estado de Nuevo León, 2025, art. 98). Por eso, tomar una fotografía y hacerla pública son situaciones que deben analizarse de manera responsable.

Un ejemplo de la vida cotidiana

Mariana tiene ocho años. Su familia está orgullosa porque participó en una competencia deportiva y su mamá quiere publicar una fotografía del evento. Antes de hacerlo, revisa la imagen y se da cuenta de que aparecen el rostro de Mariana, su uniforme con el nombre de la escuela y un letrero que permite identificar el lugar donde se realizó la competencia. La mamá decide revisar la fotografía y la información que la acompaña antes de publicarla.

¿Qué aprendemos?

No tenemos que dejar de compartir momentos familiares. Pero antes de publicar una imagen de una niña, niño o adolescente, podemos preguntarnos si estamos mostrando más información de la necesaria.



Una regla para madres, padres y personas responsables

Antes de publicar información sobre una niña, niño o adolescente, conviene detenerse a pensar sobre aspectos como qué estoy compartiendo, quién podrá verlo, qué información revela, si realmente es necesario publicarla y si aparecen otros menores. Esta pequeña revisión puede evitar que información personal termine circulando mucho más allá de lo que originalmente imaginamos.

No se trata de prohibir, sino de acompañar

La protección de datos personales no debe convertirse en una lista interminable de prohibiciones. Decir simplemente “no uses internet” no enseña a proteger los datos; es mucho más útil explicar “antes de compartir algo, piensa quién podrá verlo”. En lugar de “no hables con nadie”, podemos enseñar “si alguien que no conoces te pide información personal, no tienes que responder y puedes pedir ayuda”. El objetivo es que niñas, niños y adolescentes desarrollen herramientas que puedan utilizar incluso cuando una persona adulta no esté a su lado.



Tabla 6.2 Cinco preguntas antes de compartir.

Antes de compartir...	Pregúntate:
Una fotografía	¿Qué información aparece en ella?
Mi ubicación	¿Necesito que otras personas sepan dónde estoy?
Mi nombre o escuela	¿Realmente necesito proporcionar este dato?
Un video	¿Quién aparece y quién podrá verlo?
Información de otra persona	¿Tengo que compartirla?

Fuente: Elaboración propia con base en SaveTheChildren.mx.

Una regla fácil de recordar. “Si tienes dudas, pregunta antes de compartir.”

Una niña, niño o adolescente nunca debería sentirse mal por pedir ayuda. Si algo que ocurre en internet le causa preocupación, incomodidad o miedo, debe saber que puede acudir a una persona adulta de confianza.

Concepto clave. Los datos personales de niñas, niños y adolescentes merecen especial cuidado porque forman parte de su identidad, su vida privada y su desarrollo. Protegerlos no significa impedirles utilizar la tecnología, sino enseñarles a compartir información de manera responsable y acompañarlos para que aprendan a tomar decisiones.

Para recordar. Una fotografía puede revelar una escuela; una publicación puede revelar una ubicación; un video puede mostrar relaciones personales; un comentario puede proporcionar información sobre la vida de un menor. Por eso, antes de compartir información sobre una niña, niño o adolescente, detente y piensa si realmente es necesario hacerlo y quién podrá verla.

6.2 Proteger los datos personales de las personas adultas mayores



Las personas adultas mayores realizan trámites, utilizan servicios bancarios, reciben atención médica, hacen compras, utilizan teléfonos celulares y, cada vez más, emplean internet y aplicaciones. En todas estas actividades pueden proporcionar datos personales como su nombre, domicilio, teléfono, información médica, datos bancarios, documentos de identificación o información relacionada con sus familiares.

La protección de datos personales cobra especial importancia porque, en determinadas circunstancias, las personas adultas mayores pueden

encontrarse en situaciones de vulnerabilidad que requieren una protección reforzada. La Suprema Corte de Justicia de la Nación ha reconocido que las personas adultas mayores pueden encontrarse en condiciones de vulnerabilidad y, por ello, ha señalado que merecen una especial protección por parte de los órganos del Estado. Esta protección debe considerar las circunstancias particulares de cada persona y no únicamente su edad (Suprema Corte de Justicia de la Nación, Primera Sala, tesis aislada 1a. CCXXIV/2015 (10a.), registro digital 2009452, de rubro “ADULTOS MAYORES. AL CONSTITUIR UN GRUPO VULNERABLE MERECEN UNA ESPECIAL PROTECCIÓN POR PARTE DE LOS ÓRGANOS DEL ESTADO”).

Esta situación también puede presentarse en el entorno digital. La falta de familiaridad con determinadas herramientas, trámites o mecanismos de seguridad en internet puede dificultar la identificación de situaciones de riesgo. La policía Cibernética de la Secretaría de Seguridad Ciudadana de la Ciudad de México ha advertido sobre la exposición de las personas adultas mayores a delitos cibernéticos y ha identificado, entre los ilícitos reportados, el fraude y la extorsión cibernética.

Por ello, proteger sus datos personales no significa alejarlos de la tecnología ni hacer los trámites por ellos. Significa brindarles información clara, acompañamiento cuando lo necesiten y herramientas que les permitan tomar decisiones informadas sobre qué información compartir, con quien y para qué.

En México, las personas adultas mayores tienen derecho a vivir con dignidad, recibir un trato respetuoso y ejercer sus derechos. La protección de sus datos personales forma parte de este cuidado y requiere considerar las circunstancias particulares de cada persona, especialmente cuando puedan existir dificultades o enfrentar riesgos relacionados con el uso de tecnologías digitales



¿Qué datos debemos cuidar especialmente?

Las personas adultas mayores pueden proporcionar información personal en muchas situaciones cotidianas.

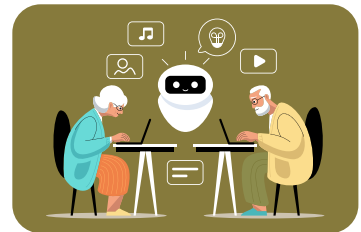
Tabla 6.3 Datos de las personas adultas mayores que requieren especial cuidado.

Información	¿Dónde puede aparecer?
Nombre y domicilio	Identificación, recibos y trámites
Número telefónico	Bancos, servicios y contactos
Datos bancarios	Cuentas, tarjetas y pagos
Información médica	Consultas, hospitales y expedientes
CURP y RFC	Trámites y servicios
Número de seguridad social	Servicios relacionados con la seguridad social
Fotografías	Identificaciones, trámites y redes sociales
Contraseñas	Aplicaciones, correo y servicios digitales
Información familiar	Trámites, servicios y comunicaciones
Datos de pensión o jubilación	Instituciones y trámites correspondientes

La lista puede ser mucho más amplia. Lo importante es entender que no todos los datos deben compartirse con cualquier persona.

El problema no siempre es la tecnología

Cuando hablamos de protección de datos de personas adultas mayores, es importante evitar la idea de que las personas mayores no utilizan o no saben utilizar la tecnología. Los datos de la Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares (ENDUTIH) muestran que las personas de este grupo de edad también utilizan internet en dispositivos tecnológicos, aunque su uso puede presentar diferencias respecto de otros grupos de edad.





El reto no depende únicamente de la edad. Las formas de obtener información personal son cada vez más diversas, una llamada telefónica, un mensaje de texto, un correo electrónico o una página de internet pueden utilizarse para solicitar información. Por ello, es importante contar con herramientas que permitan reconocer situaciones de riesgo, detenerse y verificar la información antes de compartir datos personales.

Una llamada que parece importante

Imaginemos esta situación, una persona recibe una llamada en la que le dicen “señor, hablamos de su banco; detectamos un problema con su cuenta, necesitamos confirmar algunos datos”. La persona puede sentirse preocupada y pensar que debe responder inmediatamente.

Pero antes de proporcionar información puede hacer algo muy sencillo, colgar y comunicarse directamente con el banco utilizando el número oficial que aparece en su tarjeta, estado de cuenta o sitio institucional. Esta práctica puede evitar que entregue información a alguien que pretende hacerse pasar por una institución.

Cuidado con los mensajes que generan preocupación

Algunas solicitudes de información personal buscan que la persona actúe rápidamente, mediante frases como “su cuenta será cancelada hoy”, “tiene un problema con su pensión”, “su tarjeta será bloqueada”, “necesitamos actualizar sus datos inmediatamente” o “ha ganado un premio, necesitamos sus datos para entregárselo”. La intención de estos mensajes puede ser conseguir información personal, contraseñas, datos bancarios o códigos de seguridad. La recomendación es sencilla, consiste en no actuar por presión y verificar primero.

¿Qué información nunca debe compartirse por teléfono o mensaje?

Hay información que requiere especial cuidado, particularmente cuando alguien la solicita inesperadamente, tales como contraseñas, números de identificación personal, códigos de seguridad, datos completos de tarjetas bancarias, claves de acceso, información que permita entrar a una cuenta, o fotografías de documentos personales cuando no exista una razón clara para enviarlas.



Una institución legítima puede necesitar determinados datos para realizar un trámite, pero eso no significa que debamos proporcionar información sensible a cualquier persona que diga representar a una institución.

Una regla muy sencilla “si te apresuran, verifica”

Cuando alguien diga “tiene que hacerlo ahora”, “no cuelgue”, “deme el código inmediatamente” o “no le diga a nadie”, es recomendable detenerse. Puedes decir “voy a verificar directamente con la institución” y, después, utilizar un número o medio oficial para confirmar la situación.

Los familiares también deben respetar sus datos

Proteger los datos personales de una persona adulta mayor no significa únicamente protegerla de personas desconocidas, también debemos respetar su información dentro de la familia. Por ejemplo, no deberíamos compartir sin necesidad fotografías de sus identificaciones, información médica, estados de cuenta, números telefónicos, datos sobre su patrimonio, contraseñas o información sobre sus pensiones o ingresos.

Que exista una relación familiar no significa que la información personal pueda difundirse sin considerar la voluntad, la privacidad y las posibles consecuencias para la persona. El respeto a su información también forma parte del cuidado y la convivencia dentro de la familia.

Cuidado con los documentos

En una situación distinta, las personas adultas mayores pueden tener que entregar documentos que contienen datos personales para realizar trámites o recibir servicios ante instituciones públicas o privadas. Una copia de una identificación oficial, por ejemplo, puede contener diversos datos que permiten identificar a su titular.

Antes de entregar este tipo de documentos, puede ser útil preguntar para que son necesarios, si su presentación es indispensable para el trámite y quien será responsable de recibirlos y tratarlos. Cuando los datos personales sean recabados por una institución u organización sujeta a las disposiciones aplicables en materia de protección de datos personales, esta deberá poner a disposición de la persona el aviso de privacidad correspondiente.



Cuando alguien necesita apoyo

Una persona adulta mayor puede decidir pedir ayuda a un familiar, amigo o persona de confianza para realizar un trámite digital, y eso puede ser útil. Pero existe una diferencia importante entre ayudar y decidir por la persona.

Cuando sea posible, la persona debe saber qué trámite está realizando, qué información está proporcionando, para qué se utilizará, a quién se está entregando y qué está aceptando. La tecnología debe ser una herramienta para facilitar su vida, no una razón para quitarle el control sobre sus propios datos.



Un ejemplo de la vida cotidiana

Don Ernesto recibe un mensaje en su teléfono en el que se lee “Para continuar recibiendo su beneficio, confirme sus datos en el siguiente enlace.” El mensaje incluye un logotipo que parece pertenecer a una institución que él conoce, y Don Ernesto está preocupado porque piensa que podría perder su beneficio.

En lugar de abrir el enlace inmediatamente, llama a la institución utilizando un número oficial. Le informan que no enviaron ese mensaje. Don Ernesto evita proporcionar sus datos.

¿Qué aprendemos?

El mensaje parecía legítimo, pero una apariencia no es suficiente para confiar. Antes de proporcionar información personal, especialmente cuando la solicitud llega de manera inesperada, es mejor verificar directamente con la institución.



¿Cómo pueden ayudar familiares y personas cuidadoras?

Una buena forma de acompañar a una persona adulta mayor es enseñarle algunas reglas sencillas:

1. **Nadie debe presionarte para entregar información.** Si algo parece urgente, verifica.
2. **Las contraseñas son personales.** No deben compartirse por llamadas, mensajes o correos.
3. **No abras enlaces desconocidos.** Primero verifica quién los envió.
4. **No entregues documentos sin preguntar.** Conoce para qué los necesitan.
5. **Si tienes dudas, pide ayuda.** Consultar con una persona de confianza puede evitar un problema.

Tabla 6.4 Antes de compartir tus datos.

Si recibes...	Haz esto
Una llamada inesperada	Verifica quién llama.
Un mensaje urgente	No actúes bajo presión.
Una solicitud de contraseña	No la compartas.
Un enlace desconocido	No lo abras hasta verificarlo.
Una solicitud de identificación	Pregunta para qué la necesitan.
Un trámite digital complicado	Pide apoyo si lo necesitas.
Una petición que te genera dudas	Detente y verifica.

¿Y si alguien ya compartió sus datos?

Lo primero es no entrar en pánico. Dependiendo de qué información se haya compartido, pueden tomarse distintas medidas, como cambiar contraseñas, comunicarse con la institución correspondiente, bloquear o revisar una tarjeta bancaria cuando sea necesario, informar a la institución afectada, guardar mensajes, correos o comprobantes relacionados con el incidente, y solicitar orientación sobre las acciones que correspondan. Lo importante es actuar lo antes posible y conservar evidencia de lo ocurrido.



Una idea que debemos cambiar

No debemos decir “como eres una persona mayor, no puedes hacer ese trámite”; es mejor decir “si necesitas ayuda, podemos hacerlo juntos y tú decides qué información quieres proporcionar”. La protección de datos personales también significa respetar la autonomía de cada persona.

Una regla fácil de recordar. Detente antes de entregar información. Verifica quién la está solicitando. Decide si realmente es necesario compartirla. Tres pasos sencillos pueden evitar muchos problemas.

Concepto clave. Las personas adultas mayores tienen derecho a decidir sobre sus datos personales. Acompañarlas no significa sustituir sus decisiones, sino ayudarlas a comprender qué información están compartiendo, con quién y para qué.

Para recordar. Tu banco no necesita tu contraseña para “proteger” tu cuenta. Una llamada inesperada no debe obligarte a decidir inmediatamente. Una copia de tu identificación no debe entregarse sin saber para qué será utilizada. Pedir ayuda no significa perder el control sobre tus datos. Y, sobre todo, si tienes dudas, detente, verifica directamente con la institución y después decide.

6.3 ¿Qué pasa con los datos personales de las personas en situación de vulnerabilidad?

No todas las personas enfrentan las mismas condiciones para proteger su información personal. Una persona puede encontrarse, de manera temporal o permanente, en una situación que dificulte realizar un trámite, comprender un documento, acceder a una plataforma digital, ejercer un derecho o decidir cómo compartir sus datos.

Esto puede ocurrir, por ejemplo, cuando una persona tiene alguna discapacidad, no sabe leer o escribir, tiene dificultades para utilizar herramientas digitales, se encuentra en una situación económica complicada, está atravesando una emergencia, se encuentra en situación de calle, habla una lengua indígena y el trámite no está disponible en su lengua, está privada de su libertad, es migrante o se encuentra en tránsito, o requiere apoyo para realizar determinados trámites.



Lo importante es entender que la situación de una persona no le quita sus derechos. Por el contrario, las instituciones deben procurar que pueda ejercerlos de manera efectiva.

La protección de datos debe ser para todas las personas

La protección de datos personales no debe depender de cuánto dinero tiene una persona, dónde vive, si sabe utilizar una computadora o si puede realizar un trámite por internet. Todas las personas tienen derecho a que su información personal sea tratada de manera responsable.



Cuando una persona necesita apoyo para ejercer sus derechos, ese apoyo debe buscar que pueda participar y tomar decisiones sobre su propia información. Por eso, proteger los datos personales también significa hacer accesibles los trámites y la información.

Una misma situación puede ser más difícil para algunas personas

Imaginemos que una institución solicita llenar un formulario digital para realizar un trámite. Para una persona que utiliza internet habitualmente puede resultar sencillo, pero para alguien que no tiene acceso a internet, tiene una discapacidad visual, no sabe utilizar una computadora o enfrenta una barrera de comunicación, el mismo trámite puede convertirse en un obstáculo.

En esos casos, el problema no está necesariamente en la persona; puede estar en la forma en que se diseñó el trámite. Por eso, cuando hablamos de protección de datos personales también debemos hablar de accesibilidad.

¿Qué significa proteger los datos de una persona que necesita apoyo?

Significa, entre otras cosas, explicar de manera clara qué datos se solicitan, informar para qué serán utilizados, facilitar el acceso a los avisos de privacidad, proporcionar apoyos cuando sean necesarios, evitar pedir información que no sea necesaria, respetar las decisiones de la persona y proteger la información frente a accesos o usos indebidos.



No debemos aprovechar una situación de necesidad

Este punto es especialmente importante. Una persona que necesita un apoyo, un servicio, una atención médica o realizar un trámite puede encontrarse en una posición en la que le resulte difícil cuestionar lo que le solicitan. Por ejemplo, “dame todos tus documentos y yo hago el trámite.” La persona puede aceptar porque necesita resolver rápidamente su situación; sin embargo, eso no significa que deba perder el control sobre su información.

Siempre que sea posible, debe saber qué documentos está entregando, quién los recibirá, para qué se utilizarán, qué trámite se realizará y qué información quedará registrada.

Cuidado con los intermediarios



En ocasiones, una persona necesita que alguien más la ayude a realizar un trámite, puede ser un familiar, una persona cuidadora, un trabajador social, un representante o alguien que le brinda apoyo. La ayuda puede ser necesaria y completamente válida, pero debemos recordar una diferencia, ayudar a una persona no significa apropiarse de sus datos.

Por ejemplo, si alguien ayuda a una persona con discapacidad a realizar un trámite, debe procurar que la persona conozca qué información está proporcionando y cómo será utilizada, de acuerdo con sus posibilidades y necesidades de apoyo.

¿Qué información requiere especial cuidado?

Dependiendo de la situación de cada persona, puede existir información que revele aspectos especialmente delicados de su vida.



Tabla 6.5 Información que puede requerir especial cuidado.

Información	Ejemplo
Información médica	Enfermedades, tratamientos o medicamentos.
Información sobre discapacidad	Tipo de discapacidad o necesidades de apoyo.
Situación económica	Ingresos, deudas o necesidad de asistencia.
Información familiar	Personas que dependen de ella o que la apoyan.
Ubicación	Domicilio, refugio o lugar donde recibe atención.
Documentos de identidad	Identificaciones, CURP u otros documentos.
Información relacionada con servicios sociales	Apoyos o programas de los que recibe algún beneficio.

Fuente: elaboración propia con fines ilustrativos; la naturaleza y clasificación jurídica de cada dato dependerá de la información concreta y del contexto en que sea tratada.

Esto no significa que toda esta información sea automáticamente un dato sensible; su clasificación dependerá de lo establecido en la legislación aplicable en protección de datos personales. Lo importante para la ciudadanía es comprender que una institución debe tratar cada dato con el cuidado que corresponde y no pedir información que no necesita.

Un ejemplo: una persona con discapacidad

Imaginemos que Laura tiene una discapacidad visual y necesita realizar un trámite ante una institución pública. El procedimiento únicamente está disponible en una plataforma que no puede utilizar adecuadamente con las herramientas de accesibilidad que tiene, y Laura necesita ayuda.

Una respuesta adecuada no sería “entonces alguien más tiene que hacer el trámite por usted”. Lo correcto es buscar mecanismos que permitan que Laura pueda ejercer sus derechos y tomar sus propias decisiones, proporcionando los apoyos que sean necesarios. La protección de datos también implica respetar la autonomía de las personas y facilitar su participación.

Otro ejemplo: una persona que no sabe leer



Ahora pensemos en una persona que necesita realizar un trámite, pero no sabe leer. Le presentan un documento y le dicen “firme aquí”. La persona puede no saber qué información contiene el documento ni qué está aceptando.

En una situación así, proporcionar información clara y accesible es fundamental. No basta con entregar un documento y asumir que la persona lo comprendió; debe procurarse que conozca, de acuerdo con sus circunstancias, qué información se está solicitando y para qué será utilizada.

También hay que cuidar la información de quienes reciben ayuda

Pensemos en una persona que recibe apoyo de un programa social. La institución puede necesitar determinados datos para identificarla, verificar que cumple con los requisitos o proporcionar el servicio, pero eso no significa que toda su información pueda publicarse. Por ejemplo, no sería adecuado pensar “como recibe un apoyo, podemos publicar todos sus datos”. La información debe manejarse conforme a las reglas aplicables y únicamente para las finalidades que correspondan.

¿Qué pueden hacer las instituciones?

Las instituciones tienen una responsabilidad especialmente importante, deben procurar que sus trámites y servicios sean comprensibles y accesibles para las personas que los necesitan. Algunas medidas pueden ser utilizar lenguaje claro, evitar formatos innecesariamente complicados, ofrecer alternativas cuando una persona enfrenta una barrera de acceso, explicar los avisos de privacidad de manera sencilla, evitar solicitar datos que no sean necesarios, proteger los expedientes y documentos, capacitar al personal que tiene acceso a datos personales, respetar la autonomía de las personas y proporcionar los apoyos que correspondan.

En el ámbito de los sujetos obligados de Nuevo León, estas obligaciones deben analizarse conforme a la LPDPPSONL, además de las demás disposiciones aplicables.



¿Y qué puede hacer una persona?

No necesitas conocer la ley para comenzar a proteger tus datos. Puedes utilizar cinco preguntas:

1. **¿Qué dato me están pidiendo?** Identifica qué información estás proporcionando.
2. **¿Para qué lo necesitan?** Pregunta cuál es la finalidad.
3. **¿Quién tendrá acceso?** Conoce quién manejará la información.
4. **¿Es necesario entregarlo?** Si tienes dudas, pregunta antes de proporcionar el dato.
5. **¿Necesito apoyo?** Si una persona necesita ayuda para realizar un trámite, puede solicitarla, procurando conservar el control sobre sus decisiones y su información.

Tabla 6.6 Una protección que debe estar al alcance de todas las personas.

Situación	¿Qué debemos procurar?
La persona tiene una discapacidad	Que pueda comprender y realizar el trámite con los apoyos necesarios.
No sabe leer o escribir	Que reciba información de manera comprensible y accesible.
Tiene dificultades para utilizar internet	Que pueda contar con alternativas o apoyo para realizar el trámite.
Necesita ayuda de otra persona	Que conozca qué datos está proporcionando y para qué.
Se encuentra en una situación de emergencia	Que se soliciten únicamente los datos necesarios para atenderla.
Recibe algún apoyo o servicio	Que su información no se divulgue innecesariamente.
Tiene dificultades para comprender un aviso de privacidad	Que se le explique de manera clara y accesible.

Una idea importante "vulnerabilidad no significa incapacidad"

Esta es una distinción fundamental para esta obra. Una persona puede encontrarse en una situación de vulnerabilidad sin perder su capacidad para decidir sobre sus datos personales. Por eso, conviene evitar expresiones como “hay que decidir por estas personas” y preferir, en su lugar, “hay que proporcionarles los apoyos que necesitan para que puedan decidir”. Ese cambio aparentemente pequeño coloca a la persona en el centro.



La protección de datos también es inclusión

Cuando una institución explica un aviso de privacidad de manera sencilla, ofrece un formato accesible o proporciona apoyo para realizar un trámite, no está haciendo un favor, está contribuyendo a que una persona pueda ejercer sus derechos en condiciones más equitativas.

La protección de datos personales debe ser comprensible y accesible para todas las personas, no solamente para quienes tienen conocimientos tecnológicos o jurídicos.

Una regla fácil de recordar. “Necesitar apoyo no significa perder el control sobre tus datos.” Si necesitas ayuda, pregunta, comprende, decide y comparte solamente lo necesario. Y si eres quien brinda apoyo a otra persona, acompaña, pero respeta su información y sus decisiones.

Concepto clave. Las personas que se encuentran en una situación de mayor vulnerabilidad conservan sus derechos. Proteger sus datos personales significa brindarles información clara, accesibilidad y los apoyos que necesitan, sin quitarles el control sobre su propia información.

Para recordar. Una discapacidad no elimina el derecho a la privacidad.

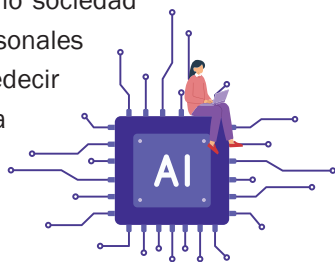
No saber utilizar internet no significa renunciar a los datos personales. Necesitar ayuda para un trámite no significa entregar el control de toda nuestra información. Recibir un apoyo no significa que nuestra información pueda hacerse pública. Por eso, la protección de datos debe estar al alcance de todas las personas.



Capítulo 7. Tecnologías emergentes y protección de datos personales

Cómo señala Mendoza Enríquez (2021), el uso cotidiano de plataformas y aplicaciones digitales genera de manera constante volúmenes de datos sobre las actividades, búsquedas y relaciones de los usuarios, sustentando el funcionamiento de los servicios actuales. La tecnología ha cambiado la manera en que vivimos. Utilizamos aplicaciones para comunicarnos, plataformas para estudiar o trabajar, servicios digitales para comprar y herramientas que nos ayudan a encontrar información, elegir una ruta o recibir recomendaciones. Muchas de estas tecnologías funcionan a partir de datos, cada vez que utilizamos un servicio digital podemos dejar información sobre lo que hacemos, qué buscamos, qué compramos, qué lugares visitamos, qué contenido consultamos o con quién nos comunicamos.

Durante la última década, han adquirido especial importancia tecnologías capaces de analizar grandes cantidades de información y encontrar patrones en ella. Entre ellas se encuentra la inteligencia artificial. Esto abre nuevas posibilidades, pero también plantea una pregunta que como sociedad debemos hacernos, ¿qué sucede con nuestros datos personales cuando una tecnología los utiliza para aprender, analizar, predecir o tomar decisiones? La respuesta no consiste en rechazar la tecnología, sino en comprender cómo funciona y saber qué información estamos proporcionando y qué puede hacerse con ella (Mendoza Enríquez, 2021).



7.1 ¿Cómo utiliza la inteligencia artificial tus datos personales?

La inteligencia artificial puede utilizar grandes cantidades de información para identificar patrones, generar resultados, hacer predicciones o apoyar determinadas tareas. No toda inteligencia artificial utiliza datos personales, algunas herramientas pueden funcionar con información que no identifica directamente a una persona, pero otras sí pueden utilizar información relacionada con personas identificadas o identificables.



Por ejemplo, una herramienta puede recibir fotografías, grabaciones de voz, textos, datos de ubicación, información de una cuenta, preferencias, historial de navegación, información de compras, documentos, o cualquier otro dato que una persona proporcione al utilizar un servicio. Por eso, antes de utilizar una herramienta basada en inteligencia artificial, conviene hacerse una pregunta sencilla, ¿qué información le estoy dando?

Una fotografía también es información

Imaginemos que una persona utiliza una aplicación que permite modificar fotografías. Sube una fotografía personal y solicita “cambia el fondo y mejora



la iluminación”. Desde la perspectiva del usuario, parece que solamente está editando una imagen; sin embargo, para realizar esa tarea la herramienta

puede recibir la fotografía original.

La pregunta entonces cambia, ¿qué ocurre con esa fotografía después de utilizarla? Dependiendo del servicio, puede existir información sobre cómo se utiliza, cuánto tiempo se conserva y con qué finalidad. Por eso es importante revisar las condiciones y el aviso de privacidad de la aplicación antes de proporcionar información personal.

La inteligencia artificial aprende de la información

Como se mencionó anteriormente, la inteligencia artificial tiene la capacidad para analizar grandes cantidades de información. Imaginemos que una



plataforma recibe información de millones de interacciones, a partir de esos datos puede encontrar patrones, por ejemplo, que muchas personas que buscan determinados productos también consultan determinadas páginas, o que personas con ciertos intereses suelen interactuar con determinado tipo de contenido.

Estos patrones pueden utilizarse para ofrecer recomendaciones, organizar información o personalizar un servicio. Cuando esos datos están relacionados con una persona identificada o identificable, entra en juego la protección de sus datos personales.

¿La inteligencia artificial puede “conocerte”?



No en el sentido humano de la palabra. Pero una herramienta puede analizar suficiente información sobre nuestras actividades como para identificar patrones relacionados con nuestros intereses o comportamiento. Por ejemplo, una plataforma puede detectar que una persona consulta frecuentemente determinado tipo de contenido, busca ciertos productos, utiliza una aplicación a determinadas horas, suele consultar información desde determinados lugares, o interactúa repetidamente con ciertos temas. A partir de ello puede generar predicciones o recomendaciones, lo que explica por qué algunas plataformas parecen “saber” qué nos interesa.

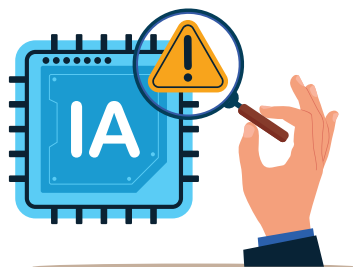
Un ejemplo de la vida cotidiana

Durante varios días buscas información sobre bicicletas en diversas plataformas de comercio electrónico; posteriormente, comienzas a ver anuncios, recomendaciones o videos relacionados con bicicletas. Puede parecer casualidad, pero también puede ser consecuencia de que la plataforma registró determinadas actividades y utilizó esa información para personalizar el contenido que te muestra.

Aquí aparece una cuestión importante, ya que nuestros datos no solamente sirven para identificarnos, sino que también pueden utilizarse para conocer nuestros hábitos y preferencias.

¿Qué debemos cuidar?

Cuando una herramienta de inteligencia artificial solicita información personal, conviene preguntarse qué datos está solicitando, si realmente los necesita, para qué los utilizará, quién tendrá acceso a ellos, durante cuánto tiempo los conservará y si es posible utilizar el servicio sin proporcionar información adicional. Estas preguntas son especialmente importantes cuando se trata de información sensible o de documentos que contienen numerosos datos personales.





No todo debe introducirse en una herramienta de inteligencia artificial

Una regla sencilla que puede evitar muchos problemas consiste en no introducir en una herramienta información personal que no sea necesario compartir. Por ejemplo, si necesitas que una herramienta te ayude a redactar un texto, tal vez no sea necesario proporcionar nombres completos, domicilios, números telefónicos, números de identificación o información médica de otras personas. Antes de compartir un documento, puedes preguntarte si es posible quitar los datos personales y obtener el mismo resultado; si la respuesta es sí, hacerlo puede ser una buena medida de protección.

¿Y qué ocurre con los datos personales de otras personas?

En este punto, también es importante recordar que no solo debemos cuidar nuestros propios datos personales. Un expediente, una fotografía, una conversación o un documento pueden contener datos de otras personas, introducir esa información en una herramienta de inteligencia artificial implica realizar operaciones de tratamiento sobre esos datos.

Por ello, antes de hacerlo, es necesario preguntarse sobre aspectos como si está permitido utilizar esos datos de esta manera, para qué se utilizarán y qué medidas deben adoptarse para protegerlos. En el caso de los sujetos obligados, además, el tratamiento debe estar vinculado con sus atribuciones y finalidades y cumplir los principios, deberes y obligaciones establecidos en la legislación aplicable. En otras palabras, utilizar una herramienta de inteligencia artificial no elimina las obligaciones de protección de datos personales. Los datos de otras personas también deben protegerse.

Inteligencia artificial y decisiones

Otra cuestión importante aparece cuando una herramienta de inteligencia artificial se utiliza para apoyar decisiones relacionadas con personas, por ejemplo, para analizar información y ayudar a identificar determinados patrones. Cuando los datos personales se utilizan de esta manera, resulta especialmente importante saber qué información se está utilizando, para

qué se utiliza, quién toma la decisión final y qué ocurre si la información es incorrecta. La tecnología puede ayudar a procesar información, pero eso no elimina las obligaciones relacionadas con la protección de datos personales.

Una idea importante

La inteligencia artificial no convierte los datos personales en información "sin dueño". Si una persona proporciona información personal, siguen existiendo obligaciones respecto de su tratamiento conforme a la legislación aplicable. En México, el tratamiento de datos personales por los sujetos obligados debe observar las disposiciones establecidas en la LGPDPPSO (2025) y, en el ámbito estatal correspondiente, en la LPDPPSONL (2019).

En pocas palabras. La inteligencia artificial puede utilizar datos para encontrar patrones, generar resultados o personalizar servicios. Por eso, antes de compartir información personal con una herramienta de este tipo, conviene saber qué datos estamos proporcionando y para qué serán utilizados.

7.2 ¿Qué es el perfilamiento y por qué influye en lo que ves en internet?

¿Alguna vez has buscado un producto y poco después has comenzado a encontrar contenido relacionado con él? ¿Has visto recomendaciones de videos parecidos a los que acabas de consultar? ¿Una plataforma parece saber qué temas te interesan? Esto puede estar relacionado con el perfilamiento.

En términos sencillos, el perfilamiento consiste en utilizar datos personales para evaluar determinados aspectos de una persona, como sus intereses, preferencias o comportamiento y, a partir de ello, generar información que permita conocer o predecir determinadas características sobre ella. Este tipo de tratamiento puede utilizarse para distintas finalidades, como personalizar servicios, ofrecer recomendaciones o mostrar determinado contenido (Reglamento General de Protección de datos (UE) [RGPD], art. 4).





¿Cómo se construye un perfil?

Imaginemos que durante una semana utilizas una plataforma. En ese tiempo buscas información sobre viajes, consultas hoteles, miras videos sobre destinos turísticos y lees opiniones sobre vuelos. La plataforma puede reunir información sobre esas actividades, no necesariamente sabe exactamente qué estás pensando, pero puede identificar un patrón, por ejemplo, que esa persona parece estar interesada en viajar. A partir de ese patrón puede mostrarte más contenido relacionado con viajes. Esa es una forma sencilla de entender cómo puede funcionar el perfilamiento.

Lo que haces en internet deja señales...
Cada actividad digital puede generar información.

Tabla 7.1 Actividades digitales y lo que pueden revelar.

Actividad	¿Qué puede revelar?
Buscar un producto	Posibles intereses de compra
Ver determinados videos	Temas de interés
Consultar una ubicación	Lugares que interesan o frecuentan
Utilizar una aplicación	Hábitos de uso
Realizar una compra	Preferencias de consumo
Interactuar con contenido	Temas que llaman nuestra atención

Una sola actividad puede decir poco, pero cuando se analizan muchas actividades juntas, pueden aparecer patrones.

¿Por qué importa?

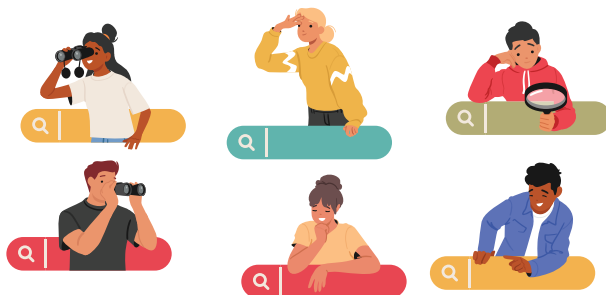
Porque el perfilamiento puede influir en lo que vemos. Dos personas pueden utilizar la misma plataforma y recibir recomendaciones diferentes, porque sus actividades anteriores pueden ser distintas, una persona que consulta frecuentemente información deportiva puede recibir más contenido deportivo; otra que busca recetas puede recibir recomendaciones

relacionadas con cocina; otra que consulta información sobre viajes puede recibir contenido relacionado con destinos turísticos.

Esto puede ser útil, pero también es importante saber que lo que vemos en internet no necesariamente representa todo lo que existe.

Internet no siempre te muestra “todo”

Imagina que buscas información sobre un tema y la plataforma comienza a mostrarte contenidos similares. Después de un tiempo puedes tener la impresión de que “esto es lo que todo el mundo está viendo”, pero puede no ser así, es posible que la plataforma esté seleccionando información de acuerdo con determinados criterios, entre ellos nuestras actividades anteriores. Por eso es recomendable consultar diferentes fuentes, comparar información, no depender de una sola plataforma y mantener una mirada crítica sobre las recomendaciones que recibimos.



El análisis de tus datos puede ocurrir sin que lo notes

Cuando utilizamos internet, muchas veces no podemos ver cómo se analiza la información que generamos. Las búsquedas que realizamos, los contenidos que consultamos y nuestras preferencias pueden ser analizados para identificar patrones y mostrarnos contenidos, recomendaciones o publicidad relacionados con nuestros intereses.

Por ejemplo, una persona que busca información sobre viajes puede comenzar a recibir recomendaciones de hoteles, vuelos o destinos similares. La persona únicamente observa lo que aparece en su pantalla, sin necesariamente saber qué información de su actividad fue tomada en cuenta para generar esas recomendaciones.



Por eso, podemos ver el resultado del análisis sin conocer qué información fue utilizada ni cómo se llegó a ese resultado.

En materia de protección de datos personales, la legislación establece reglas específicas para determinados tratamientos automatizados. En Nuevo León, la ley regula aquellos que, bajo las condiciones previstas en ella, pueden utilizarse para evaluar, analizar o predecir determinados aspectos personales (LPDPPSONL, 2019, art. 57, fracción II).

Un ejemplo de la vida cotidiana

Supongamos que Pedro busca durante varios días información sobre cámaras fotográficas. Después comienza a recibir recomendaciones de cámaras, lentes, cursos de fotografía, accesorios y videos sobre fotografía. Pedro puede pensar que su teléfono lo está escuchando, pero no necesariamente es así, la plataforma puede estar utilizando información sobre sus búsquedas, páginas consultadas o interacciones para identificar que existe un interés por la fotografía. Ese es uno de los efectos que puede producir el perfilamiento.

¿Podemos evitar completamente el perfilamiento?

No siempre. Dependiendo del servicio que utilicemos, algunas funciones pueden requerir determinados datos para personalizar la experiencia. Pero sí podemos adoptar medidas para tener mayor control sobre nuestra información, revisar las opciones de privacidad, limitar los permisos que no sean necesarios, evitar proporcionar información que no necesitamos compartir, revisar las cuentas que mantenemos activas, consultar los avisos de privacidad, utilizar diferentes fuentes de información y pensar antes de aceptar una solicitud de datos. No se trata de dejar de utilizar internet, sino de utilizarlo con mayor conocimiento.

Una pregunta que vale la pena hacerse

La próxima vez que una plataforma te muestre una recomendación, pregúntate por qué la estás viendo. Tal vez sea una coincidencia, tal vez corresponda a tus búsquedas anteriores, tal vez esté relacionado con tus



intereses, o puede responder a otros criterios utilizados por la plataforma. La pregunta ayuda a recordar algo importante, lo que aparece en nuestra pantalla también puede ser resultado de la información que hemos generado.

Un pequeño ejercicio puede ayudarte a comprobarlo, durante un día, observa las recomendaciones que recibes en internet y pregúntate qué buscaste recientemente, qué videos viste, qué productos consultaste y qué temas te interesaron. Después observa si las recomendaciones que recibes tienen alguna relación con esas actividades. El objetivo no es generar desconfianza, sino aprender a reconocer cómo nuestros datos pueden influir en nuestra experiencia digital.

Para recordar. Tus datos pueden ayudar a una plataforma a conocerte mejor, identificar tus intereses y decidir qué contenido mostrarte. Por eso, proteger los datos personales no significa solamente evitar que alguien conozca nuestro nombre o domicilio; también significa comprender qué información sobre nuestros hábitos y preferencias estamos generando y cómo puede utilizarse.

7.3 Cómo proteger tus datos frente a amenazas digitales

Desde el teléfono podemos comunicarnos, consultar información, realizar compras, utilizar servicios bancarios, estudiar, trabajar y mantener contacto con familiares y amistades. Todo esto resulta práctico, pero también significa que una parte importante de nuestra información circula por medios digitales.



Por eso, proteger nuestros datos personales no consiste únicamente en tener una contraseña. Se trata de desarrollar hábitos que reduzcan las posibilidades de que nuestra información llegue a manos de quien no debería tenerla.

El riesgo puede comenzar con algo muy sencillo

Imaginemos que recibes un mensaje, “Detectamos un problema con tu cuenta. Entra aquí para solucionarlo.” El mensaje incluye un enlace y parece provenir de una institución conocida. La reacción más común puede ser abrirlo inmediatamente, pero antes de hacerlo conviene detenerse

y preguntarse si esperabas ese mensaje, si conoces a quien lo envió, si el enlace realmente pertenece a la institución y si te están pidiendo información que normalmente no solicitan. Una pausa de unos segundos puede evitar que entreguemos información personal sin darnos cuenta.

No todo mensaje merece una respuesta inmediata

Algunas situaciones digitales buscan generar preocupación, curiosidad o urgencia con mensajes como “tu cuenta será suspendida”, “tienes un pago pendiente”, “ganaste un premio”, “tu paquete no pudo ser entregado” o “alguien intentó ingresar a tu cuenta”. El problema no está necesariamente en que el mensaje sea verdadero o falso; el problema es actuar sin verificar. Una regla sencilla puede ayudarnos, si un mensaje te presiona para actuar inmediatamente, detente y verifica.

Las contraseñas son una primera barrera

Una contraseña protege una cuenta, pero utilizar una contraseña sencilla o repetirla en todos los servicios aumenta el riesgo. Por ejemplo, si utilizamos la misma contraseña para el correo electrónico, las redes sociales, las compras y la banca electrónica, y esa contraseña llega a manos de otra persona, varias cuentas podrían quedar comprometidas.

Por eso es recomendable utilizar contraseñas diferentes para servicios importantes y evitar aquellas que puedan adivinarse fácilmente. También es conveniente activar, cuando el servicio lo permita, un segundo método de comprobación para ingresar a la cuenta; de esta manera, una contraseña por sí sola no será suficiente para acceder.

No compartas códigos de seguridad



Una situación frecuente ocurre cuando alguien solicita el código que acaba de llegar al teléfono para “confirmar que es usted”. Ese código puede ser precisamente la herramienta que permite entrar a una cuenta. Por eso, un código de seguridad es personal, si alguien te lo solicita inesperadamente por teléfono, mensaje o correo, no debes compartirlo sin verificar directamente con la institución correspondiente.



Cuidado con las redes sociales

Las redes sociales permiten compartir fotografías, lugares, actividades y momentos importantes, pero cada publicación puede revelar información. Una fotografía de vacaciones puede indicar que una familia está fuera de casa; una publicación sobre una escuela puede revelar dónde estudia una niña o un niño; una fotografía tomada frente a un domicilio puede mostrar la ubicación; una publicación sobre una rutina diaria puede revelar horarios.

No significa que debamos dejar de compartir. Significa que antes de publicar podemos preguntarnos qué información estamos revelando además de lo que queremos mostrar.

Mantén actualizados tus dispositivos

Las actualizaciones no solamente incorporan nuevas funciones; también pueden corregir problemas de seguridad. Por eso es recomendable mantener actualizado el teléfono celular, la computadora, las aplicaciones, el navegador de internet y otros dispositivos conectados. También conviene descargar aplicaciones únicamente desde sitios o tiendas oficiales y revisar los permisos que solicitan.

No todas las aplicaciones necesitan conocer todo sobre ti

Cuando instalamos una aplicación, puede solicitar acceso a determinadas funciones del teléfono, por ejemplo, ubicación, cámara, micrófono, contactos o fotografías. Antes de aceptar, podemos preguntarnos si esa aplicación realmente necesita ese acceso para funcionar. Si una aplicación para consultar información no necesita conocer nuestra ubicación permanente, quizá no sea necesario otorgarle ese permiso. Revisar periódicamente los permisos de las aplicaciones también es una buena práctica.

Protege tus documentos

Hoy es común enviar fotografías o copias de documentos mediante aplicaciones de mensajería, y una identificación oficial puede contener numerosos datos personales. Antes de enviarla, pregunta si realmente necesitan una copia, para qué la utilizarán, a quién se la estás enviando

y si estás utilizando un medio seguro. Cuando sea posible, evita compartir documentos completos si no son necesarios.

¿Qué hacer si algo ya ocurrió?

No siempre podemos evitar todos los incidentes. Si una persona cree que sus datos pudieron quedar expuestos, lo importante es actuar con rapidez. Dependiendo de la situación, puede ser necesario cambiar contraseñas, cerrar sesiones abiertas, activar medidas adicionales de seguridad, comunicarse con la institución correspondiente, revisar movimientos de cuentas, conservar mensajes o evidencias, y solicitar orientación sobre las acciones que correspondan. Lo importante es no ignorar el problema.

Cinco hábitos que pueden proteger tus datos

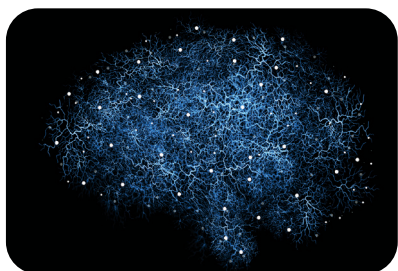
1. Piensa antes de hacer clic.
2. No compartas contraseñas ni códigos de seguridad.
3. Utiliza contraseñas diferentes en cuentas importantes.
4. Revisa qué información compartes en internet.
5. Verifica quién solicita tus datos y para qué los necesita.

Fuente: Elaboración propia con base a las recomendaciones para una ciberseguridad efectiva emitida por el Gobierno de México.

Son acciones sencillas, pero pueden hacer una diferencia importante.

Una idea para llevar contigo. La seguridad digital no depende de saber de tecnología. Muchas veces comienza con algo tan sencillo como detenerse, preguntar y verificar antes de compartir información.

7.4 Neurodatos, cuando la tecnología puede conocer lo que piensas



Hasta hace algunos años, hablar de tecnologías capaces de obtener información relacionada con la actividad cerebral podía parecer propio de una película de ciencia ficción. Hoy existen tecnologías que permiten registrar y analizar señales producidas por la actividad cerebral para realizar determinadas funciones.



Una de ellas son las interfaces cerebro-computadora, sistemas que permiten establecer una comunicación entre la actividad cerebral y un dispositivo. En términos sencillos, una persona genera determinadas señales cerebrales, estas son captadas por sensores y posteriormente procesadas por una computadora para identificar patrones y convertirlos en una acción.

En México existen investigaciones sobre este tipo de tecnologías. El Instituto Nacional de Rehabilitación ha documentado trabajos relacionados con interfaces cerebro-computadora para aplicaciones de rehabilitación, mientras que el Tecnológico de Monterrey ha desarrollado investigaciones en las que se utilizan señales obtenidas mediante electroencefalografía para controlar dispositivos.

¿Qué son los neurodatos?

Podemos utilizar el término neurodatos para referirnos a la información obtenida a partir de la medición, registro o análisis de señales relacionadas con la actividad o el funcionamiento del sistema nervioso, particularmente del cerebro.

Sin embargo, es importante hacer una precisión, el hecho de que una información provenga de la actividad cerebral no significa, por sí mismo, que constituye automáticamente una nueva categoría jurídica de datos personales.

¿Pueden saber lo que estás pensando?

Las tecnologías actuales no deben entenderse como herramientas capaces de leer libremente todos los pensamientos de una persona. Lo que determinadas tecnologías pueden hacer es registrar señales de la actividad cerebral y procesarlas para identificar patrones específicos. Algunas investigaciones han utilizado estas señales para que una persona pueda controlar dispositivos mediante su actividad cerebral.

También existen investigaciones que buscan identificar determinadas palabras imaginadas a partir de señales cerebrales. Para la protección de datos personales, lo importante no es solamente preguntarnos si una tecnología puede “leer la mente”, sino qué información puede obtener,



cómo se procesa, para qué se utiliza y qué información adicional puede revelar o permitir inferir sobre una persona.

¿Por qué los neurodatos son importantes para la privacidad?

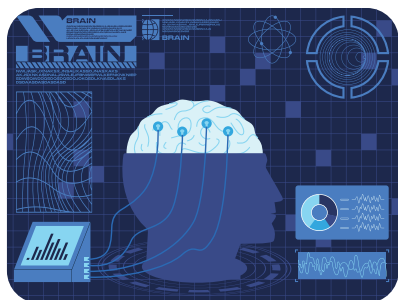
Los neurodatos son importantes para la privacidad no únicamente por su origen en la actividad del sistema nervioso, sino por la información que pueden revelar o permitir inferir sobre una persona.

Dependiendo de la tecnología utilizada y de la forma en que sean tratados, estos datos pueden relacionarse con aspectos como el estado de salud, determinadas características fisiológicas o respuestas ante distintos estímulos. Además, su análisis y combinación con otras fuentes de información podría permitir generar perfiles o inferencias sobre una persona, incluso respecto de aspectos que esta no proporciona directamente.

En este sentido, el principal desafío no se encuentra solamente en la obtención de una señal relacionada con la actividad cerebral, sino también en lo que puede ocurrir después; su almacenamiento, análisis, correlación con otros datos y utilización para generar nueva información.

Especialistas de la Universidad Nacional Autónoma de México han advertido que los neurodatos pueden adquirir un valor significativo precisamente por su potencial para elaborar perfiles de las personas y han señalado la importancia de cuestionar quien obtiene esta información, para qué la utiliza y cuáles son las consecuencias de su tratamiento.

Por ello, la protección de la privacidad exige analizar no solo qué información se obtiene inicialmente, sino también que puede revelarse o inferirse a partir de ella.



Un ejemplo para entenderlo

Imaginemos que una persona participa en un estudio realizado por una institución de salud que utiliza una tecnología capaz de registrar determinadas señales relacionadas con su actividad cerebral. Para participar, la persona proporciona sus datos personales y acepta



que la información obtenida sea utilizada exclusivamente para los fines informados en el estudio.

Durante el estudio se generan registros relacionados con su actividad cerebral. Estos registros pueden estar vinculados con su nombre, expediente, resultados médicos u otros datos que permitan identificarla. Posteriormente, la institución pretende utilizar esos registros para una finalidad diferente a la que originalmente informó a la persona.

Aquí entra directamente la protección de datos personales.

La institución tendría que analizar si ese nuevo tratamiento está permitido y si cuenta con la base jurídica correspondiente. También tendría que considerar aspectos como la finalidad para la que fueron obtenidos los datos, la información proporcionada a la persona, la naturaleza de los datos tratados, las medidas de seguridad aplicables y las demás obligaciones previstas por la legislación.

El punto importante es que no basta con preguntarnos qué puede hacer la tecnología. Desde la perspectiva de protección de datos personales, debemos preguntarnos qué datos se están obteniendo, para qué se obtienen, cómo se utilizan, quién tiene acceso a ellos y si pueden utilizarse para una finalidad diferente.

Este ejemplo permite entender por qué los neurodatos representan un reto para la protección de datos personales, una tecnología puede obtener información relacionada con la actividad cerebral y, mediante su tratamiento, generar o revelar información adicional sobre una persona. Por ello, cada caso debe analizarse conforme a la legislación aplicable y a las circunstancias concretas del tratamiento.

La protección de los neurodatos plantea nuevos desafíos

La tecnología avanza más rápido que nuestra capacidad para imaginar todos sus posibles usos. Por eso, la protección de datos personales debe mantenerse atenta a estos nuevos escenarios, una tecnología puede evolucionar de tal manera que información que hoy parece limitada pueda adquirir nuevos usos mañana. Esto hace todavía más importante aplicar los principios y deberes, así como las demás obligaciones que se encuentran



establecidos en la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Nuevo León.

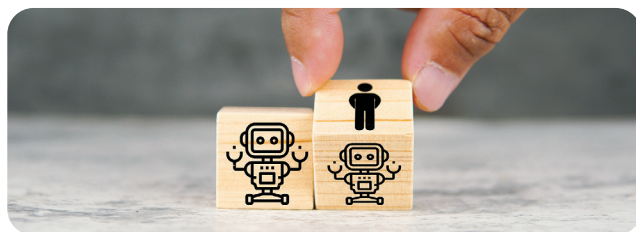
En el ámbito de los sujetos obligados de Nuevo León, la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Nuevo León establece que el tratamiento debe estar relacionado con las atribuciones correspondientes y que las finalidades deben ser concretas, lícitas, explícitas y legítimas; también establece la obligación de adoptar medidas de seguridad para proteger los datos frente a accesos o tratamientos no autorizados.

¿Qué debería preguntarse una persona?

Si alguna vez utilizamos una tecnología que recopila información relacionada con nuestra actividad cerebral, sería razonable preguntar qué información está obteniendo, para qué la necesita, quién tendrá acceso, cuánto tiempo será conservada, si puede utilizarse para otra finalidad y cómo está protegida. Estas preguntas pueden parecer adelantadas para una tecnología que todavía se encuentra en desarrollo, pero precisamente por eso son importantes.

La tecnología no debe estar por encima de la persona

El desarrollo tecnológico puede mejorar la vida de muchas personas, puede ayudar a quienes tienen determinadas condiciones de salud, facilitar la comunicación o abrir nuevas posibilidades de interacción con dispositivos. El objetivo de la protección de datos no debe ser detener esos avances, sino procurar que el desarrollo tecnológico avance respetando los derechos de las personas. En otras palabras, la innovación debe estar al servicio de las personas, no las personas al servicio de la tecnología.





Un nuevo tipo de privacidad

Durante mucho tiempo pensamos en privacidad principalmente como “que nadie entre a mi casa”. Después aprendimos que también significa “que nadie conozca información sobre mi vida sin una razón válida”. Ahora la tecnología nos obliga a hacernos una pregunta todavía más profunda, ¿cómo protegemos la información relacionada con nuestra propia actividad cerebral? Este es uno de los desafíos que las nuevas tecnologías plantean para la protección de datos personales.

Para cerrar el capítulo

La inteligencia artificial, el perfilamiento y las tecnologías relacionadas con el cerebro pueden parecer temas alejados de nuestra vida cotidiana, pero todos tienen algo en común, utilizan información para conocer, analizar, predecir o interactuar con las personas. Por eso, proteger nuestros datos en la era digital no significa tener miedo a la tecnología, sino comprenderla lo suficiente para tomar decisiones informadas.

Hoy puede tratarse de una fotografía; mañana, de una conversación; después, de nuestros hábitos; y en el futuro, de información relacionada con nuestra propia actividad cerebral. La pregunta que debemos mantener vigente es siempre la misma, centrada en evaluar qué información estoy proporcionando y qué puede hacerse con ella.



BLOQUE III.

TU PODER DE DEFENSA

Capítulo 8. Tus derechos sobre tus datos personales

Hasta ahora hemos hablado de qué son los datos personales, por qué tienen valor, quién puede utilizarlos y qué podemos hacer para protegerlos. Pero existe una pregunta todavía más importante, relacionada con qué puedo hacer si quiero saber qué datos tienen sobre mí, necesito corregirlos o ya no quiero que los utilicen. La respuesta está en nuestros derechos.

La protección de datos personales no consiste solamente en pedir a las instituciones que cuiden nuestra información; también significa que cada persona tiene derechos que puede ejercer respecto de sus propios datos personales. En México, estos derechos permiten a las personas conocer qué información se tiene sobre ellas, solicitar que se corrija cuando sea incorrecta, pedir su eliminación cuando corresponda y oponerse a determinados usos.

En el ámbito de los sujetos obligados, estos derechos se encuentran reconocidos en la LGPDPPSO y, para el ámbito estatal de Nuevo León, en la LPDPPSONL.



8.1 ¿Qué son los derechos ARCOP?

La palabra ARCOP reúne cinco derechos relacionados con nuestros datos personales.

Tabla 8.1 Los cinco derechos ARCOP.

Acrónimo	Derecho	En pocas palabras
A	Acceso	Saber qué datos personales tienen sobre mí y conocer información relacionada con su tratamiento.
R	Rectificación	Pedir que corrijan mis datos cuando sean incorrectos, incompletos o inexactos.
C	Cancelación	Solicitar que mis datos sean eliminados de los registros cuando corresponda.
O	Oposición	Pedir que mis datos no sean utilizados para determinados fines, cuando proceda.
P	Portabilidad	Solicitar que determinados datos personales puedan ser obtenidos y, cuando corresponda, transmitidos en los términos previstos por la legislación mexicana en materia de Protección de Datos Personales.

Fuente: Elaboración propia con base en LPDPPSONL (2019), LGPDPPSO (2025) y LFPDPPP (2025).

Una forma sencilla de recordarlos: **A)** quiero saber qué tienen de mí; **R)** quiero corregir lo que está mal; **C)** quiero que eliminen mis datos cuando corresponda; **O)** no quiero que los utilicen para determinada finalidad; **P)** quiero obtener o trasladar determinados datos cuando la ley lo permita.

Estos derechos no son favores que una institución concede, son derechos de las personas.



¿Por qué existen estos derechos?

Porque nuestros datos pueden cambiar. Podemos mudarnos de domicilio, cambiar de teléfono, corregir un error en nuestro nombre o actualizar determinada información. También pueden existir datos que ya no deban conservarse para una finalidad determinada, o situaciones en las que una persona tenga razones legítimas para oponerse a un tratamiento. Los derechos ARCOP permiten que las personas tengan una participación más activa respecto de la información que les pertenece; por eso podemos pensar en ellos como una especie de herramienta de control sobre nuestros datos.

8.2 Derecho de Acceso



El derecho de acceso responde a una pregunta muy sencilla, la cual es ¿qué datos personales tienen sobre mí? Pero no se limita necesariamente a conocer una lista de datos, sino que también permite conocer información relacionada con las condiciones y generalidades del tratamiento

de esos datos, en los términos establecidos por la legislación aplicable (LGPDPPO, 2025, art. 38; LPDPPSONL, 2019, art. 53).

Por ejemplo, una persona puede querer saber qué información personal conserva una institución sobre ella. Puede tratarse de datos contenidos en un expediente, una solicitud, un registro, una base de datos, un trámite o un servicio que haya recibido.

Un ejemplo de la vida cotidiana

Imaginemos que Mariana realizó un trámite ante una institución pública. Tiempo después se da cuenta de que quiere saber qué información personal quedó registrada. Puede ejercer su derecho de acceso para conocer los datos personales que obran en poder de la institución y obtener la información que corresponda conforme a la legislación.

No necesita ser abogada para hacerlo, ni conocer el nombre técnico de la base de datos donde se encuentra su información. Lo importante es poder identificar qué datos busca y ante qué institución se encuentran.



¿Qué puedo conocer mediante el derecho de acceso?

En términos ciudadanos, este derecho permite preguntar qué datos personales tienen sobre mí, para qué los utilizan, cómo obtuvieron esos datos y con quién los comparten, cuando corresponda. La información específica que debe proporcionarse y las condiciones para ejercer este derecho se encuentran determinadas por la legislación mexicana vigente de protección de datos personales. Por eso, el derecho de acceso es mucho más que recibir una copia de un documento, es una oportunidad para conocer qué sucede con nuestra información personal.

El derecho de acceso no es lo mismo que pedir información pública

Aquí es importante hacer una distinción que puede evitar confusiones. Si una persona quiere conocer cómo ejerce el presupuesto una institución pública, está buscando información pública. Pero si pregunta qué datos personales tiene esa dependencia sobre ella, está ejerciendo un derecho relacionado con la protección de sus datos personales. Son derechos diferentes, aunque ambos buscan que las personas puedan conocer información.

Una forma sencilla de distinguirlos, mientras la información pública responde a “quiero saber qué hace una institución con recursos y asuntos públicos”; los datos personales responden a “quiero saber qué información tiene una institución sobre mí”. Esta diferencia será importante cuando, en capítulos posteriores, expliquemos ante quién y cómo ejercer cada derecho.

¿Para qué sirve conocer nuestros datos?

Porque podemos encontrar información incorrecta, desactualizada o que no reconocemos. Imaginemos que una institución tiene registrado un número telefónico que ya no utilizamos, o que aparece un domicilio anterior, o que encontramos información que no reconocemos. Si no sabemos qué información tiene una institución, difícilmente podremos pedir que sea corregida o ejercer otros derechos cuando corresponda. Por eso, el derecho de acceso puede ser el primer paso para tomar el control de nuestra información.

No necesitas utilizar palabras complicadas, puedes comenzar con una pregunta sencilla, “¿qué datos personales tienen sobre mí y para qué los utilizan?”. A partir de ahí puede comenzar el ejercicio de tus derechos.

Los derechos ARCOP están relacionados

Aunque cada derecho tiene una finalidad distinta, pueden estar conectados. Por ejemplo, María ejerce su derecho de acceso y descubre que su domicilio está registrado incorrectamente; entonces puede solicitar la rectificación. En otro caso, puede considerar que ya no corresponde conservar determinados datos y solicitar su cancelación, si se cumplen las condiciones legales. O puede existir una situación en la que tenga razones para solicitar la oposición a determinado tratamiento. Por eso, conocer nuestros datos es muchas veces el primer paso.

Una idea para recordar. Tus datos personales hablan de ti. El derecho de acceso te permite saber qué información tiene una institución sobre ti y conocer cómo se utiliza, en los términos que establece la ley.

Lo que viene. Conocer nuestros datos es importante, pero no siempre es suficiente. ¿Qué ocurre si encontramos un error? ¿Qué podemos hacer si nuestro nombre está mal escrito, el domicilio está desactualizado o algún dato es incorrecto? Ahí entra el siguiente derecho: el derecho de rectificación, que nos permite pedir que nuestros datos sean correctos. Y en el capítulo 9 daremos el siguiente paso, al explicar cómo ejercer los derechos ARCOP de manera sencilla, paso a paso, para que el lector no solamente conozca sus derechos, sino que sepa qué hacer cuando necesite utilizarlos.

8.3 Derecho de Rectificación

Los datos personales pueden cambiar con el tiempo. También puede ocurrir que una institución tenga registrada información incorrecta, incompleta o que ya no corresponda con la realidad. Imaginemos que una persona cambia de domicilio y, meses después, descubre que una institución todavía tiene registrado su domicilio anterior, o que su nombre aparece escrito de manera incorrecta, o que un número telefónico que ya no utiliza continúa asociado a sus datos.





En situaciones como estas existe el derecho de rectificación. En palabras sencillas, el derecho de rectificación permite solicitar que nuestros datos personales sean corregidos cuando son incorrectos, inexactos o están incompletos, de acuerdo con las condiciones previstas en la legislación mexicana en materia de protección de datos personales.

¿Por qué es importante que nuestros datos sean correctos?

Un dato incorrecto puede tener consecuencias que van mucho más allá de un simple error en un registro. Por ejemplo, una persona que está por pensionarse puede descubrir que no aparecen registradas todas las semanas que ha cotizado. Si esa información permanece incompleta o incorrecta, podría afectar la determinación de los derechos que le correspondan y, en su caso, el monto de la pensión que recibirá. En otras palabras, un dato que parece pequeño puede representar una diferencia importante en el dinero que una persona recibirá durante su retiro. Por eso, cuando detectamos que nuestros datos son incorrectos o están incompletos, solicitar su rectificación puede ser fundamental para que la información utilizada en un trámite corresponda con nuestra situación real.

Un ejemplo de la vida cotidiana

Supongamos que Carlos realizó un trámite ante una institución pública. Al consultar posteriormente la información relacionada con sus datos personales, descubre que su apellido está escrito incorrectamente. Carlos puede solicitar la rectificación correspondiente y proporcionar la información que permita acreditar cuál es el dato correcto, conforme a las reglas aplicables. No está pidiendo un favor, está ejerciendo un derecho.

¿Cuándo puede ser necesario rectificar un dato?

Puede ocurrir, por ejemplo, cuando el nombre está escrito incorrectamente, el domicilio cambió, el número telefónico está desactualizado, existe un error en algún dato registrado, la información está incompleta, o las circunstancias de la persona cambiaron y corresponde actualizar determinada información.



Pero es importante recordar algo, no todo dato que no nos gusta puede simplemente eliminarse o modificarse. La rectificación tiene como finalidad que la información personal sea correcta, completa y actualizada cuando corresponda, no cambiar información únicamente porque el resultado no sea de nuestro agrado.

Rectificar no significa borrar

Esta diferencia es importante. Si encontramos un error en nuestros datos, lo que buscamos es que el dato sea corregido; por ejemplo, de “José Martínez” (incorrecto) a “José Martínez López” (correcto). En este caso, la finalidad es corregir la información, no eliminarla. Por eso podemos recordar, rectificación es corregir.

¿Qué debo hacer si encuentro un error?

Lo primero es identificar qué dato está incorrecto, después cuál es el dato correcto y, finalmente, qué institución tiene registrada esa información. En el siguiente capítulo veremos cómo presentar una solicitud y qué información puede ser necesaria para ejercer este derecho.

Para recordar. Si una institución tiene un dato personal incorrecto o incompleto sobre ti, puedes solicitar que sea rectificado cuando se cumplan las condiciones establecidas por la ley.

8.4 Derecho de Cancelación

Hay información que puede ser necesaria para realizar un trámite o proporcionar un servicio. Pero también existen situaciones en las que una persona puede considerar que sus datos personales ya no deben continuar siendo utilizados o conservados para determinada finalidad. Para estos casos existe el derecho de cancelación.

En términos sencillos, el derecho de cancelación permite solicitar que los datos personales sean eliminados de los registros o bases de datos cuando corresponda conforme a la legislación mexicana en materia de protección de datos personales. Pero aquí es necesario hacer una precisión importante: pedir la cancelación no significa que todos los datos tengan que eliminarse



inmediatamente. Existen situaciones en las que una institución está obligada a conservar determinada información durante un periodo establecido por una disposición legal, por razones administrativas, históricas, fiscales, judiciales o de otra naturaleza. Por eso, la cancelación debe analizarse de acuerdo con cada caso.



Un ejemplo de la vida cotidiana

Imaginemos que una persona realiza un trámite ante una institución pública del Estado de Nuevo León y proporciona sus datos personales para llevarlo a cabo. Tiempo después, considera que determinada información ya no debe continuar utilizándose para esa finalidad y solicita su cancelación. La institución deberá analizar si se cumplen las condiciones para que la cancelación proceda, conforme a la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Nuevo León.

Si legalmente corresponde cancelar los datos, deberá realizar las acciones previstas en dicha ley. Sin embargo, si existe una disposición jurídica que obligue a conservar determinada información durante un periodo, esta no podrá eliminarse simplemente porque la persona lo solicite.

Cancelar no es lo mismo que rectificar.

Tabla 8.2 Rectificación y cancelación.

Derecho	¿Qué busca?
Rectificación	Corregir un dato que está mal o incompleto.
Cancelación	Solicitar que un dato deje de estar en los registros cuando corresponda.

Por ejemplo, si tu domicilio está incorrecto, se trata de rectificación; si solicitas que determinados datos dejen de conservarse porque ya no existe una razón legal para mantenerlos, se trata de cancelación, cuando proceda.



¿Siempre se pueden cancelar los datos?

No. Esta es una de las ideas más importantes que debe conservar el lector. Una institución pública puede tener la obligación legal de conservar determinada información; por ejemplo, un expediente puede necesitar mantenerse durante cierto periodo establecido por las disposiciones aplicables. En estos casos, aunque una persona solicite la cancelación, puede existir una razón legal para conservar los datos. Por eso, el derecho de cancelación existe, pero su ejercicio tiene límites establecidos por la ley.

¿Qué pasa después de solicitar la cancelación?

En Nuevo León después de presentar una solicitud de cancelación, la institución debe analizar si se cumplen las condiciones para que esta proceda. Cuando la cancelación se lleva a cabo, el responsable debe informar al titular mediante una constancia, previa acreditación de su identidad y, en su caso, la de su representante.

De acuerdo con el artículo 87 de los Lineamientos de Protección de Datos Personales para los Sujetos Obligados del Estado de Nuevo León, la constancia debe señalar dónde se encontraban los datos personales, el periodo de bloqueo cuando corresponda, las medidas de seguridad implementadas durante dicho periodo y las políticas, métodos y técnicas utilizadas para suprimir definitivamente los datos, procurando que la posibilidad de recuperarlos o reutilizarlos sea mínima.

La constancia debe notificarse al titular dentro de un plazo que no exceda de quince días establecido en el artículo 62 (LPDPPSONL, 2019).

Una idea importante sostiene que conservar no significa utilizar para cualquier cosa

Que una institución tenga una obligación legal de conservar determinados datos no significa que pueda utilizarlos libremente para cualquier finalidad. La información debe continuar siendo tratada de acuerdo con las obligaciones aplicables y con las medidas de protección correspondientes. Por eso conviene distinguir entre “la institución tiene que conservar este dato” y “la institución puede utilizar este dato para cualquier finalidad”, ya que no significan lo mismo.

¿Qué puede preguntarse una persona?

Si quiere solicitar la cancelación de sus datos, puede comenzar por identificar qué datos quiere cancelar, qué institución los tiene, para qué fueron recabados y si existe alguna razón por la que todavía deban conservarse. Estas preguntas ayudarán a comprender mejor la situación antes de presentar una solicitud.

Para recordar la diferencia entre estos dos derechos, la rectificación responde a “mi información está mal, quiero que la corrijan”; la cancelación responde a “quiero que mis datos dejen de estar registrados cuando legalmente corresponda”. Y todavía nos faltan dos derechos ARCOP por conocer, oposición y portabilidad. En el siguiente capítulo veremos cuándo una persona puede pedir que sus datos no sean utilizados para determinadas finalidades.

Para recordar. Tus datos personales no tienen que permanecer incorrectos para siempre. Puedes solicitar su rectificación cuando estén mal y, cuando legalmente corresponda, solicitar su cancelación. La clave está en conocer la diferencia, entendiendo que rectificar es corregir; cancelar es solicitar que los datos dejen de conservarse, cuando proceda.

8.5 Derecho de Oposición

Hay ocasiones en las que una persona puede estar de acuerdo con que una institución tenga determinados datos personales, pero no estar de acuerdo con que sean utilizados para una finalidad específica. Para estas situaciones existe el derecho de oposición.

En términos sencillos, el derecho de oposición permite solicitar que el uso de nuestros datos personales se detenga o no se realice para determinadas finalidades, cuando se cumplen las condiciones establecidas por la ley. No significa que una persona pueda impedir cualquier tratamiento de sus datos simplemente porque así lo desea; la institución debe analizar cada caso y determinar si la oposición es legalmente procedente.



Un ejemplo para entenderlo

Imaginemos que una persona proporciona sus datos personales a una institución pública para realizar un trámite relacionado con su cuenta de agua. Posteriormente, comienza a recibir en su teléfono mensajes que no están relacionados con su trámite, como invitaciones a participar en encuestas, campañas informativas o actividades que utilizan sus datos para una finalidad distinta. Si considera que ese tratamiento no debe realizarse, puede solicitar que sus datos dejen de utilizarse para esa finalidad mediante el derecho de oposición, siempre que se cumplan las condiciones previstas en la legislación aplicable.

Esto no significa que la institución pública deba eliminar sus datos de la cuenta, ya que puede necesitar conservarlos para prestar el servicio, atender trámites o cumplir con sus obligaciones legales. La oposición se refiere al tratamiento específico al que la persona desea oponerse.

Oposición no significa cancelación

Esta diferencia puede parecer pequeña, pero es fundamental.

Tabla 8.3 Rectificación, cancelación y oposición.

Derecho	En pocas palabras
Rectificación	"Mi dato está mal; quiero corregirlo."
Cancelación	"Quiero que mis datos dejen de estar registrados, cuando corresponda."
Oposición	"No quiero que mis datos sean utilizados para determinada finalidad, cuando legalmente proceda."

Por ejemplo, la cancelación busca que determinados datos dejen de conservarse cuando ya no exista una razón legal para mantenerlos; la oposición permite que los datos sigan existiendo en un registro, pero solicita que no sean utilizados para determinado tratamiento cuando se actualicen las condiciones legales para ello.

¿Por qué puede ser importante este derecho?

Porque nuestros datos pueden utilizarse para diferentes actividades y no todos los usos tienen necesariamente el mismo propósito. Una persona puede preguntarse si realmente es necesario utilizar sus datos de determinada manera; el derecho de oposición permite plantear esa preocupación ante la institución correspondiente, lo que contribuye a que las personas tengan una participación más activa respecto del uso de su información.

No siempre será posible oponerse

Este punto debe quedar muy claro. Existen tratamientos de datos personales que las instituciones públicas deben realizar porque una ley les obliga o porque son necesarios para cumplir con sus atribuciones; en esos casos, la oposición puede no resultar procedente. Por eso, este derecho no debe entenderse como “puedo impedir cualquier uso de mis datos”, sino como “puedo solicitar que no se utilicen para determinada finalidad cuando la ley permita ejercer este derecho”.



Una situación cotidiana

Imaginemos que una persona detecta que sus datos están siendo utilizados para una actividad que considera distinta de aquella para la que fueron recabados. En lugar de quedarse únicamente con la duda, puede preguntar para qué están utilizando sus datos, cuál es la finalidad de ese tratamiento y si existe una razón legal para hacerlo. Y, cuando corresponda, puede ejercer su derecho de oposición.

Para recordar. Oponerse significa pedir que tus datos no sean utilizados para determinada finalidad cuando la ley permite hacerlo. No significa necesariamente borrar tus datos.

8.6 Derecho de Portabilidad



El derecho de portabilidad permite que una persona pueda obtener sus datos personales y, cuando se cumplen las condiciones previstas por la legislación mexicana aplicable en materia de protección de datos personales, transmitirlos de un responsable a otro, o recibirlos en un formato que permita utilizarlos posteriormente.

La idea central es que los datos personales puedan pasar de una institución, empresa o sistema a otro, sin que sea necesario comenzar nuevamente desde cero, siempre que se trate de información susceptible de portabilidad y que los sistemas involucrados permitan su utilización o intercambio mediante tecnologías interoperables.

¿Por qué existe este derecho?

Porque cada vez generamos más información personal mediante sistemas digitales y, en determinadas situaciones, puede ser necesario continuar utilizándola cuando cambiamos de institución o de sistema.

Por ejemplo, una persona que durante varios años ha recibido atención en una institución de seguridad social puede tener determinada información personal registrada electrónicamente. Si posteriormente cambia de institución, puede necesitar que algunos de esos datos estén disponibles en el nuevo sistema. Cuando se cumplen las condiciones establecidas por la legislación mexicana aplicable en materia de protección de datos personales, el derecho de portabilidad permite obtener determinados datos en un formato que pueda seguir utilizándose o, cuando corresponda, transmitirlos a otro sistema.

De esta manera, la portabilidad busca facilitar que determinados datos personales puedan obtenerse y, cuando legalmente proceda, transmitirse de un sistema a otro, sin que esto signifique que toda la información pueda trasladarse automáticamente.

Un ejemplo sencillo

Imaginemos que una persona utiliza un servicio digital que genera y conserva determinados datos personales. Después decide utilizar otro servicio. En determinadas circunstancias, podría solicitar que sus datos

sean entregados o transmitidos en condiciones que permitan su utilización. La idea puede resumirse como la solicitud de “quiero poder obtener mis datos de una manera que me permita utilizarlos nuevamente cuando la ley lo permita”.

La portabilidad no significa llevarse cualquier información

También aquí es importante evitar una interpretación equivocada, no significa que una persona pueda exigir que cualquier institución le entregue absolutamente toda la información que posee. La portabilidad está sujeta a las condiciones y supuestos establecidos en la legislación de protección de datos personales. Por ello, debe analizarse qué datos pueden ser objeto de portabilidad, en qué circunstancias procede, cómo deben entregarse y si existen condiciones que impidan o limiten su ejercicio.

Portabilidad no es lo mismo que acceso

Ambos derechos están relacionados, pero no significan lo mismo. El acceso busca que una persona conozca sus datos personales y la información relacionada con su tratamiento; la portabilidad, cuando resulta procedente, busca que determinados datos puedan ser obtenidos o transmitidos en condiciones que permitan su utilización. Podemos recordarlo considerando que el acceso responde a “quiero saber qué datos tienen sobre mí”, mientras que la portabilidad responde a “quiero obtener determinados datos de una manera que permita utilizarlos o transmitirlos, cuando la ley lo permita”.



Los cinco derechos ARCOP

Con estos dos capítulos terminamos de conocer los cinco derechos.

Tabla 8.4 Los cinco derechos ARCOP y su pregunta clave.

Derecho	Pregunta sencilla
Acceso	¿Qué datos tienen sobre mí?
Rectificación	¿Qué dato está mal y quiero corregir?
Cancelación	¿Qué datos quiero que dejen de conservarse cuando corresponda?
Oposición	¿A qué uso de mis datos quiero oponerme, cuando legalmente proceda?
Portabilidad	¿Qué datos puedo obtener o transmitir en los casos previstos por la ley?

Una forma fácil de recordarlos: conozco → corrijo → cancelo → me opongo → obtengo y transfiero. No siempre tendremos que ejercer los cinco; dependiendo de la situación, uno puede ser más adecuado que otro.

Tus datos, tus derechos

Conocer los derechos ARCOP cambia la manera en que vemos nuestros datos personales. Ya no se trata solamente de pensar “espero que la institución cuide mi información”; también podemos pensar “tengo derechos y puedo ejercerlos”. Si nuestros datos son incorrectos, podemos solicitar su rectificación; si corresponde que dejen de conservarse, podemos solicitar su cancelación; si existe una razón legal para oponernos a determinado tratamiento, podemos ejercer nuestro derecho de oposición; y cuando nuestros datos sean tratados mediante medios automatizados, podemos ejercer la portabilidad o cuando corresponda, transmitirlos a otro responsable.

Conocer tus derechos es el primer paso para proteger tus datos personales. No necesitas ser abogado ni conocer todas las leyes para comenzar; lo importante es reconocer que tus datos personales son tuyos y que la legislación mexicana aplicable en materia de protección de datos personales te proporciona herramientas para ejercer control sobre ellos. El siguiente paso es saber cómo utilizar esas herramientas.

8.7 ¿Cuándo pueden limitarse estos derechos?

Conocer nuestros derechos ARCOP nos permite tomar un papel más activo respecto de nuestros datos personales. Sin embargo, es importante saber que estos derechos no son absolutos. Esto significa que puede haber situaciones previstas por la ley en las que una institución no pueda atender una solicitud en los términos que la persona espera, o en las que el ejercicio de un derecho deba limitarse para proteger otros derechos, cumplir una obligación legal o atender una situación de interés público. Esto no significa que una institución pueda simplemente responder “no se puede”; cuando un derecho se limita, debe existir una razón legal que lo justifique.

¿Por qué puede existir una limitación?

Imaginemos que una persona solicita la cancelación de determinados datos personales que forman parte de un expediente que una autoridad tiene obligación legal de conservar. Aunque la persona tenga derecho a solicitar la cancelación, la institución puede no estar facultada para eliminar esa información si existe una disposición que obliga a conservarla. En este caso, el derecho no desaparece, lo que sucede es que existe una razón legal que impide que la solicitud tenga el resultado esperado.

Algunos ejemplos

Las situaciones pueden ser diferentes dependiendo del derecho y de las circunstancias.

Tabla 8.5 Ejemplos de posibles limitaciones a los derechos ARCOP.

Situación	¿Por qué podría existir una limitación?
Se solicita cancelar información que debe conservarse por ley.	La institución tiene una obligación legal de conservarla.
Se solicita modificar información que debe mantenerse como parte de un registro oficial.	La institución debe preservar la integridad del registro.



Situación	¿Por qué podría existir una limitación?
Se solicita acceso a información cuya entrega podría afectar derechos de otra persona.	Deben protegerse también los datos personales de terceros.
Se solicita información relacionada con una investigación o procedimiento.	Su entrega podría afectar determinadas funciones o actuaciones de la autoridad.
Se solicita oponerse a un tratamiento que la institución está obligada a realizar.	Puede existir una obligación legal que impida dejar de tratar esos datos.

Estos son ejemplos generales. La procedencia de una limitación siempre debe analizarse conforme al caso concreto y a la legislación aplicable.

Proteger los datos de una persona no significa afectar los derechos de otra

Esta situación puede ser difícil de entender. Imaginemos que una persona solicita un documento que contiene sus datos personales, pero el mismo documento también contiene información personal de otras personas. La institución no necesariamente puede entregar el documento completo sin ninguna protección, podría ser necesario proteger los datos de terceros, de acuerdo con las disposiciones aplicables. Esto nos muestra algo importante, la protección de datos personales también implica respetar la privacidad de otras personas.

¿Puede una institución negar una solicitud simplemente porque quiere?

No debería. Cuando una persona ejerce un derecho ARCOP y la institución considera que no puede atenderlo, debe existir un fundamento legal para ello y debe informarse la razón correspondiente en los términos establecidos por la legislación mexicana vigente de protección de datos personales. Esto es importante porque permite distinguir entre “no quiero entregarte esa información” y “la ley establece una razón por la cual, en este caso, no puedo atender tu solicitud de la manera que pides”, son situaciones completamente diferentes.

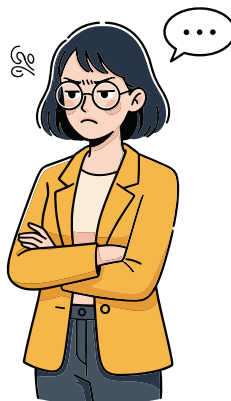
Los derechos pueden tener límites, pero no desaparecen

Una limitación no significa que la persona deje de tener derechos sobre sus datos. Por ejemplo, si no procede la cancelación porque una institución tiene la obligación legal de conservar determinada información, eso no significa que pueda utilizarla para cualquier finalidad. La información debe continuar siendo tratada conforme a las disposiciones aplicables y con las medidas de protección correspondientes. Por eso es importante recordar, que un dato deba conservarse no significa que pueda utilizarse sin límites.

¿Qué pasa si no estoy de acuerdo?

Aquí comienza la parte de acción de este bloque. Si una persona considera que su solicitud fue rechazada injustificadamente, que no recibió una respuesta adecuada o que sus derechos fueron afectados, no significa que ahí termine el camino, existen mecanismos para inconformarse y, dependiendo del caso, acudir ante la autoridad competente.

En Nuevo León, el Instituto Estatal de Transparencia, Acceso a la Información y Protección de Datos Personales (INFONL) tiene un papel fundamental dentro del ámbito de sus atribuciones para garantizar el ejercicio de los derechos relacionados con la protección de datos personales en poder de la autoridad. El procedimiento concreto para presentar una solicitud y, en su caso, inconformarse, lo desarrollaremos en el siguiente capítulo.



Una regla sencilla

Cuando una institución no atiende nuestra solicitud, podemos hacer tres preguntas referidas a por qué no pueden hacerlo, qué disposición legal lo establece y qué podemos hacer si no estamos de acuerdo. Estas preguntas ayudan a pasar de la duda a la acción.

No debe confundirse una limitación con una negativa arbitraria. Una limitación es una restricción que tiene una razón jurídica; una negativa arbitraria sería impedir el ejercicio de un derecho sin una justificación legal

válida. La diferencia es importante, ya que las instituciones públicas tienen obligaciones respecto de la protección de datos personales y no pueden establecer restricciones simplemente por decisión propia.



Una última idea

Los derechos AR COP son herramientas para que las personas tengan mayor control sobre sus datos personales, pero ese control debe convivir con otros derechos y obligaciones; por eso la ley establece determinadas excepciones y límites. La idea no es que la ciudadanía memorice todas esas excepciones. Lo importante es comprender el hecho de que tus derechos existen, puedes ejercerlos y, si una institución considera que no puede atender tu solicitud, debe existir una razón legal que lo justifique. Y si consideras que esa decisión no es correcta, existen mecanismos para defender tus derechos.

Para recordar. Que un derecho pueda tener límites no significa que pueda negarse arbitrariamente. Toda limitación debe estar respaldada por la legislación mexicana de protección de datos personales aplicable y atender las circunstancias del caso.

Capítulo 9. ¿Cómo ejercer tus derechos paso a paso?

Conocer nuestros derechos es importante, pero saber cómo ejercerlos es lo que permite llevarlos a la práctica. Si una institución tiene nuestros datos personales, podemos preguntarnos qué información conserva, solicitar que se corrija cuando sea incorrecta, pedir su cancelación cuando corresponda u oponernos a determinados tratamientos, entre otras posibilidades previstas por la legislación.



La buena noticia es que no necesitas ser abogado para presentar una solicitud de derechos ARCOP. Lo importante es identificar quién tiene tus datos, explicar qué necesitas y seguir el procedimiento establecido. En este capítulo recorreremos el proceso paso a paso.

9.1 Paso 1. Identifica quién tiene tus datos

Antes de presentar una solicitud, necesitamos saber qué institución tiene nuestros datos personales. Puede parecer obvio, pero este es uno de los primeros puntos que debemos identificar.

Piensa en todas las ocasiones en las que has proporcionado información, por ejemplo, al realizar un trámite, al acudir a una institución de salud, al inscribirte en una escuela, al solicitar un servicio público, al realizar una gestión administrativa, al participar en un programa, o al proporcionar información a una institución pública. Cada una de esas actividades puede generar registros que contienen datos personales.

Una pregunta sencilla puede ayudarte, ¿a quién le entregué mis datos? Si acudiste a una dependencia estatal para realizar un trámite, probablemente esa institución sea el primer lugar donde debes preguntar. Si realizaste un trámite ante un municipio, tendrás que identificar al área o institución municipal correspondiente. Si tus datos fueron entregados a una institución pública federal, deberás acudir al sujeto obligado federal que corresponda.



No necesitas conocer el nombre de la base de datos

Una persona no tiene por qué saber en qué sistema informático está registrado su expediente, ni conocer el nombre técnico de la base de datos. Es suficiente con identificar, en la medida de lo posible, qué institución tiene relación con el trámite, servicio o actividad en la que proporcionaste tus datos. Por ejemplo, si entregaste tus datos cuando solicitaste una licencia, la pregunta siguiente sería qué institución recibió esa información.



Haz memoria, ¿dónde has dejado tus datos?

Una manera práctica de comenzar es hacer una pequeña lista.

Tabla 9.1 ¿Dónde podrían estar tus datos personales?

Situación	¿Quién podría tener mis datos?
Realicé un trámite estatal.	La dependencia o entidad estatal correspondiente.
Realicé un trámite municipal.	El municipio o la unidad administrativa correspondiente.
Acudí a un centro de salud público.	La institución pública que proporcionó el servicio.
Me inscribí en una escuela pública.	La institución educativa correspondiente.
Solicité un programa o apoyo público.	La dependencia o entidad responsable del programa.
Realicé otro trámite ante una autoridad.	El sujeto obligado que recibió la información.

La institución concreta dependerá del trámite o servicio de que se trate.

¿Y si no estoy seguro de quién tiene mis datos?

No te preocupes. Puedes comenzar identificando dónde realizaste el trámite o con quién tuviste contacto; por ejemplo, “hace dos años entregué mis documentos para realizar un trámite ante una dependencia estatal”. Ese dato puede ser suficiente para comenzar a investigar cuál es el área responsable.

También puedes consultar el aviso de privacidad relacionado con el trámite, que tiene precisamente una función importante, informar a las personas sobre el tratamiento que se dará a sus datos personales y otros aspectos relacionados con dicho tratamiento.

Cuando una institución pública recaba datos personales, normalmente debe proporcionar información sobre su tratamiento mediante el aviso de privacidad correspondiente. Por eso, si conservas un documento, formulario o comprobante del trámite, revisa si contiene o señala dónde consultar el aviso de privacidad, ya que puede ayudarte a identificar quién recaba los datos, para qué los utiliza, qué datos solicita y otros aspectos relacionados con su tratamiento.



¿Qué pasa si mis datos están en varias instituciones?

Es posible. Por ejemplo, para realizar un determinado trámite pueden intervenir distintas instituciones o áreas; en ese caso, es importante distinguir qué información tiene cada una. Si quieres conocer los datos que tiene una institución, la solicitud debe dirigirse al sujeto obligado que corresponda, no necesariamente una sola solicitud permite obtener información que se encuentra bajo responsabilidad de instituciones diferentes.

Antes de presentar tu solicitud, recuerda dónde entregaste tus datos, identifica la institución que los recibió, revisa documentos o avisos de privacidad que tengas y, si intervienen varias instituciones, identifica cuál tiene la información que buscas. Y entonces estarás listo para el siguiente paso.

9.2 Paso 2. Presenta tu solicitud

Una vez que identificaste qué institución tiene tus datos personales y qué derecho deseas ejercer, el siguiente paso es presentar tu solicitud. No necesitas redactar un documento con lenguaje jurídico ni utilizar términos complicados; lo más importante es proporcionar la información y la documentación necesarias para que la institución pueda identificar tu solicitud y atenderla correctamente.



Presentar una solicitud con los requisitos completos ayuda a evitar retrasos en el procedimiento. Si la información es insuficiente o falta algún requisito previsto por la ley, la institución podrá requerirte que completes o aclares tu solicitud antes de continuar con su trámite.

¿Qué debe contener una solicitud de derechos ARCOP?

La Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Nuevo León establece los requisitos mínimos que debe contener una solicitud de derechos ARCOP. Antes de presentarla, verifica que incluya la siguiente información:

Tabla 9.2 Requisitos para presentar una solicitud de derechos ARCOP.

Requisito	¿Para qué sirve?
Nombre de la persona titular	Identificar quién ejerce el derecho.
Domicilio o cualquier medio para recibir notificaciones	Permitir que la institución envíe la respuesta por el medio elegido.
Documentos que acrediten la identidad	Confirmar que quien presenta la solicitud es la persona titular de los datos o quien legalmente la representa.
En su caso, documentos que acrediten la representación	Demostrar que la persona actúa en nombre de la persona titular cuando la solicitud se presenta por medio de un representante.
De ser posible, señalar el área o institución que tiene los datos personales	Facilitar la localización de la información dentro de la institución.
Descripción clara y precisa de los datos personales o del derecho que deseas ejercer	Permitir que la institución entienda exactamente qué estás solicitando.
Cualquier elemento que facilite localizar los datos	Ayudar a identificar el trámite, expediente, programa, fecha o cualquier información relacionada con los datos personales.

Importante: Estos son los requisitos mínimos previstos por la legislación para presentar una solicitud de derechos ARCOP ante sujetos obligados del Estado de Nuevo León.

Fuente: Elaboración propia con base en la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Nuevo León, 2019, art. 63.

¿Qué documentos debo acompañar?

Además de la información de la solicitud, es importante presentar la documentación que corresponda al caso.

Tabla 9.3 Documentos que pueden acompañar una solicitud.

Situación	Documento que puede requerirse
Presentar la solicitud personalmente.	Documento que acredite tu identidad (Identificación Oficial).
La solicitud la presenta un representante.	Documento que acredite la identidad del titular, la identidad del representante y el documento que acredite la representación como lo es un poder simple.
Solicitar una rectificación.	Documentación que permita acreditar cuál es la información correcta que solicitas registrar.

¿Por qué es necesario acreditar la identidad?

Porque la institución debe asegurarse de que los datos personales únicamente sean entregados o modificados a solicitud de la persona titular o de quien legalmente pueda representarla.

¿Dónde puedo presentar la solicitud?

En Nuevo León existen diferentes medios para presentar una solicitud de derechos ARCOP ante los sujetos obligados.



Tabla 9.4 Medios para presentar una solicitud de derechos ARCOP en Nuevo León.

Medio	¿Cómo funciona?
Plataforma Nacional de Transparencia (PNT)	Permite presentar solicitudes de derechos ARCOP por medios electrónicos ante los sujetos obligados.
Unidad de Transparencia de la institución	Puedes presentar la solicitud directamente en la Unidad de Transparencia del sujeto obligado.
Correo electrónico u otros medios habilitados por la institución	Algunos sujetos obligados cuentan con medios electrónicos autorizados para recibir solicitudes.

La Plataforma Nacional de Transparencia (PNT) es una de las herramientas más útiles para la ciudadanía, ya que permite presentar solicitudes de derechos ARCOP por internet, dar seguimiento al trámite y recibir respuestas por el medio seleccionado.

Fuente: La Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Nuevo León, 2019, artículo. 63.

Utiliza el formato oficial del INFONL

No es necesario elaborar un formato desde cero. El INFONL puso a disposición de la ciudadanía un Formato Único de Solicitud de Acceso, Rectificación, Cancelación y Oposición de Datos Personales, diseñado para facilitar el ejercicio de estos derechos.

Este formato te guía paso a paso para:

- Identificar el derecho que deseas ejercer.
- Proporcionar la información necesaria.
- Señalar el medio para recibir la respuesta.
- Incorporar la documentación requerida cuando corresponda.



HERRAMIENTA CIUDADANA

El formato oficial puede descargarse gratuitamente desde el portal del INFONL y utilizarse para presentar solicitudes de derechos ARCO ante sujetos obligados del Estado de Nuevo León. El cual puede ser descargado en el siguiente hipervínculo:

<https://infonl.mx/wp-content/uploads/2024/05/formato-nuevo-solicitud-ARCO.pdf>

¿Qué información adicional debo incluir según el derecho que ejerza?

El propio INFONL recomienda agregar algunos elementos específicos dependiendo del derecho que deseas ejercer.

Tabla 9.5 Información específica según el derecho ARCO.

Derecho	Información que conviene incluir
Acceso	Indicar la modalidad en la que prefieres recibir o consultar tus datos personales.
Rectificación	Precisar qué dato deseas corregir y proporcionar la documentación que sustente la modificación.
Cancelación	Señalar las causas por las que solicitas la cancelación de tus datos personales.
Oposición	Explicar las causas legítimas o la situación específica por la que solicitas que determinado tratamiento deje de realizarse.
Portabilidad	El derecho de portabilidad es la facultad del titular de obtener del responsable sus datos personales tratados por medios electrónicos, en un formato estructurado y comúnmente utilizado que permita su reutilización, así como de solicitar, cuando resulte procedente, su transmisión a otro responsable sin impedimentos.



Estas recomendaciones forman parte del Formato Único de Solicitud de Derechos ARCOP elaborado por el INFONL y ayudan a que la solicitud sea más clara y completa.

¿Qué pasa si mi solicitud está incompleta?

Si la solicitud no contiene alguno de los requisitos previstos por la ley o falta documentación necesaria para atenderla, la institución no la desecha de inmediato.

En ese caso, el sujeto obligado puede emitir una **prevención**, es decir, solicitarle que completen o aclaren la información faltante.

- La prevención debe notificarse dentro de los cinco días siguientes a la presentación de la solicitud.
- Tendrás diez días para atender la prevención y proporcionar la información solicitada.
- Mientras atiendes la prevención, se interrumpe el plazo que tiene la institución para responder la solicitud.
- Si no atiendes la prevención dentro del plazo establecido, la solicitud se tendrá por no presentada.

Consejo ciudadano: Revisa cuidadosamente tu solicitud antes de enviarla. Incluir todos los requisitos desde el inicio puede evitar una prevención y agilizar el trámite.

Fundamento: artículo 63 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Nuevo León.

Un ejemplo de la vida cotidiana

María desea corregir su domicilio registrado en una Institución Pública del Estado de Nuevo León.

Antes de presentar la solicitud:

- Identifica que ejercerá el derecho de rectificación;
- Utiliza el Formato Único del INFONL;
- Señala cuál es el domicilio registrado y cuál es el correcto;
- Adjunta el documento que sustenta la modificación; y
- Elige recibir la respuesta por correo electrónico.

Con esta información, la institución cuenta con los elementos necesarios para analizar la solicitud y determinar si la rectificación procede conforme a la ley.

Antes de enviar la solicitud, revisa esta lista de verificación

Revisa que la solicitud esté completa.

- Identifica correctamente a la institución que tiene tus datos personales.
- Señala el derecho ARCOP que deseas ejercer.
- Explica claramente qué solicitas.
- Incluye los datos que facilitan localizar la información.
- Acredita tu identidad.
- Acredita la representación, en el caso de ser presentada la solicitud por otra persona.
- Adjunta los documentos necesarios, cuando corresponda.
- Elige el medio para recibir la respuesta.



Para recordar

Presentar una solicitud de derechos ARCOP es más sencillo cuando utilizas las herramientas correctas. El formato único del INFONL y la Plataforma Nacional de Transparencia fueron creados para facilitar a la ciudadanía el ejercicio de estos derechos y ayudar a que las solicitudes cumplan con los requisitos previstos por la ley.

9.3 Paso 3. Espera la respuesta

Presentar una solicitud de derechos ARCOP no significa que la institución tenga que responder de inmediato. En Nuevo León, la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Nuevo León establece plazos para que la institución reciba, analice y responda la solicitud.





El responsable tiene un plazo de hasta 20 días hábiles, contados a partir del día siguiente a la recepción de la solicitud, para emitir una respuesta. Este plazo puede ampliarse una sola vez hasta por 10 días hábiles, cuando las circunstancias lo justifiquen y se informe oportunamente a la persona titular.

Si la solicitud resulta procedente, la institución debe hacer efectivo el derecho correspondiente en un plazo que no podrá exceder de 15 días, contados a partir del día siguiente a aquel en que se haya notificado la respuesta.

Por eso, es importante conservar el acuse o comprobante de tu solicitud y estar atento al medio que hayas señalado para recibir notificaciones (LPDPPSONL, 2019, art. 62 y 63).

¿Qué puede ocurrir después de presentar la solicitud?

Después de presentar una solicitud para ejercer tus derechos ARCOP, la institución debe darle trámite y entregarte un acuse de recibo. A partir de ese momento, pueden presentarse distintas situaciones.

La institución puede atender tu solicitud cuando se cumplen los requisitos y el ejercicio del derecho resulta procedente. Dependiendo de lo que hayas solicitado, esto puede significar que te permitan acceder a tus datos personales, corregirlos, cancelarlos o atender tu solicitud de oposición.

También puede suceder que falte algún requisito o información necesaria para tramitar la solicitud. En ese caso, si la institución no cuenta con elementos para subsanar la omisión, deberá prevenirte una sola vez para que completes la información. Esta prevención debe realizarse dentro de los cinco días siguientes a la presentación de la solicitud y tendrás diez días hábiles para atenderla.

Si la institución no es competente para atender tu solicitud, debe informártelo dentro de los tres días siguientes a su presentación y, cuando sea posible, orientarte sobre cuál es el responsable que podría atenderla.



También puede ocurrir que tu solicitud no sea procedente por alguna de las causas previstas en la ley. Por ejemplo, cuando los datos no se encuentren en posesión de la institución, exista un impedimento legal, se afecten los derechos de otra persona o exista una resolución de una autoridad que limite el ejercicio del derecho. En estos casos, la institución debe informarte el motivo de su determinación.

Por eso, después de presentar tu solicitud, es importante guardar el acuse de recibo y estar atento al medio que señalaste para recibir notificaciones. La institución tiene, por regla general, hasta 20 días hábiles para responder y, cuando el ejercicio del derecho resulte procedente, hasta 15 días hábiles adicionales para hacerlo efectivo (LPDPPSONL, 2019, art. 62, 63, 64 y 66).

No confundas una respuesta con una solución favorable

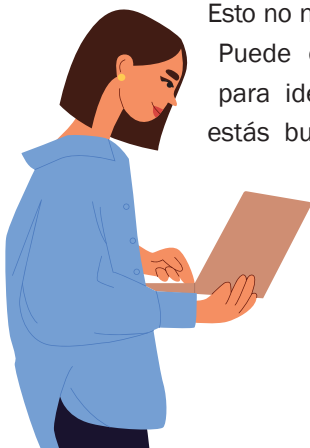
Recibir una respuesta no significa necesariamente que la institución haya concedido lo que solicitaste. Por ejemplo, ante la solicitud “quiero que se cancelen mis datos personales”, la respuesta podría ser “no procede la cancelación porque existe una obligación legal de conservarlos”. En este caso sí existe una respuesta, aunque no sea la que esperaba la persona.

Por eso, cuando recibas la contestación, no solamente revises si dice “sí” o “no”. Pregúntate si ¿respondieron exactamente a lo que solicité?, ¿me explicaron la razón? y ¿la respuesta indica qué puedo hacer si no estoy de acuerdo?

¿Y si me piden más información?

Esto no necesariamente significa que tu solicitud haya sido rechazada.

Puede ocurrir que la institución necesite información adicional para identificar correctamente tus datos, saber qué información estás buscando, confirmar tu identidad, acreditar que actúas en representación de otra persona, cuando corresponda, o atender adecuadamente la solicitud. Si recibes una prevención o solicitud de información adicional, revísala con cuidado y atiéndela dentro del plazo que corresponda.





¿Qué hago mientras espero?

No necesitas hacer nada complicado. Te recomendamos guardar el comprobante de tu solicitud, anotar la fecha en que la presentaste, conservar cualquier comunicación que recibas, revisar el medio que señalaste para recibir la respuesta y no eliminar los mensajes o documentos relacionados con tu solicitud. Estos elementos pueden ser importantes si posteriormente necesitas demostrar qué solicitaste y cuándo lo hiciste.



Elementos que debes considerar

Tabla 9.6 Elementos de una solicitud de derechos ARCOP.

Elemento	¿Para qué sirve?
Identificación de la persona solicitante	Permite saber quién está ejerciendo el derecho y realizar las verificaciones necesarias.
Derecho que deseas ejercer	Ayuda a identificar si se trata de acceso, rectificación, cancelación, oposición o portabilidad.
Datos o información que buscas	Permite a la institución localizar y atender tu solicitud.
Medio para recibir la respuesta	Permite que la institución pueda comunicarte el resultado.
Información adicional, cuando sea necesaria	Puede ayudar a localizar los datos o comprender mejor lo que solicitas.

En determinados casos también puede ser necesario acreditar la identidad o la representación de otra persona.

Si quieres corregir tus datos, explica qué está mal

Supongamos que tu domicilio aparece incorrectamente. En lugar de escribir únicamente “quiero ejercer mi derecho de rectificación”, es mucho más útil explicar de forma detallada “solicito la rectificación del domicilio registrado en mis datos personales, ya que actualmente aparece como _____ y el domicilio correcto es _____”. La institución podrá comprender con mayor facilidad qué dato debe revisar.



Si quieres acceder a tus datos, sé específico

Puedes decir “solicito conocer los datos personales que esa institución tiene registrados a mi nombre”. Si buscas información relacionada con un trámite específico, puedes agregar una precisión como “la solicitud se refiere a los datos personales que proporcioné con motivo del trámite realizado en _____”. Esto puede facilitar la localización de la información.

Si solicitas cancelación u oposición

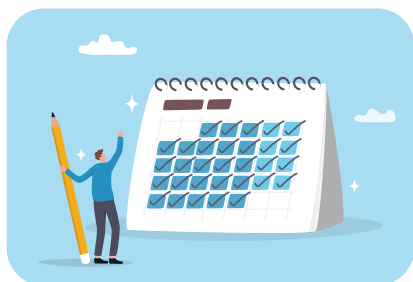
También conviene explicar claramente qué información y qué tratamiento estás señalando. Por ejemplo, “solicito la cancelación de los datos personales relacionados con _____, en los casos en que legalmente proceda”, o “solicito ejercer mi derecho de oposición respecto del tratamiento de mis datos personales relacionado con _____, en los términos que resulten aplicables”. No necesitas elaborar una explicación jurídica extensa, la claridad es más importante que utilizar palabras complicadas.

Un consejo para la ciudadanía

Antes de enviar tu solicitud, léela como si fueras la persona que va a recibirla, y pregúntate si alguien que no conoce tu situación entendería exactamente qué estás pidiendo. Si la respuesta es sí, probablemente has explicado lo necesario.

9.4 Plazos que debes conocer

Cuando presentas una solicitud para ejercer tus derechos ARCOP, la institución no tiene que responder de manera inmediata, pero tampoco puede dejar tu solicitud sin respuesta indefinidamente. La Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Nuevo León establece los plazos que deben observarse para responder y, cuando corresponda, hacer efectivo el derecho solicitado.



El responsable debe comunicar al titular la determinación adoptada dentro de los 20 días hábiles, contados a partir del día siguiente a la recepción de la solicitud.

Este plazo puede ampliarse una sola vez hasta por 10 días hábiles, cuando exista una causa justificada. La institución debe informar al titular sobre esta ampliación dentro del plazo original.

Cuando el ejercicio del derecho resulte procedente, el responsable debe hacerlo efectivo dentro de un plazo que no podrá exceder de 15 días hábiles, contados a partir del día siguiente a aquel en que se haya notificado la respuesta.

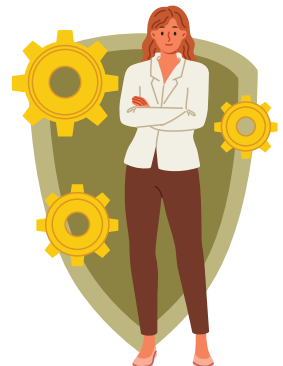
Tabla 9.7 Plazos para el ejercicio de derechos ARCOP.

Situación	Plazo
Comunicación de la respuesta	20 días hábiles
Ampliación del plazo para responder	Hasta 10 días hábiles adicionales, por una sola ocasión y cuando exista causa justificada
Hacer efectivo el derecho cuando resulte procedente	Hasta 15 días hábiles después de notificada la respuesta

Por eso, cuando presentes una solicitud, es importante **guardar el acuse o comprobante de recepción** y estar atento al medio que hayas señalado para recibir la respuesta (LPDPPSONL, 2019, art. 62).

¿Por qué es importante conocer los plazos?

Porque te permite saber si tu solicitud está avanzando dentro del tiempo establecido. Por ejemplo, si presentaste una solicitud y conservaste el comprobante, a partir de ahí puedes llevar un registro de los días hábiles transcurridos. Si llega la respuesta, podrás revisar si se encuentra dentro del plazo aplicable; y si no recibes respuesta o consideras que la atención fue incorrecta, podrás valorar las acciones que correspondan.



¿Qué pasa si no recibo respuesta?

No recibir respuesta dentro del plazo establecido no significa que debas simplemente olvidarte de tu solicitud. Si la institución no atiende tu solicitud dentro del plazo correspondiente, o si consideras que la respuesta vulnera tu derecho, existen mecanismos para inconformarte.

Aquí comienza una parte muy importante del siguiente tramo del capítulo, centrada en la pregunta sobre qué puedo hacer si no me responden o si no estoy de acuerdo con la respuesta. La respuesta a esa pregunta debe llevarnos directamente al siguiente capítulo.

Una recomendación práctica

Desde el momento en que presentes tu solicitud, crea una pequeña carpeta —física o digital— con la solicitud que presentaste, el comprobante de recepción, las comunicaciones que recibas, la respuesta de la institución y cualquier documento que hayas presentado posteriormente. Esto puede parecer innecesario cuando todo marcha bien, pero si posteriormente necesitas defender tus derechos, contar con esta información puede ser muy útil.

Tu ruta hasta ahora



Paso 1: identificar quién tiene tus datos.



Paso 2: presentar tu solicitud.



Paso 3: esperar la respuesta, revisando que tu solicitud contenga la información necesaria y controlando los plazos.



Si no estás de acuerdo, puedes buscar mecanismos para defender tu derecho.

Para recordar. No necesitas escribir una solicitud complicada. Lo importante es explicar con claridad qué derecho quieres ejercer, qué datos buscas y proporcionar los elementos necesarios para que la institución pueda atender tu petición. Y recuerda, los plazos se cuentan en días hábiles y es importante conservar el comprobante de tu solicitud para poder dar seguimiento.

Capítulo 10. ¿Qué hacer si tus derechos no son respetados?

Ejercer un derecho no siempre significa recibir la respuesta que esperabas. Puede ocurrir que una institución pública no dé trámite a tu solicitud, no responda dentro del plazo establecido, niegue el acceso a tus datos personales o entregue información incompleta o que no corresponda con lo solicitado.

Si esto sucede, no significa que el procedimiento haya terminado. La Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Nuevo León establece mecanismos para que puedas inconformarte y solicitar que la autoridad competente revise lo ocurrido.

Uno de estos mecanismos es el recurso de revisión, que permite cuestionar determinadas respuestas, omisiones o actuaciones relacionadas con el ejercicio de tus derechos ARCOP. La ley establece los casos en que procede, el plazo para presentarlo y el procedimiento que debe seguirse para resolverlo.

La protección de tus datos personales no termina cuando presentas una solicitud. También tienes derecho a inconformarte cuando consideres que tu solicitud no fue atendida conforme a la ley (LPDPPSONL, 2019, art. 62, 108 a 130).



10.1 Cuando una institución pública no responde

Cuando presentas una solicitud para ejercer tus derechos ARCOP, es importante conservar el comprobante de recepción y estar atento al medio que hayas señalado para recibir la respuesta.

La Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Nuevo León establece un plazo para que el responsable comunique la determinación correspondiente. Si ese plazo transcurre sin que recibas una respuesta, la falta de respuesta es un supuesto que puede dar lugar a la presentación de un recurso de revisión.

El recurso de revisión es el medio por el cual puedes inconformarte ante la autoridad garante cuando consideres que tu solicitud no fue atendida conforme a la legislación.

- La ley también contempla otros casos en los que puede presentarse este recurso, entre ellos:
- la negativa al ejercicio de los derechos ARCOP;
- la falta de respuesta dentro del plazo establecido;
- la entrega de datos personales incompletos;
- la entrega de datos que no correspondan con lo solicitado; y
- otros supuestos previstos expresamente por la legislación.

Por ello, si la institución no responde dentro del plazo establecido, no significa que tu solicitud haya quedado sin efecto. La propia ley contempla la posibilidad de presentar un recurso de revisión por falta de respuesta (LPDPPSONL, 2019, art. 62, 67 y 118).

¿Qué puedo hacer si no recibo respuesta?

Si transcurre el plazo que tenía el responsable para atender la solicitud sin que se haya emitido una respuesta, la persona titular puede interponer un recurso de revisión. En Nuevo León, cuando se trata de una solicitud presentada ante un sujeto obligado estatal o municipal, el recurso debe interponerse dentro de los quince días hábiles siguientes al vencimiento

del plazo que tenía el responsable para responder (LPDPPSONL, 2019, art. 117) o de la notificación de la respuesta.

El recurso puede presentarse ante el Instituto Estatal de Transparencia, Acceso a la Información y Protección de Datos Personales (INFONL) o ante la Unidad de Transparencia del responsable que conoció de la solicitud. La ley permite presentarlo, entre otros medios, mediante escrito libre, correo certificado con acuse de recibo, los formatos correspondientes o los medios electrónicos autorizados (LPDPPSONL, 2019, art. 108).

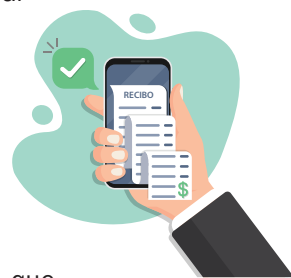
Para presentar el recurso, es importante contar con información que permita identificar la solicitud original y explicar qué ocurrió. Entre otros elementos, la ley contempla señalar el área responsable ante la cual se presentó la solicitud, los datos de identificación de la persona titular o su representante, la fecha de presentación de la solicitud cuando no hubo respuesta, así como el acto que se recurre y los motivos de inconformidad (LPDPPSONL, 2019, art. 119).

No es necesario que la persona vuelva a iniciar el procedimiento de ejercicio de derechos ARCOP. El recurso de revisión tiene precisamente la finalidad de permitir que la autoridad garante revise la actuación del responsable y, en su caso, ordene las medidas correspondientes.

El comprobante de la solicitud es importante

Cuando presentamos una solicitud, es recomendable conservar el acuse, folio o comprobante que acredite su recepción. También conviene guardar las comunicaciones posteriores y, en su caso, la respuesta de la institución. Estos documentos permiten reconstruir el proceso, lo que ayuda a saber qué se pidió, cuándo se presentó y qué ocurrió después.

Puede parecer un detalle menor, pero resulta especialmente importante cuando la persona necesita demostrar que presentó una solicitud y que el plazo correspondiente transcurrió sin obtener respuesta. En particular, cuando no existe respuesta, la fecha de presentación de la solicitud permite determinar cuándo comenzó a correr el plazo que tenía el responsable para atenderla y, posteriormente, cuándo puede comenzar el plazo para interponer el recurso de revisión.





¿A quién acudir en Nuevo León?

Cuando se trata de datos personales que se encuentran bajo responsabilidad de sujetos obligados del Estado o de los municipios de Nuevo León, la persona puede acudir al INFONL, en el ámbito de sus atribuciones. La legislación estatal aplicable en materia de protección de datos personales reconoce a la autoridad garante local facultades para conocer, sustanciar y resolver los recursos de revisión relacionados con el ejercicio de los derechos sobre datos personales. El recurso también puede presentarse ante la Unidad de Transparencia del responsable que conoció de la solicitud, conforme a los medios previstos por la legislación estatal vigente en materia de protección de datos personales.

Esto significa que la sociedad cuenta con una instancia especializada a la cual pueden acudir cuando consideran que una institución pública no atendió correctamente su solicitud.

Cuando el silencio también afecta un derecho

La falta de respuesta puede resultar especialmente frustrante porque deja a la persona sin saber qué ocurrió con su solicitud. Sin embargo, jurídicamente no se trata simplemente de esperar indefinidamente, la legislación reconoce la falta de respuesta como uno de los supuestos que pueden dar lugar a un recurso de revisión. En Nuevo León, cuando no se emitió respuesta, el plazo para presentar este recurso comienza a partir del vencimiento del plazo que tenía el responsable para atender la solicitud (LPDPPSONL, 2019, art. 117).

Por eso es tan importante conservar la fecha en que se presentó la solicitud y el comprobante de recepción. Si la persona considera que su solicitud no fue atendida, puede revisar el procedimiento completo para presentar una solicitud en el apartado 9.2 de esta obra.



10.2 Cuando no estás de acuerdo con la respuesta

Existe otra posibilidad que consiste en que la institución responde, pero la persona considera que la respuesta no atiende adecuadamente su solicitud. Puede ocurrir, por ejemplo, que se entreguen datos incompletos, que la información proporcionada no corresponda con lo solicitado, que se niegue el acceso a los datos o que no se realice la rectificación, cancelación u oposición solicitada.

En estos casos, lo primero es leer con atención la respuesta y compararla con la solicitud original. No basta con preguntarse si la respuesta fue favorable o desfavorable, es necesario revisar si la institución atendió realmente lo que se pidió y, cuando haya una negativa, conocer la razón que la sustenta.

La LGPDPPSO contempla como supuestos para interponer un recurso de revisión, entre otros, la entrega incompleta de datos personales, la entrega de datos que no corresponden con lo solicitado, la negativa al ejercicio de los derechos y la falta de respuesta. La LPDPPSONL contempla de manera similar estos supuestos.

Una respuesta también puede ser cuestionada

Recibir una respuesta no significa necesariamente que el asunto haya terminado. Una persona puede considerar que la institución no respondió a todo lo que solicitó, entregó información incompleta, proporcionó datos que no corresponden con su petición, negó el ejercicio de alguno de sus derechos, entregó la información en una modalidad o formato que no corresponde, o utilizó una razón que la persona considera que no justifica la negativa.

Cuando se presenta alguna de estas situaciones, existe la posibilidad de acudir al recurso de revisión correspondiente. En Nuevo León, este recurso puede presentarse ante la autoridad garante o ante la Unidad de Transparencia del responsable, por los medios que establece la legislación estatal. El plazo general para interponerlo es de quince días hábiles contados a partir del día siguiente a la notificación de la respuesta; cuando no hubo respuesta, el plazo se cuenta a partir del vencimiento del plazo para responder.

¿Qué debe hacer la persona?



La inconformidad debe explicar, de manera clara, qué parte de la respuesta considera incorrecta y por qué. No es necesario convertir la inconformidad en un documento lleno de palabras jurídicas; lo importante es explicar los hechos. Por ejemplo, “Pedí conocer todos los datos personales que la institución tiene registrados sobre mí; sin embargo, únicamente recibí información relacionada con uno de los trámites que he realizado. Por ello, solicito que se revise nuevamente mi petición y se me proporcione la información correspondiente a todos los datos personales que la institución tenga registrados sobre mí.” Una explicación clara permite identificar el problema y facilita su análisis.

La documentación ayuda a explicar lo ocurrido

Al presentar un recurso de revisión, es importante contar con los documentos relacionados con el caso. La legislación de protección de datos personales de Nuevo León contempla, entre los requisitos del recurso, la identificación del área ante la cual se presentó la solicitud, los datos de la persona titular, la fecha de la respuesta o de la solicitud cuando no hubo contestación, el acto que se impugna y las razones de inconformidad. También contempla la presentación de la solicitud original, su acuse y, cuando exista, la respuesta que se cuestiona.

En otras palabras, la persona debe poder mostrar con claridad qué pidió, ante quién lo pidió, qué respondió la institución si respondió y por qué considera que esa respuesta no respetó su derecho.

La finalidad no es complicar el procedimiento

El recurso de revisión es un mecanismo para que una autoridad garante analice la actuación del responsable y determine lo que corresponda conforme a la legislación. En Nuevo León, la autoridad garante (INFONL) puede confirmar la respuesta del responsable, modificarla o revocarla, u ordenar la entrega de los datos personales cuando exista una omisión, entre otras posibilidades. La legislación también prevé una etapa de conciliación entre las partes en determinados casos.



Esto permite que el procedimiento no se reduzca a una confrontación entre la persona y la institución, también puede existir un espacio para buscar una solución al problema.

Cuando tus datos están en manos de una institución pública

Es importante recordar que la protección de datos personales forma parte de los derechos que corresponden a todas las personas. La legislación nacional establece las bases para que quienes tienen datos personales bajo su responsabilidad los traten adecuadamente y para que las personas puedan ejercer sus derechos frente a ese tratamiento; la LGPDPSO vigente establece estas reglas para los sujetos obligados de los ámbitos federal, estatal y municipal.

En Nuevo León, la legislación local establece los procedimientos aplicables a los sujetos obligados estatales y municipales y reconoce al organismo garante local las atribuciones para conocer y resolver los recursos de revisión en materia de protección de datos personales.

Por eso, cuando una persona considera que su derecho no fue respetado, lo primero es identificar qué institución tiene sus datos y cuál es la autoridad competente para revisar su caso.

Defender tus datos también es ejercer tus derechos

La protección de datos personales no termina cuando entregamos nuestros datos a una institución, ni tampoco cuando presentamos una solicitud. Una verdadera cultura de protección de datos implica conocer los derechos, ejercerlos y saber qué hacer cuando la respuesta no es satisfactoria.

Si una institución no responde, existe un camino para inconformarse. Si responde, pero la persona considera que la respuesta no atiende su solicitud, también existen mecanismos para solicitar que el caso sea revisado. La finalidad no es generar conflictos innecesarios con las instituciones públicas, sino que las personas conozcan las herramientas que tienen a su alcance y puedan utilizarlas cuando lo necesiten.

En una sociedad donde cada vez más actividades requieren proporcionar información personal, saber cómo defender nuestros datos es tan importante como saber cómo protegerlos.



10.3 ¿Qué puede hacer el INFONL?



Cuando una persona considera que sus datos personales no fueron tratados correctamente por un sujeto obligado del Estado de Nuevo León, puede acudir al INFONL, dentro del ámbito de sus atribuciones.

El INFONL es la autoridad garante local en materia de protección de datos personales. Su función es contribuir a que este derecho sea respetado y proporcionar a las personas mecanismos para ejercerlo y defenderlo. Esto significa que el INFONL no sustituye a la institución que tiene los datos personales, su función es vigilar y garantizar que las reglas de protección de datos se cumplan, además de atender los procedimientos que la legislación establece cuando una persona considera que sus derechos fueron afectados.

Una de las principales herramientas con las que cuenta la sociedad es el recurso de revisión. Este recurso permite que una persona pida que se revise la actuación de un sujeto obligado cuando, por ejemplo, no recibió respuesta a su solicitud, recibió información incompleta, obtuvo datos que no corresponden con lo solicitado o se le negó el ejercicio de alguno de sus derechos. La legislación de Nuevo León establece diversos supuestos en los que procede este recurso y señala que puede presentarse ante la autoridad garante o ante la Unidad de Transparencia del responsable que atendió la solicitud.

Por otro lado, el INFONL también cuenta con el Procedimiento de Verificación, el cual es una atribución para verificar que los sujetos obligados cumplan con las leyes de protección de datos personales al llevar a cabo su tratamiento.

Por lo que, cuando una persona considere que una Institución Pública ha realizado un indebido tratamiento de su información personal, es decir, algún tratamiento que no se encuentre acorde a lo establecido en la ley, puede interponer una denuncia en materia de datos personales.

El INFONL puede revisar lo ocurrido

Cuando se presenta un recurso de revisión, el Instituto analiza la situación planteada y la información relacionada con el caso. Esto permite revisar si la actuación del sujeto obligado se ajustó a las disposiciones aplicables.

El procedimiento también contempla la posibilidad de buscar una solución mediante la conciliación entre la persona titular de los datos y el responsable. Si se alcanza un acuerdo, este puede tener efectos vinculantes y el INFONL verifica su cumplimiento. Si no se llega a una solución por esta vía, el procedimiento continúa hasta que se emita la resolución correspondiente.

La autoridad garante puede, según las circunstancias del caso, confirmar la respuesta de la institución, modificarla o revocarla, u ordenar la entrega de los datos personales cuando exista una omisión, conforme a lo previsto por la legislación estatal.

El INFONL también puede actuar para proteger este derecho

La labor del Instituto no se limita a resolver recursos de revisión. La legislación estatal también le atribuye facultades relacionadas con la verificación del cumplimiento de las obligaciones en materia de protección de datos personales y, cuando corresponde, con la determinación de medidas de apremio y sanciones. Asimismo, tiene entre sus funciones promover y difundir el derecho a la protección de datos personales y favorecer que las personas puedan ejercerlo en condiciones de accesibilidad.

Por ello, el trabajo del INFONL tiene dos dimensiones, las cuales se orientan a atender los problemas que ya se presentaron y a contribuir a que las instituciones conozcan y cumplan sus obligaciones para prevenirlos.

10.4 ¿Cómo puede ayudarte el INFONL?

Para la sociedad, todas estas atribuciones pueden resumirse en algo mucho más sencillo, el INFONL puede orientarte sobre tus derechos y, cuando corresponde, intervenir mediante los procedimientos establecidos para revisar si fueron respetados.

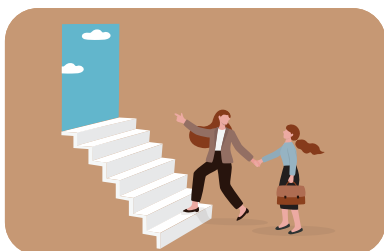
Esto es importante porque una persona que tiene un problema con sus datos personales puede no saber qué hacer después de recibir una respuesta negativa o cuando una institución simplemente no contesta. En esos momentos, el INFONL puede convertirse en un punto de orientación y defensa dentro de su ámbito de competencia.



Antes de acudir, reúne la información de tu caso

No necesitas preparar un expediente complicado. Sin embargo, es conveniente tener a la mano los documentos que permitan conocer qué ocurrió, tales como la solicitud que presentaste, el comprobante de recepción, la respuesta de la institución (si la recibiste), las comunicaciones relacionadas con el caso, y los documentos que ayuden a explicar tu situación. Esta información permite identificar con mayor facilidad qué ocurrió y qué mecanismo puede resultar aplicable.

También puedes pedir orientación



El INFONL cuenta con mecanismos para facilitar a la ciudadanía información y formatos relacionados con el ejercicio de los derechos sobre sus datos personales y con los medios de defensa. Su Unidad de Transparencia proporciona orientación y asesoría, y el Instituto dispone de información sobre el ejercicio de los derechos y los recursos correspondientes.

Por ello, si no sabes cómo presentar una solicitud o qué hacer después de recibir una respuesta con la que no estás de acuerdo, puedes buscar orientación antes de continuar. La finalidad es que las personas puedan ejercer sus derechos sin que el desconocimiento del procedimiento se convierta en una barrera.

Cuando se actualiza alguno de los supuestos previstos por la legislación, respecto a la atención de una solicitud de derechos ARCOP puedes presentar un recurso de revisión directamente con el sujeto obligado responsable, o bien a través de los medios establecidos por el INFONL.

En caso de considerar un tratamiento de tu información que no sea acorde a lo establecido en la Ley, puedes interponer una denuncia en materia de datos personales a través del Micrositio ubicado en el portal oficial del Instituto.



¿Y si quiero presentar un recurso de revisión?

Cuando se actualiza alguno de los supuestos previstos por la legislación, puedes presentar un recurso de revisión. En Nuevo León, la ley establece que el recurso puede presentarse ante la autoridad garante o ante la Unidad de Transparencia del responsable que atendió la solicitud. También contempla medios como el escrito, formatos y medios electrónicos autorizados.

La legislación establece, además, los elementos que debe contener el recurso, como identificar a la persona que recurre, señalar la solicitud y la respuesta que se impugna cuando exista, y explicar las razones por las que no está de acuerdo. No se trata de escribir un documento lleno de términos jurídicos, lo importante es explicar con claridad qué solicitaste, qué ocurrió y por qué consideras que tu derecho no fue respetado.

El INFONL como acompañante institucional

En materia de protección de datos personales, conocer a dónde acudir puede marcar una diferencia importante. Una persona puede saber que tiene derecho a acceder a sus datos, corregirlos, solicitar su cancelación u oponerse a determinado tratamiento, pero si desconoce qué hacer cuando una institución no respeta alguno de esos derechos, ese conocimiento queda incompleto.

Por eso, la existencia de una autoridad garante resulta fundamental. El INFONL no decide por la persona qué hacer con sus datos ni sustituye su voluntad, su función es ofrecer un marco institucional para que el derecho pueda ejercerse y, cuando exista una controversia, pueda ser revisada conforme a las reglas aplicables.

La protección de datos personales, entonces, no termina cuando entregamos nuestra información ni cuando presentamos una solicitud. También implica saber a quién acudir cuando necesitamos defenderla.

Una ruta sencilla para la sociedad

Si consideras que una institución pública de Nuevo León no respetó tus derechos sobre tus datos personales, puedes seguir la ruta que consiste en: identificar qué institución tiene tus datos; después, presentar la solicitud correspondiente; conservar el comprobante y toda comunicación



relacionada con ella; revisar la respuesta y verificar si atendió realmente lo que solicitaste; si existe un problema, identifica si procede un recurso de revisión; y finalmente, acude al INFONL o a la instancia que corresponda para recibir orientación o ejercer el mecanismo de defensa previsto por la legislación.

De esta manera, la protección de datos deja de ser un concepto lejano y se convierte en una herramienta que cualquier persona puede utilizar.

Para tener presente. El derecho a la protección de datos personales no consiste únicamente en saber que nuestros datos deben ser protegidos. También significa poder preguntar, solicitar, corregir, cuestionar y, cuando sea necesario, defender nuestros datos. El INFONL forma parte de ese camino en Nuevo León.

¿Cómo redacto un recurso de revisión en materia de protección de datos personales?

Explica los hechos de forma simple, no necesitas lenguaje jurídico, usando una expresión como “Pedí conocer los datos personales que la institución tiene sobre mí, pero no recibí respuesta. Solicito que se revise mi petición completa”.

Para facilitar este trámite, el INFONL cuenta con un formato de recurso de revisión que puedes llenar para presentar tu inconformidad. Esto permite contar con una herramienta sencilla para iniciar el procedimiento sin necesidad de redactar el recurso desde cero.



El formato de recurso de revisión en materia de protección de datos personales del INFONL, lo puedes descargar en el siguiente enlace:

https://infonl.mx/descargas/Formato_Recurso_de_Revision_en_materia_de_DP_INFONL.docx



Capítulo 11. Herramientas para protegerte

Conocer nuestros derechos es importante. Saber cómo ejercerlos es todavía más útil.

A lo largo de esta obra hemos hablado sobre los datos personales que compartimos todos los días, las instituciones que pueden tenerlos, las situaciones que pueden ponerlos en riesgo y los derechos que tenemos para ejercer un mayor control sobre nuestra información. Este último capítulo reúne herramientas para llevar ese conocimiento a la práctica.

Aquí encontrarás modelos sencillos para solicitar el ejercicio de tus derechos sobre tus datos personales, así como información que te permitirá identificar a la autoridad competente cuando necesites orientación o quieras presentar un recurso de revisión.

Los modelos que se presentan pueden servir como punto de partida. No es necesario copiarlos exactamente, lo importante es adaptar cada solicitud a la situación particular de la persona y proporcionar la información necesaria para que pueda ser atendida.



11.1 Formato oficial para ejercer tus derechos ARCOP

No necesitas elaborar desde cero un escrito para ejercer tus derechos de acceso, rectificación, cancelación u oposición. El INFONL cuenta con un Formato Único de Solicitud de Acceso, Rectificación, Cancelación y Oposición de Datos Personales, elaborado para facilitar a la ciudadanía el ejercicio de estos derechos.

El formato permite señalar el derecho que se desea ejercer y proporcionar la información necesaria para que el responsable pueda localizar los datos personales relacionados con la solicitud. El INFONL también establece algunas consideraciones específicas para cada derecho. Por ejemplo, en una solicitud de acceso puedes indicar la modalidad en la que prefieres recibir o consultar la información; para rectificación es importante señalar con precisión qué dato deseas corregir; para cancelación debes expresar las causas que motivan tu solicitud, y para oposición debes explicar las causas legítimas o la situación específica que motiva tu petición.





Consulta y utiliza el formato oficial del INFONL:

<https://infonl.mx/wp-content/uploads/2024/05/formato-nuevo-solicitud-ARCO.pdf>

Importante: El ejercicio de los derechos ARCOP es gratuito. La información deberá ser entregada de forma gratuita cuando la entrega no sea de más de veinte (20) hojas simples.

Antes de enviar una solicitud

No olvides revisar que identificaste a la institución correcta, explicaste claramente qué necesitas, señalaste el derecho que deseas ejercer, proporcionaste los elementos necesarios para localizar tus datos, acreditaste tu identidad o representación cuando corresponda, y conservaste una copia de la solicitud y su comprobante de recepción. Una solicitud clara facilita su atención.

11.2 Formato para presentar una denuncia



Si consideras que tu derecho a la protección de datos personales ha sido lesionado por alguna conducta u omisión de alguna autoridad estatal y municipal, cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos del Estado de Nuevo León, o presumes alguna violación a las disposiciones previstas en la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados para el Estado de Nuevo León y demás marco normativo, puedes interponer una denuncia ante el Instituto Estatal de Transparencia, Acceso a la Información y Protección de Datos Personales del Estado de Nuevo León (INFONL).



https://infonl.mx/descargas/Formato_de_Denuncia_en_materia_de_Datos_Personales_INFONL.docx

11.3 Directorio de autoridades competentes

Cuando se trata de proteger nuestros datos personales, saber a quién acudir es tan importante como conocer nuestros derechos. No todas las instituciones pertenecen al mismo ámbito de gobierno; por ello, la autoridad competente dependerá de quién tenga bajo su responsabilidad los datos personales y de la naturaleza del asunto. Para esta obra, el punto de referencia principal es el ámbito de Nuevo León, debido a que el INFONL es la autoridad garante local.

Autoridad garante de Nuevo León

El Instituto Estatal de Transparencia, Acceso a la Información y Protección de Datos Personales (INFONL) es la autoridad garante local en materia de transparencia, acceso a la información y protección de datos personales, dentro del ámbito de sus atribuciones. Entre sus funciones relacionadas con la protección de datos personales se encuentran conocer y resolver los recursos de revisión, promover el ejercicio del derecho y vigilar el cumplimiento de las obligaciones establecidas por la legislación aplicable.

¿Cuándo puede ser relevante acudir al INFONL? Cuando tus datos personales se encuentran bajo responsabilidad de un sujeto obligado estatal o municipal de Nuevo León y consideras que tus derechos no fueron respetados; por ejemplo, cuando no recibiste respuesta a una solicitud, recibiste una respuesta con la que no estás de acuerdo, te entregaron información incompleta, se negó el ejercicio de alguno de tus derechos, o se presentó alguna de las situaciones previstas por la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Nuevo León, para acudir al recurso de revisión.

Sitio oficial: INFONL



<https://infonl.mx/>

¿Y si la institución pública es federal?

Si la institución que tiene tus datos pertenece al ámbito federal, no corresponde acudir al INFONL. En ese caso debe acudir ante la Unidad de Protección de Datos Personales, la cual está adscrita a la Secretaría

Anticorrupción y Buen Gobierno del Poder Ejecutivo Federal a través de su órgano desconcentrado Transparencia para el Pueblo, quien es la autoridad competente conforme al ámbito de gobierno y a la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados. Esta distinción es importante porque la autoridad que puede conocer de un asunto depende, entre otros factores, de quién tiene bajo su responsabilidad los datos personales, ya sea del ámbito estatal o federal.

¿Y si mis datos están en manos de una empresa y/o institución privada?

Cuando el responsable de los datos pertenece al sector privado, se debe identificar la Ley Federal de Protección de Datos Personales en Posesión de los Particulares y la autoridad competente para ese caso es la Unidad de Protección de Datos Personales, la cual está adscrita a la Secretaría Anticorrupción y Buen Gobierno del Poder Ejecutivo Federal a través de su órgano desconcentrado Transparencia para el Pueblo.

Por ello, antes de presentar una inconformidad, conviene preguntarse quién tiene mis datos, especialmente si se trata de una institución pública estatal o federal, o una persona particular o empresa. La respuesta ayudará a determinar cuál es el camino adecuado.

Una última herramienta: tu propio registro

Además de los formatos anteriores, existe una herramienta que cualquier persona puede utilizar y que no requiere ningún trámite, llevar un pequeño registro de los lugares donde has proporcionado tus datos personales.

Tabla 11.1 Registro personal de datos compartidos.

Institución o empresa	¿Qué datos proporcioné?	¿Para qué los entregué?	Fecha aproximada
-----------------------	-------------------------	-------------------------	------------------

Este registro puede ayudarte a identificar quién podría tener determinada información y facilitar una futura solicitud.

Tus datos, tus decisiones

La protección de datos personales no debe quedarse en las páginas de una ley ni en los documentos de las instituciones; también debe formar parte de nuestras decisiones cotidianas. Antes de entregar información, podemos preguntarnos para qué será utilizada. Cuando una institución conserva nuestros datos, podemos conocer qué información tiene y ejercer los derechos que la legislación reconoce. Y cuando consideramos que nuestros derechos no fueron respetados, podemos buscar orientación y utilizar los mecanismos de defensa correspondientes.

Los formatos incluidos en este capítulo son una herramienta para comenzar. Conocer tus derechos es el primer paso. Ejercerlos es el siguiente.

11.4 Sitios oficiales

En internet es fácil encontrar información sobre protección de datos personales, pero no toda la información que aparece en una página web es confiable o está actualizada. Cuando necesites realizar una solicitud, consultar tus derechos o conocer un procedimiento, procura acudir directamente a los sitios oficiales de las instituciones responsables.



Una forma sencilla de identificar un sitio oficial es verificar quién publica la información, revisar que la dirección electrónica corresponda a la institución y evitar proporcionar datos personales en páginas a las que llegaste mediante enlaces desconocidos o mensajes que no esperabas.

Para los temas relacionados con esta obra, estas son algunas fuentes oficiales que pueden ser de utilidad.



El INFONL. El Instituto Estatal de Transparencia, Acceso a la Información y Protección de Datos Personales es la autoridad garante local de Nuevo León en las materias de transparencia, acceso a la información y protección de datos personales, dentro del ámbito de sus atribuciones. En su sitio oficial puedes consultar información sobre protección de datos personales, derechos, procedimientos, avisos de privacidad y otros recursos de interés ciudadano. <https://infonl.mx/>



Cámara de Diputados

El sitio de la Cámara de Diputados permite consultar el texto vigente de diversas leyes federales; es una fuente útil cuando necesitas verificar directamente el contenido de una disposición legal federal. Leyes federales de México:

<https://www.diputados.gob.mx/LeyesBiblio/index.htm>



Diario Oficial de la Federación

Es una fuente oficial para consultar decretos, reformas y publicaciones de carácter federal. Cuando encuentres información sobre una reforma legal en redes sociales, medios de comunicación o páginas particulares, puedes acudir al Diario Oficial para verificar la publicación correspondiente.

<https://www.dof.gob.mx>



Congreso del Estado de Nuevo León

El sitio del Congreso del Estado permite consultar las leyes estatales y conocer el marco jurídico aplicable en Nuevo León. Para esta obra resulta particularmente importante porque ahí puede consultarse la legislación estatal relacionada con la protección de datos personales en posesión de sujetos obligados.

<https://www.hcnl.gob.mx>

Antes de confiar en una página

Cuando busques información sobre tus datos personales, detente unos segundos y revisa quién publica la información, si es una institución oficial, si la dirección electrónica corresponde realmente a esa institución, si la información tiene fecha o se encuentra actualizada, y si te están pidiendo datos personales que no necesitas proporcionar. Estas preguntas pueden evitar que tomes decisiones a partir de información incorrecta o entregues tus datos en un sitio que no corresponde a la institución que buscas.



11.5 Micrositios del INFONL

El INFONL cuenta con espacios especializados en su sitio institucional para facilitar el acceso de la sociedad a información sobre sus derechos y obligaciones. Estos espacios pueden ser especialmente útiles cuando una persona necesita pasar de la información general a una acción concreta. Entre los contenidos relacionados con protección de datos personales se encuentran recursos sobre el ejercicio de derechos, avisos de privacidad y otros materiales de consulta.

Protección de datos personales

Este espacio reúne información y recursos para conocer el derecho a la protección de datos personales y los mecanismos para ejercerlo.

<https://infonl.mx/proteccion-de-datos-personales/proteccion-de-tus-datos-personales/>



Avisos de privacidad

Los avisos de privacidad son una herramienta importante para conocer qué ocurre con los datos personales que entregamos a una institución. El INFONL cuenta con un espacio dedicado a este tema, que puede servir como referencia para comprender su función y consultar información relacionada.

<https://infonl.mx/proteccion-de-datos-personales/avisos-de-privacidad/>



Derechos de las personas

Cuando quieras ejercer tus derechos sobre tus datos personales, consulta los recursos que el INFONL pone a disposición de la ciudadanía para conocer el procedimiento correspondiente.

<https://infonl.mx/proteccion-de-datos-personales/>



Una recomendación para utilizar los sitios oficiales

Los sitios institucionales pueden cambiar de diseño, dirección interna o nombre de sus secciones. Por eso, si un enlace deja de funcionar, lo recomendable es entrar directamente al sitio oficial del INFONL y utilizar su buscador o menú de navegación para localizar nuevamente la información.

Esto también reduce el riesgo de llegar a páginas falsas o sitios que imitan a una institución pública.

11.6 Lista de verificación antes de compartir tus datos

Todos los días entregamos información personal, lo hacemos al registrarnos en un servicio, realizar un trámite, comprar un producto, descargar una aplicación, participar en una actividad o llenar un formulario. Muchas veces proporcionamos nuestros datos automáticamente, sin detenernos a pensar qué estamos compartiendo.

Antes de hacerlo, vale la pena hacer una pausa. No se trata de desconfiar de todo ni de negarse a proporcionar información, sino de entender qué estamos entregando y por qué. Puedes utilizar esta lista como una pequeña herramienta antes de compartir tus datos.

Tabla 11.2 Antes de proporcionar mis datos, pregunto...

Pregunta	¿Por qué importa?
¿Quién me está solicitando esta información?	Identifica a la institución, empresa o persona que solicita tus datos.
¿Para qué necesitan mis datos?	Debes poder entender cuál es la finalidad de proporcionar la información.
¿Realmente necesitan todos estos datos?	Que un formulario tenga muchos espacios no significa que tengas que entregar información innecesaria.
¿Qué datos me están solicitando?	No es lo mismo proporcionar un nombre que entregar información financiera, médica, biométrica o cualquier otro dato que pueda requerir mayor protección.
¿Dónde puedo consultar el aviso de privacidad?	Si una institución está recabando tus datos personales, busca información sobre el tratamiento que dará a ellos.
¿Qué harán con mi información después?	Cuando corresponda, revisa si tus datos serán utilizados para otras finalidades o comunicados a terceros.

Pregunta	¿Por qué importa?
¿Estoy utilizando un sitio oficial o confiable?	Antes de proporcionar información en internet, verifica la dirección del sitio y quién se encuentra detrás de él.
¿Estoy compartiendo más información de la necesaria?	Antes de enviar una fotografía, documento o identificación, pregúntate si realmente es necesario proporcionar toda la información que contiene.
¿Estoy seguro de que quiero compartir esta información?	Una vez que proporcionamos nuestros datos, pueden incorporarse a registros, sistemas o bases de datos y su control puede resultar más difícil.

Una pausa antes de compartir

Puedes convertir estas preguntas en un hábito. Antes de entregar información personal, detente unos segundos y piensa quién la solicita, para qué la necesita, si es necesario proporcionarla, cómo será utilizada y dónde puedes consultar el aviso de privacidad. Si puedes responder estas preguntas, estarás tomando una decisión más informada.

Cuando te solicitan una copia de tu identificación

Una situación frecuente es que alguien solicite una copia de nuestra identificación oficial. Antes de entregarla, conviene preguntar por qué la necesitan, si es indispensable para realizar el trámite, quién conservará la copia, para qué será utilizada y si existe otra forma de acreditar tu identidad.

No se trata de negarse automáticamente, algunos trámites requieren acreditar la identidad y pueden existir disposiciones que justifiquen la solicitud de determinados documentos. Lo importante es no entregar una copia de nuestra identificación por costumbre o sin conocer la razón.

Cuando una aplicación solicita muchos permisos

Algo parecido ocurre con las aplicaciones y servicios digitales, una aplicación puede solicitar acceso a diferentes elementos del dispositivo. Antes de aceptar, revisa qué permisos está solicitando y pregúntate si guardan relación con el servicio que quieres utilizar. Por ejemplo, si una aplicación necesita conocer tu ubicación para ofrecerte



una función específica, puede tener sentido que solicite este permiso; pero si solicita acceso a información que aparentemente no guarda relación con el servicio, vale la pena detenerse y revisar las condiciones antes de continuar. No todos los permisos son necesarios para todas las aplicaciones.

Una regla sencilla para la vida cotidiana

No necesitas memorizar leyes para comenzar a proteger tus datos. Puedes empezar con una regla muy sencilla: antes de compartir un dato personal, pregunta quién lo solicita, para qué lo necesita y si realmente es necesario entregarlo. Esa pequeña pausa puede ayudarte a tomar mejores decisiones.

➤ REFERENCIAS

- Boletín Mexicano De Derecho Comparado, 1(120). <https://doi.org/10.22201/ij.24484873e.2007.120.3933>
- Calcano Monts, M. A. (2019). Big data, big data analytics y datos personales en los tiempos del Internet: de la autorregulación estadounidense al Reglamento General de Protección de Datos de la Unión Europea. *Estudios en Derecho a la Información*, (8), 21-44. <https://doi.org/10.22201/ij.25940082e.2019.8.13882>
- Cámara de Diputados del H. Congreso de la Unión. (2002). Ley de los Derechos de las Personas Adultas Mayores. Texto vigente, última reforma publicada en el Diario Oficial de la Federación el 14 de junio de 2024. <https://www.diputados.gob.mx/LeyesBiblio/pdf/LDPAM.pdf>
- Cámara de Diputados del H. Congreso de la Unión. (2025). Ley Federal de Protección de Datos Personales en Posesión de los Particulares. Texto vigente, última reforma publicada en el Diario Oficial de la Federación el 14 de noviembre de 2025. <https://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf>
- Cámara de Diputados del H. Congreso de la Unión. (2025). Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados. Texto vigente, última reforma publicada en el Diario Oficial de la Federación el 14 de noviembre de 2025. <https://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPSO.pdf>
- Cámara de Diputados del H. Congreso de la Unión. (2026). <https://www.diputados.gob.mx/LeyesBiblio/index.htm>
- Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros. (2021, junio). Aunque te vengan con cuentas, no sueltes tus datos. Proteja su Dinero, 22(255), 20–22. <https://revista.condusef.gob.mx/destacados-2/2021/06/aunque-te-vengan-con-cuentas-no-sueltes-tus-datos/>
- Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros. (s. f.). Sistema de Registro de Prestadores de Servicios Financieros (SIPRES). Gobierno de México. <https://webapps.condusef.gob.mx/SIPRES/jsp/pub/index.jsp>
- Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros. (s. f.). Sistema de Registro de Prestadores de Servicios Financieros (SIPRES). Gobierno de México. <https://webapps.condusef.gob.mx/SIPRES/jsp/pub/index.jsp>
- Congreso del Estado de Nuevo León. (1917). Constitución Política del Estado Libre y Soberano de Nuevo León. Texto vigente. https://www.hcnl.gob.mx/trabajo_legislativo/leyes/leyes/constitucion_politica_del_estado_libre_y_soberano_de_nuevo_leon/
- Congreso del Estado de Nuevo León. (2005). Ley de los Derechos de las Personas Adultas Mayores en el Estado de Nuevo León. Texto vigente. https://www.hcnl.gob.mx/trabajo_legislativo/leyes/leyes/ley_de_los_derechos_de_las_personas_adultas_mayores_en_el_estado_de_nuevo_leon/
- Congreso del Estado de Nuevo León. (2015). Ley de los Derechos de Niñas, Niños y Adolescentes para el Estado de Nuevo León. Texto vigente. https://www.hcnl.gob.mx/trabajo_legislativo/leyes/leyes/ley_de_los_derechos_de_ninas_ninos_y_adolescentes_para_el_estado_de_nuevo_leon/
- Congreso del Estado de Nuevo León. (2019). Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Nuevo León. Texto vigente, última reforma publicada el 11 de diciembre de 2019. https://www.hcnl.gob.mx/trabajo_legislativo/leyes/leyes/ley_de_proteccion_de_datos_personales_en_posesion_de_sujetos_obligados_del_estado_de_nuevo_leon/
- Congreso del Estado de Nuevo León. (2026). <https://www.hcnl.gob.mx>
- Constitución Política de los Estados Unidos Mexicanos. (1917). Texto vigente. <https://www.diputados.gob.mx/LeyesBiblio/pdf/CPEUM.pdf>
- Davara Fernández de Marcos, I., Cervantes Padilla, A. y Barco Vega, G. (2019). Remisión de datos personales. En I. Davara Fernández de Marcos (Coord.), *Diccionario de protección de datos personales: Conceptos fundamentales* (p. 768). Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales. https://inicio.inai.org.mx/PublicacionesComiteEditorial/DICCIONARIO_PDP_digital.pdf
- Davara Fernández de Marcos, I., Cervantes Padilla, A. y Barco Vega, G. (2019). Remisión de datos personales. En I. Davara Fernández de Marcos (Coord.), *Diccionario de protección de datos personales: Conceptos fundamentales* (p. 768). Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales. https://inicio.inai.org.mx/PublicacionesComiteEditorial/DICCIONARIO_PDP_digital.pdf
- Diario Oficial de la Federación. (2025, 20 de marzo). Decreto por el que se expiden la Ley General de Transparencia y Acceso a la Información Pública; la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados; la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, y se reforma el artículo 37, fracción XV, de la Ley Orgánica de la Administración Pública Federal. https://www.dof.gob.mx/nota_detalle.php?codigo=5752569
- Diario Oficial de la Federación. (2025, 20 de marzo). Diario Oficial de la Federación. (2026). <https://www.dof.gob.mx>
- García González, A. (2007). La protección de datos personales: derecho fundamental del siglo XXI. Un estudio comparado.
- Guardia Nacional CERT-MX. (2023, 28 de diciembre). Suplantación de identidad. Gobierno de México. <https://www.gob.mx/gncertmx/articulos/suplantacion-de-identidad-264141>
- Guardia Nacional. (2025, 10 de noviembre). Tips y recomendaciones. Gobierno de México. <https://www.gob.mx/gncertmx/articulos/tips-y-recomendaciones-264060>
- Guardia Nacional. (2025, 16 de abril). Recomendaciones para evitar afectaciones ante mensajes dirigidos con fines de fraude. Gobierno de México. <https://www.gob.mx/gncertmx/articulos/155283>
- Guardia Nacional. (2026, 13 de enero). Recomendaciones para proteger tu información personal en redes sociales. Gobierno de México. <https://www.gob.mx/gncertmx/articulos/recomendaciones-para-proteger-tu-informacion-personal-en-redes-sociales>

- Guardia Nacional. (2026, 4 de marzo). Recomendaciones para prevenir la usurpación de identidad derivada de ataques cibernéticos a instituciones o empresas reconocidas. Gobierno de México. <https://www.gob.mx/gncertmx/articulos/recomendaciones-para-prevenir-la-usurpacion-de-identidad-derivada-de-ataques-ciberneticos-a-instituciones-o-empresas-reconocidas>
- IBM. (2025). ¿Qué es la información de identificación personal (PII)? <https://www.ibm.com/es-es/think/topics/pii>
- Instituto Estatal de Transparencia, Acceso a la Información y Protección de Datos Personales. (2026). Página oficial <https://infonl.mx/>
- Instituto Estatal de Transparencia, Acceso a la Información y Protección de Datos Personales. (2026). Avisos de Privacidad. <https://infonl.mx/proteccion-de-datos-personales/aviso-de-privacidad/>
- Instituto Estatal de Transparencia, Acceso a la Información y Protección de Datos Personales. (2024). Formato de Recurso de Revisión en materia de Datos Personales. https://infonl.mx/descargas/Formato_Recurso_de_Revision_en_materia_de_DP_INFONL.docx
- Instituto Estatal de Transparencia, Acceso a la Información y Protección de Datos Personales. (2024). Formato Único Solicitud de Acceso, Rectificación, Cancelación y Oposición de Datos Personales. <https://infonl.mx/wp-content/uploads/2024/05/formato-nuevo-solicitud-ARCO.pdf>
- Instituto Estatal de Transparencia, Acceso a la Información y Protección de Datos Personales. (2024, 30 de mayo). Protección de tus datos personales. <https://infonl.mx/?p=210>
- Instituto Estatal de Transparencia, Acceso a la Información y Protección de Datos Personales. (2024). Solicitud de acceso al INFONL. <https://infonl.mx/acceso-a-la-informacion/solicitud-acceso/>
- Instituto Estatal de Transparencia, Acceso a la Información y Protección de Datos Personales. (2022). Medios para solicitar información. <https://infonl.mx/unidad-de-transparencia/medios-para-solicitar-informacion/>
- Instituto Estatal de Transparencia, Acceso a la Información y Protección de Datos Personales. (2025, 27 de marzo). Acuerdo 07/2025 por el cual se establecen las disposiciones en materia de transparencia, acceso a la información y protección de datos personales que deben regir en el Estado durante el régimen de transición. https://infonl.mx/descargas/mn/Acuerdo_07_2025_Disposiciones_Transicion2025.pdf
- Instituto Estatal de Transparencia, Acceso a la Información y Protección de Datos Personales. (2026). Protección de datos personales. <https://infonl.mx/proteccion-de-datos-personales/>
- Instituto Estatal de Transparencia, Acceso a la Información y Protección de Datos Personales. (2026a). Padrón de sujetos obligados responsables en materia de protección de datos personales del Estado de Nuevo León. <https://infonl.mx/conocenos-borrador/padron-de-sujetos-obligados-datos-personales/>
- Instituto Estatal de Transparencia, Acceso a la Información y Protección de Datos Personales. (2026). Programa Anual de Trabajo 2026. https://infonl.mx/descargas/mn/PLAN_ANUAL_TRABAJO_INFONL_2026.pdf
- Instituto Federal de Telecomunicaciones. (s. f.). Micrositio de ciberseguridad para usuarios de servicios de telecomunicaciones. <https://www.ift.org.mx/comunicacion-y-medios/comunicados-ift/es/el-ift-presenta-micrositio-de-ciberseguridad-para-usuarios-de-servicios-de-telecomunicaciones>
- Instituto Nacional de Estadística y Geografía (INEGI). (2025). Encuesta Nacional Sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares (ENDUTIH) 2025. Reporte de Resultados. <https://www.inegi.org.mx/programas/endutih/2025/>
- Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales. (2017). Lineamientos Generales de Protección de Datos Personales para el Sector Público. Diario Oficial de la Federación. <https://datos-personales.scjn.gob.mx/sites/default/files/normativa-materia/Lineamientos-Generales-Proteccion-Datos-Personales-Sector-Publico.pdf>
- Mendoza Enríquez, O. A. (2021). El derecho de protección de datos personales en los sistemas de inteligencia artificial. *Revista IUS*, 15(48), 179-207. <https://doi.org/10.35487/rius.v15i48.2021.743>
- Sánchez Díaz, M. F. (2023). El derecho a la protección de datos personales en la era digital. *Revista Eurolatinoamericana de Derecho Administrativo*, 10(1), e235. <https://doi.org/10.14409/reodoeda.v10i1.12626>
- Santana Vargas, Á. D. (2010). Desarrollo de una interfaz cerebro-computadora para comunicación mediante P300 [Tesis de doctorado, Universidad Nacional Autónoma de México]. Repositorio Institucional UNAM. <https://tesinamdocumentos.dgb.unam.mx/pdt2010/abril/0656795/Index.html>
- Secretaría de Seguridad y Protección Ciudadana. (2024, 29 de noviembre). La SSPC advierte sobre páginas de comercio electrónico y servicios de paquetería falsos. Gobierno de México. <https://www.gob.mx/sspc/prensa/la-sspc-advierte-sobre-paginas-de-comercio-electronicas-y-servicios-de-paqueteria-falsos>
- Secretaría de Seguridad y Protección Ciudadana. (2026, 12 de febrero). SSPC emite recomendaciones para el uso responsable, seguro y constructivo de las tecnologías digitales. Gobierno de México. <https://www.gob.mx/sspc/prensa/sspc-emite-recomendaciones-para-el-uso-responsable-seguro-y-constructivo-de-las-tecnologias-digitales>
- Secretaría de Seguridad y Protección Ciudadana. (2026, 16 de junio). La SSPC emite recomendaciones para el uso adecuado de redes sociales. Gobierno de México. <https://www.gob.mx/sspc/prensa/la-sspc-emite-recomendaciones-para-el-uso-adecuado-de-redes-sociales>
- Secretaría de Seguridad y Protección Ciudadana. (2026, 7 de mayo). En el Día Mundial de la Contraseña, la SSPC emite recomendaciones para fortalecer la seguridad digital. Gobierno de México. <https://www.gob.mx/sspc/prensa/en-el-dia-mundial-de-la-contrasena-la-sspc-emite-recomendaciones-para-fortalecer-la-seguridad-digital>
- Secretariado Ejecutivo del Sistema Nacional de Seguridad Pública. (2025, 26 de noviembre). Recomendaciones para una ciberseguridad efectiva. Gobierno de México. <https://www.gob.mx/sesnspp/articulos/recomendaciones-para-una-ciberseguridad-efectiva>
- UNESCO. (2025). Recomendación sobre la Ética de la Neurotecnología. <https://www.unesco.org/es/legal-affairs/recommendation-ethics-neurotechnology>
- Universidad Nacional Autónoma de México, "Neurodatos, nuevo oro digital, advierte Anahibey Becerril", Dirección General de Comunicación Social, 8 de junio de 2025. https://www.dgcs.unam.mx/boletin/bdboletin/2025_384.html



info.nl
INSTITUTO ESTATAL DE TRANSPARENCIA, ACCESO A LA
INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

Instituto Estatal de Transparencia,
Acceso a la Información y Protección
de Datos Personales (INFONL)
Av. Constitución 1465-1 Centro
Monterrey, Nuevo León, México

