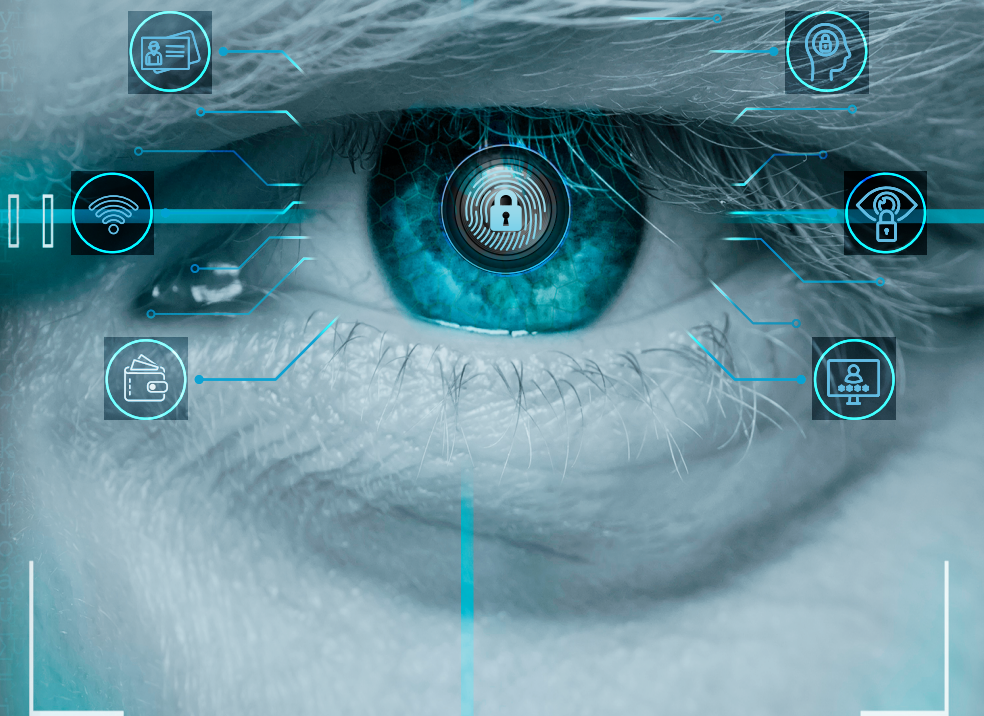


PROTECCIÓN DE DATOS PERSONALES

Conoce y protege
tu información

Versión abreviada



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

PROTECCIÓN DE DATOS PERSONALES

Conoce y protege
tu información

Versión abreviada

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: 978-968-9780-06-9

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

Presentación	7
Cómo usar este libro	10
Glosario	11

BLOQUE I • EL DIAGNÓSTICO

¿Por qué debería importarme?



Capítulo 1. Tus datos personales, el valor que no sabías que tenían	17
1.1 ¿Qué son los datos personales?	17
1.2 ¿Por qué son importantes?	19
1.3 Ejemplos cotidianos sobre donde dejas tus datos sin darte cuenta	20
1.4 Privacidad, protección de datos y acceso a la información: tres derechos, no uno	22
1.5 El derecho a la protección de datos personales en México	23
1.6 ¿Qué ley protege tus datos?	25
Capítulo 2. Un universo de datos	27
2.1 Tipos de datos personales, de un vistazo	27
2.2 Datos personales sensibles: los que requieren más cuidado	29
2.3 Datos en registros de seguridad y justicia	30
2.4 Casos ilustrativos	31

Capítulo 3. ¿Quién tiene tus datos y por qué los quiere? 32

3.1 Sector público y sector privado 32

3.2 ¿Cuándo pueden compartir tus datos? 35

3.3 ¿Qué autoridad puede ayudarte? 36

Capítulo 4. Protege tus datos en el mundo digital 38

4.1 Situaciones que pueden comprometer tus datos personales 38

4.2 Hábitos digitales básicos 40

4.3 ¿Qué hacer si algo ya ocurrió? 41

4.4 Casos ilustrativos 42

BLOQUE II • GUÍA DE SUPERVIVENCIA

Casos prácticos



Capítulo 5. Tus datos personales en la vida cotidiana 44

5.1 ¿Qué te pueden pedir según el contexto? 44

5.2 ¿Cuándo te solicitan más de lo necesario? 46

5.3 Copia de tu identificación oficial 48

5.4 Cámaras de seguridad, fotografías y videograbaciones 50

Capítulo 6. Protección de datos para grupos de atención prioritaria 52

6.1 Niñas, niños y adolescentes 52

6.2 Personas adultas mayores 54

6.3 Grupos de atención prioritaria 56

Capítulo 7. Tecnologías emergentes y protección de datos personales 58

7.1 ¿Cómo utiliza la inteligencia artificial tus datos personales? 58

7.2 ¿Qué es el perfilamiento y por qué influye en lo que ves en internet? 60

7.3 Neurodatos: cuando la tecnología puede conocer lo que piensas 61

BLOQUE III • TU PODER DE DEFENSA

Acción



Capítulo 8. Tus derechos sobre tus datos personales (ARCOP) 64

8.1 Los cinco derechos ARCOP 65

8.2 Distinciones que conviene tener claras 66

8.3 ¿Cuándo pueden limitarse estos derechos? 68

Capítulo 9. ¿Cómo ejercer tus derechos ARCOP

paso a paso? 69

9.1 Ruta para ejercer tus derechos ARCOP 70

Capítulo 10. ¿Qué hacer si tus derechos ARCOP no son respetados por sujetos obligados en materia de protección de datos personales de Nuevo León? 74

10.1 ¿Qué hago si un sujeto obligado en materia de protección de datos personales de Nuevo León no me responde o no estoy de acuerdo? 75

10.2 ¿Qué necesitas para presentar el recurso de revisión en materia de protección de datos personales? 76

10.3 ¿Cómo redacto un recurso de revisión en materia de protección de datos personales? 78

10.4 El Instituto Estatal de Transparencia, Acceso a la Información y Protección de Datos Personales (INFONL) protege tus datos personales 83

Capítulo 11. Herramientas para protegerte 84

11.1 Modelo para ejercer tus derechos ARCOP 85

11.2 Formato para presentar una denuncia 90

11.3 Directorio de autoridades competentes 94

11.4 Micrositios del INFONL 96

11.5 Lista de verificación antes de compartir tus datos personales 97

Referencias 99



Presentación

En el Instituto Estatal de Transparencia, Acceso a la Información y Protección de Datos Personales (INFONL) sabemos que tus datos personales te acompañan en prácticamente todo lo que haces, cuando vas al médico, cuando inscribes a tus hijas o hijos en la escuela, cuando solicitas un crédito, cuando usas una aplicación en tu teléfono o simplemente cuando compartes una fotografía. Esa información te identifica, cuenta parte de tu historia y, cuando se usa de forma indebida, puede exponerte a riesgos muy concretos, desde un fraude hasta la suplantación de tu identidad. Por eso consideramos indispensable poner a disposición de todas las personas un material que explique, en un lenguaje cercano y sin tecnicismos innecesarios, qué son tus datos personales, quién puede tenerlos y, sobre todo, qué puedes hacer para protegerlos.

Esta publicación busca responder a una necesidad muy concreta, que las personas conozcan sus datos personales, distingan cuándo su información está siendo tratada correctamente y cuándo no, además de saber qué herramientas tienen a su alcance para ejercer su derecho a la protección de datos personales. No es un texto pensado solo para quienes ya conocen el tema. Está construido para acompañar a cualquier persona, desde el primer momento en que se pregunta "¿por qué me piden este dato?" hasta el momento en que decide ejercer sus derechos ante una institución pública o un particular.

En sus páginas encontrarás un recorrido organizado en tres grandes momentos. Primero, un diagnóstico que explica qué son los datos personales, por qué son valiosos y quién puede tenerlos en su poder. Después, una guía de situaciones prácticas acerca de los datos personales y su uso en la vida diaria, el cuidado especial que merecen niñas, niños, adolescentes, personas adultas mayores y otros grupos de atención prioritaria, así como los retos que traen consigo la inteligencia artificial y otras tecnologías emergentes. Finalmente, la parte más orientada a la acción, explica los derechos de Acceso, Rectificación, Cancelación, Oposición y Portabilidad (lo que en este libro llamamos ARCOP), la forma de ejercerlos paso a paso y qué hacer si una institución pública no te responde o no estás de acuerdo con su respuesta, incluyendo los formatos y el directorio de autoridades a las que puedes acudir.

Está dirigida a cualquier persona que realice trámites o servicios públicos en Nuevo León, así como a toda la sociedad que busca una primera orientación clara antes de tomar una decisión sobre sus datos personales, como puede ser qué compartir, con quién hacerlo y bajo qué condiciones. Su utilidad no depende de tener conocimientos jurídicos previos, basta con la disposición de informarse.

Este documento forma parte de la obra *"Protección de datos personales. Herramientas para conocer y proteger tu información"*, de la cual se deriva esta versión abreviada. Su propósito es ofrecer una aproximación más ágil y accesible a los contenidos fundamentales sin perder el enfoque, el sentido ni la esencia de la obra original.

Decidimos ofrecer esta versión porque sabemos que no todas las personas tienen el tiempo o la necesidad de consultar, en un primer momento, el desarrollo jurídico completo de cada tema. Por ello, esta edición conserva el contenido sustantivo de la obra extendida, pero lo presenta de manera más sencilla y dinámica, mediante recuadros breves, ejemplos cotidianos y pasos concretos que puedes aplicar de inmediato.

Si deseas profundizar en el fundamento jurídico o conocer el desarrollo completo de algún tema, los recuadros **"Para profundizar"** te remiten directamente a la sección correspondiente de la obra extendida *"Protección de datos personales. Herramientas para conocer y proteger tu información"*.

Con esta publicación, el Instituto Estatal de Transparencia, Acceso a la Información y Protección de Datos Personales (INFONL) reafirma su compromiso institucional con la divulgación, la promoción y el ejercicio efectivo del derecho a la protección de tus datos personales. Estamos seguros que cuando las personas se encuentran debidamente informadas, es posible construir una sociedad con mayor capacidad de decidir sobre su propia información y ese es, precisamente, el propósito de esta obra, que cada persona conozca sus derechos y cuente con las herramientas necesarias para ejercerlos.

Brenda Lizeth González Lara

Consejera Presidenta

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



Cómo usar este libro

Este libro que tienes en tus manos es la versión abreviada de la obra completa que el INFONL ha desarrollado sobre la protección de datos personales. Conserva el mismo enfoque, la misma estructura por bloques y la esencia de sus contenidos; lo que cambia es la forma de presentarlos, que se basa en una selección, síntesis y adecuación editorial de la obra extendida *“Protección de datos personales. Herramientas para conocer y proteger tu información”*, pensada para que puedas consultarla de manera más ágil, práctica y accesible en tu vida cotidiana; sin que ello implique una obra distinta ni un enfoque diferente al de origen.

Por eso, este libro está pensado para consultarse, no solo para leerse de principio a fin.

Cada capítulo se abre con un recuadro, titulado **"Lo esencial"**, que resume en tres o cuatro líneas lo que vas a encontrar. Si tu duda es puntual, ese recuadro y las tablas o flujogramas del capítulo suelen ser suficientes.

A lo largo del texto encontrarás cuatro tipos de recuadros:

Recuadro	Para qué sirve
Idea clave	El concepto central de la sección, en una o dos frases.
Ejemplo	Un caso cotidiano que ilustra el concepto.
Qué hacer	Una acción concreta que puedes tomar.
Para profundizar	Remite a la sección correspondiente de la versión extendida, cuando quieras más detalle jurídico.

Si buscas un término específico, revisa el glosario o el índice temático al inicio del libro.



Glosario

ARCOP. Acrónimo que usa este libro para agrupar cinco derechos sobre tus datos personales (Acceso, Rectificación, Cancelación, Oposición y Portabilidad). La legislación identifica como “ARCO” a los primeros cuatro y regula la portabilidad de forma específica.

Acceso. Derecho que permite a una persona conocer qué datos personales tiene una institución o empresa sobre ella, cómo los utiliza y, cuando corresponda, obtener una copia de esa información.

Rectificación. Derecho que permite pedir que se corrija un dato incorrecto, incompleto o desactualizado. Corregir no es lo mismo que eliminar.

Cancelación. Derecho que permite solicitar que tus datos sean eliminados de un registro, cuando corresponda conforme a la ley. No siempre procede, algunas instituciones tienen obligación legal de conservar cierta información.

Oposición. Derecho que permite pedir que tus datos no se usen para determinado fin, sin que necesariamente se eliminen del registro.

Portabilidad. Derecho que permite obtener o transmitir ciertos datos personales en un formato utilizable, cuando la ley lo prevé; por ejemplo, al cambiar de un servicio digital a otro.

Aviso de privacidad. Documento ya sea físico, electrónico o en audio que una institución o empresa debe darte a conocer para informarte qué datos personales recopila, para qué los usará, si los compartirá y cómo puedes ejercer tus derechos sobre ellos.

Biometría o datos biométricos. Características físicas, fisiológicas o de comportamiento que pueden utilizarse para identificar a una persona, como las huellas dactilares, determinados rasgos faciales, la voz o el iris.

Correo electrónico. Medio de comunicación digital que permite enviar y recibir mensajes y archivos. Una dirección de correo electrónico puede constituir un dato personal cuando permite identificar o hacer identificable a una persona.

CURP. Clave Única de Registro de Población. Es un dato utilizado para identificar individualmente a las personas en México y, por ello, debe tratarse como dato personal.

Datos personales. Toda información relacionada con una persona física que permite identificarla o hacerla identificable, de forma directa o indirecta (LPDDPPSONL, 2019).

Datos personales sensibles. Información que revela la esfera más íntima de una persona o cuyo mal uso podría generar discriminación o un riesgo grave, como el origen racial o étnico, el estado de salud, características biométricas, creencias religiosas o filosóficas, opiniones políticas, preferencias sexuales. Recibe una protección reforzada.

Datos de contacto. Información que permite comunicarse con una persona, como domicilio, número telefónico o correo electrónico.

Datos de identificación. Información que permite distinguir o identificar a una persona, como nombre, firma, CURP, RFC, fecha de nacimiento, edad o nacionalidad.

Grupos de atención prioritaria. Personas o grupos que enfrentan mayores obstáculos para ejercer sus derechos y requieren medidas de atención, protección o apoyo.

Identificación oficial. Documento emitido por una autoridad competente que permite acreditar la identidad de una persona.

Identificable. Persona cuya identidad pueda determinarse, directa o indirectamente, mediante información disponible, siempre que ello no requiera medios o actividades desproporcionadas.

Inteligencia artificial. Tecnología que permite a sistemas informáticos realizar tareas que normalmente requieren capacidades asociadas con la inteligencia humana, como analizar información, reconocer patrones, generar contenido o realizar predicciones.

INFONL. Instituto Estatal de Transparencia, Acceso a la Información y Protección de Datos Personales de Nuevo León. Es la autoridad garante local que resuelve recursos de revisión, orienta a la sociedad y vigila el cumplimiento de

las obligaciones de protección de datos por parte de sujetos obligados estatales y municipales.

LFPDPPP. Ley Federal de Protección de Datos Personales en Posesión de los Particulares. Regula cómo empresas, asociaciones y particulares (bancos, hospitales privados, escuelas particulares, comercios, plataformas digitales) deben tratar tus datos personales.

LGPDPSSO. Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados. Regula cómo las autoridades e instituciones públicas (dependencias, municipios, universidades públicas, poderes Legislativo y Judicial) deben tratar tus datos personales.

LPDPPSONL. Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Nuevo León. Aplica, a los sujetos obligados estatales y municipales de Nuevo León, en lo que no se oponga a la LGPDPPSO.

Neurodatos. Información obtenida a partir de la actividad o funcionamiento del cerebro mediante determinadas tecnologías.

Perfilamiento. Proceso mediante el cual se analizan datos de una persona para identificar características, preferencias, comportamientos o posibles intereses y, a partir de ello, realizar clasificaciones, predicciones o tomar decisiones.

Privacidad. Esfera de la vida de una persona que debe mantenerse protegida frente a intromisiones injustificadas.

Recurso de revisión. Medio de defensa que puedes presentar ante el INFONL (o ante la Unidad de Transparencia de la institución responsable) cuando no recibiste respuesta a tu solicitud ARCOP, o cuando no estás de acuerdo con la respuesta recibida.

Redes sociales. Plataformas digitales que permiten crear perfiles, comunicarse, publicar contenidos e interactuar con otras personas.

Responsable. Persona física o jurídica, pública o privada, que decide sobre la finalidad y los medios del tratamiento de los datos personales.

RFC (Registro Federal de Contribuyentes). Clave utilizada para identificar a las personas físicas y morales en materia fiscal. Cuando se relaciona con una persona física, constituye un dato personal.

Sector privado. Ámbito integrado por empresas, profesionistas y organizaciones particulares que realizan tratamiento de datos personales.

Sector público. Ámbito integrado por autoridades, dependencias, entidades, órganos y demás instituciones públicas que realizan tratamiento de datos personales en el ejercicio de sus atribuciones.

Sujeto obligado. Cualquier institución pública (dependencia, municipio, organismo autónomo, universidad pública, poder Legislativo o Judicial, fiscalía, entre otros) que trata datos personales y debe cumplir la LPDDPPSONL.

Titular. Persona física a quien corresponden los datos personales.

Tratamiento de datos personales. Cualquier acción que se realiza con un dato personal, tal como obtenerlo, usarlo, conservarlo, compartirlo o eliminarlo.

Transferencia. Comunicación de datos personales a una persona, institución o autoridad distinta del responsable, en los casos y bajo las condiciones establecidas por la legislación aplicable.

Transparencia. Principio y práctica que busca que las personas puedan conocer de manera clara cómo actúan las instituciones y, en materia de datos personales, cómo y para qué se utiliza su información.

Unidad de Transparencia. Área de los sujetos obligados encargada de realizar diversas funciones relacionadas con transparencia, acceso a la información y protección de datos personales, conforme a las atribuciones que establece la legislación.

Versión pública. Documento o parte de un documento que puede darse a conocer públicamente después de proteger, ocultar o eliminar la información que legalmente debe mantenerse reservada o confidencial, incluidos determinados datos personales.

Vulnerabilidad. Condición o circunstancia que puede aumentar la posibilidad de que una persona enfrente dificultades para proteger sus datos personales o ejercer sus derechos.

BLOQUE I

EL DIAGNÓSTICO

¿Por qué debería importarme?

Capítulo 1.

Tus datos personales, el valor que no sabías que tenían



Lo esencial

Un dato personal es cualquier información que te identifica o te hace identificable, sola o combinada con otras. México protege este derecho desde la Constitución, con dos leyes distintas según quién trate tus datos (sector público, sector privado o profesionista). Este capítulo te da el mapa completo en pocas páginas.

1.1 ¿Qué son los datos personales?

Un dato personal es toda información relacionada con una persona física que permite identificarla o hacerla identificable, de forma directa o indirecta. Así lo definen tanto la LGPDPPSO como la LFPDPPP (2025, art. 3, fracc. XXI), que comparten esta definición para dar un concepto uniforme entre el sector público y el privado.





Idea clave

Eres identificado cuando un solo dato revela quién eres (tu nombre con tu fotografía).

Eres identificable cuando la combinación de varios datos (edad, profesión, ciudad, lugar de trabajo) permite reconocerte, aunque ninguno por separado lo haga. Esta segunda forma es cada vez más relevante, debido a que la tecnología permite cruzar información de distintas fuentes para construir perfiles muy precisos.



Tabla 1.1 Clasificación de datos personales

Categoría	Ejemplos
Identificación	Nombre, firma, RFC, CURP, fecha de nacimiento, edad y nacionalidad.
Contacto	Domicilio, teléfono, correo electrónico.
Laborales o profesionales	Puesto, historial académico, trayectoria laboral y cédula profesional.
Patrimoniales o financieros	Cuentas bancarias, bienes muebles e inmuebles, ingresos y créditos.

También son datos personales los expedientes clínicos, historial académico, información laboral y financiera, imágenes de videovigilancia y, en ciertos casos, registros que



genera el uso de dispositivos electrónicos (dirección IP, ubicación, historial de navegación, entre otros), que pueden afectar de forma directa o indirecta.



1.2 ¿Por qué son importantes?

Los datos personales forman parte de tu identidad y hacen posible el ejercicio de otros derechos, como salud, educación, seguridad social, servicios financieros, programas públicos y derechos político-electorales; de igual forma, permiten que puedas identificarte y gestionar trámites y servicios.



Idea clave

Proporcionar datos personales no es, por sí mismo un riesgo, es una condición necesaria para acceder a derechos y servicios. El riesgo aparece cuando esos datos se usan de forma indebida.

Tabla 1.2 Cuando el uso indebido de tus datos te afecta

Puede ocurrir	¿En qué consiste?
Suplantación de identidad	Alguien usa tus datos para hacerse pasar por ti y actuar en tu nombre.
Fraude	Se usa tu información para engañarte y obtener un beneficio económico.
Discriminación	Se usa indebidamente información de salud, discapacidad, origen étnico u otra condición para limitar tus derechos u oportunidades.



Puede ocurrir**¿En qué consiste?**Pérdida de
privacidadDivulgación o acceso no autorizado a tu
información.Daño a tu
reputación

Difusión de información que perjudica tu imagen.

**Qué hacer**

Cuando una institución informa con claridad para qué recaba tus datos y los protege, genera confianza. Eso no es un obstáculo burocrático, es la forma en que la ley busca que las cosas funcionen.



1.3 Ejemplos cotidianos sobre donde dejas tus datos sin darte cuenta.

Ámbitos donde compartes datos personales todos los días

- **Salud:** Nombre, antecedentes médicos, alergias y, en algunos casos, información genética (dato sensible).
- **Educación:** Identificación oficial, CURP, historial académico, datos de contacto de madres/padres/tutores.
- **Servicios financieros:** Identificación oficial, RFC, domicilio, información patrimonial.
- **Trabajo:** CURP, RFC, número de seguridad social, datos bancarios para tu pago.



- **Trámites de gobierno:** Identificación oficial, comprobante de domicilio, firma.
- **Compras en línea:** Nombre, domicilio de entrega, datos de pago.
- **Apps y plataformas digitales:** Ubicación, identificadores del dispositivo, permisos que concedes.
- **Redes sociales:** Nombre de usuario, fotos, publicaciones e interacciones.



Idea clave

Lo importante es tener plena conciencia sobre el tipo de información que compartimos, a quien se la compartimos y para qué será usada esta información. Cabe destacar que todo tratamiento de datos personales debe ajustarse a los siguientes principios y deberes: licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información, responsabilidad y seguridad.

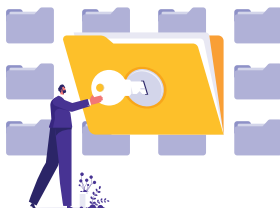


1.4 Privacidad, protección de datos y acceso a la información: tres derechos, no uno

Estos tres términos suelen confundirse, pero cada uno protege algo distinto.

Tabla 1.3 Privacidad, protección de datos y acceso a la información

	Privacidad	Protección de datos	Acceso a la información
¿Qué es?	Tu derecho a mantener un ámbito de vida libre de intromisiones.	Tu derecho a decidir sobre el tratamiento de la información que te identifica.	Tu derecho a solicitar información pública que generan las autoridades.
¿Qué protege?	Tu vida privada, comunicaciones y relaciones familiares.	Tu nombre, domicilio, expediente clínico, datos biométricos o financieros.	Fortalece la transparencia y la rendición de cuentas, y permite conocer cómo actúan las instituciones públicas.
Ejemplo	Una conversación privada con tu médico.	Que una escuela use tus datos solo para lo que informo.	Consultar el presupuesto de una obra pública.





Idea clave

La privacidad, la protección de datos y el acceso a la información no compiten entre sí, se complementan. Puedes solicitar información sobre requisitos de trámites en las instituciones públicas (acceso a la información) sin que eso autorice a que te den acceso a la información personal de algún usuario que lo haya gestionado en específico (protección de datos personales).

En aplicación al principio de máxima publicidad, cuando en el ejercicio del derecho de acceso a la información se solicite a un sujeto obligado un documento que contenga información pública y, a su vez, información confidencial como datos personales, deberá elaborarse una versión pública que permita el acceso a la información de naturaleza pública, mediante el testado de las partes o secciones clasificadas como confidenciales, debidamente fundado y motivado.

1.5 El derecho a la protección de datos personales en México

La protección de datos personales está reconocida en el artículo 16 de la Constitución Política de los Estados Unidos Mexicanos. Menciona que toda persona tiene derecho a la protección de sus datos personales, así como al acceso,



rectificación y cancelación de los mismos, y a manifestar su oposición (CPEUM, art. 16, segundo párrafo). Esto no depende de la voluntad de ninguna institución, es un derecho humano que debe respetarse.



Idea clave

Gracias a este derecho puedes conocer quién tiene tus datos, saber para qué los usarán, pedir corrección si están mal, solicitar su cancelación cuando proceda, y oponerte a su tratamiento en los casos que la ley prevé. (Estos son los derechos ARCOP, los cuales se explican a fondo en el Capítulo 8).



Quien trata tus datos también tiene obligaciones, como recabar solo lo necesario, informar con claridad, proteger la información con medidas de seguridad, evitar accesos no autorizados y facilitar que ejerzas tus derechos.



1.6 ¿Qué ley protege tus datos?

Tabla 1.4 ¿Qué ley aplica?

Ley / Ordenamiento	¿Qué establece?	¿A quién aplica?
Constitución Política de los Estados Unidos Mexicanos (CPEUM)	Reconoce el derecho humano a la protección de los datos personales y los derechos de acceso, rectificación, cancelación, oposición y portabilidad.	Protege a todas las personas y constituye el fundamento constitucional de este derecho.
Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados	Establece las bases, principios, deberes y procedimientos para proteger los datos personales en posesión de sujetos obligados.	Cualquier autoridad, entidad, órgano y organismo de los poderes ejecutivo, legislativo y judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos, en el ámbito federal, estatal y municipal o de las demarcaciones territoriales de la Ciudad de México.
Ley de Protección de Datos Personales en Posesión de Sujetos Obligados de Nuevo León (LPDDPPSONL)	Regula la protección y el tratamiento de datos personales en posesión de sujetos obligados de Nuevo León, conforme al marco jurídico vigente.	En el ámbito estatal y municipal, cualquier autoridad, entidad, órgano y organismo de los poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos.
Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP)	Regula la protección y el tratamiento de datos personales en posesión de particulares.	A personas físicas y morales de carácter privado sujetas a esta legislación, como empresas, profesionistas y organizaciones particulares.





Qué hacer

Si entregaste tus datos a una institución pública federal, aplica la LGPDPPSO, en caso de ser una institución pública estatal de Nuevo León aplica la LPDDPPSONL. Si fue a una empresa o particular, aplica la LFPDPPP. Sin importar cuál sea, conservas tus derechos sobre tu información.



Para profundizar

En Nuevo León, las disposiciones de la LPDPPSONL continúan siendo aplicables en aquello que no contravenga la legislación general vigente y de conformidad con las disposiciones transitorias aplicables. Este criterio fue establecido por el INFONL mediante el Acuerdo 07/2025 (INFONL, 2025). Si deseas conocer más, te invitamos a consultar nuestra versión extendida: *“Protección de datos personales. Herramientas para conocer y proteger tu información”*.



Capítulo 2.

Un universo de datos



Lo esencial

No todos los datos personales son iguales ni implican los mismos riesgos para nuestra privacidad. En este capítulo encontrarás una tabla sencilla que te ayudará a identificar qué tipo de dato es cada uno y por qué algunos requieren mayor cuidado que otros. La idea es que puedas reconocerlos fácilmente, sin necesidad de conocer definiciones jurídicas complicadas.

2.1 Tipos de datos personales, de un vistazo

Tabla 2.1 Categorías de datos personales (no sensibles)

Categoría	¿Qué incluye?	¿Cuándo se solicita?	¿Por qué protegerla?
Identificación	Nombre, fecha y lugar de nacimiento, fotografía, firma, CURP, RFC, teléfono, domicilio y correo personal.	En casi cualquier trámite, contrato o servicio.	Su mal uso facilita el fraude o suplantación de identidad.
Patrimonial	Bienes inmuebles, vehículos, inversiones, deudas.	Al gestionar créditos, seguros, trámites notariales o fiscales, bancarios.	Puede revelar tu situación económica y facilitar fraudes o extorsión.



Categoría	¿Qué incluye?	¿Cuándo se solicita?	¿Por qué protegerla?
Financiera	Cuenta bancaria, CLABE, historial crediticio, tarjetas.	Gestión de créditos, inversiones y pagos.	Un acceso no autorizado puede causar pérdidas económicas.
Laboral	Puesto, antigüedad, empleador, salario, evaluaciones, currículum, incapacidades médicas.	Contratación y trámites de seguridad social.	Por ser información de naturaleza confidencial.
Académica	Nivel de estudios, títulos, cédula profesional, calificaciones.	Ingreso a instituciones educativas, procesos de admisión.	Forma parte de tu trayectoria personal y profesional.



Idea clave

Ninguna institución o empresa debe pedirte más de lo necesario para la finalidad concreta que justifica el trámite. Todas tienen la obligación de proteger estos datos contra acceso, alteración o pérdida no autorizados.



2.2 Datos personales sensibles: los que requieren más cuidado



Idea clave

Un dato es sensible cuando revela la esfera más íntima de una persona o su mal uso podría generar discriminación o un riesgo grave, no por el tipo de trámite en que aparece, sino por sus consecuencias si se divulga.

Tabla 2.2 Categorías de datos sensibles

Categoría	Ejemplos
Origen racial o étnico	Pertenencia a un pueblo indígena, adscripción afromexicana.
Estado de salud presente o futuro	Expediente clínico, diagnósticos, discapacidades, información genética.
Características biométricas	Huellas, iris, retina, reconocimiento facial.
Creencias religiosas, filosóficas o morales	Religión, convicciones espirituales o filosóficas.
Opiniones políticas	Militancia partidista, participación política.
Preferencias sexuales	Orientación sexual.





Qué hacer

Comparte solo lo necesario, verifica que solo te soliciten los datos indispensables para el trámite o servicio que vas a realizar, lee el aviso de privacidad, evita publicar información médica o biométrica en redes sociales y conserva tus documentos en lugares seguros.

2.3 Datos en registros de seguridad y justicia

Los expedientes de investigación, denuncias, procesos judiciales y registros penitenciarios contienen datos personales de denunciante, víctimas, testigos, personas imputadas y servidores públicos involucrados, entre otros.



Idea clave

Que exista el derecho de acceso a la información pública no significa que todo lo que las autoridades tienen sea público. Divulgar indebidamente esta información puede afectar una investigación, la presunción de inocencia o la seguridad de víctimas y testigos, por eso su acceso está sujeto a reglas específicas, y el ejercicio de algunos derechos sobre estos datos puede tener limitaciones o procedimientos particulares.



2.4 Casos ilustrativos

Ejemplo de inscripción universitaria

Sofía entrega acta de nacimiento, CURP y foto (identificación), certificado de bachillerato (académico), domicilio y contacto, e información médica (sensible). La universidad solo debe pedir lo estrictamente necesario para el expediente escolar.



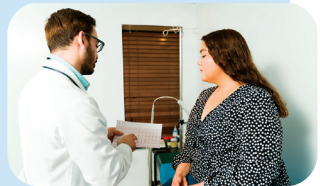
Ejemplo de crédito bancario

Miguel entrega identificación y RFC, comprobante de domicilio, y estados de cuenta e historial crediticio (financiero/patrimonial) para que el banco evalúe su capacidad de pago.



Ejemplo de consulta médica

Laura entrega nombre (identificación) y antecedentes médicos, alergias y diagnóstico (sensible), información que solo debe usarse para su atención.



Capítulo 3.

¿Quién tiene tus datos y por qué los quiere?



Lo esencial

Tus datos pueden estar en manos de una autoridad o de una empresa, y cada una se rige por una ley distinta, pero ambas tienen la misma obligación de protegerlos. Aquí está la diferencia entre ambos sectores, cuándo pueden compartir tu información y a qué autoridad acudir según tu caso.

3.1 Sector público y sector privado

Cuando compartes tus datos con una institución pública (dependencia, municipio, escuela pública, hospital público, etc.) o con una empresa privada (banco, aseguradora, tienda en línea, etc.), es importante que recuerdes que, en ambos casos, conservas tu derecho sobre esa información; es decir, el hecho que la hayas compartido y que alguien más la tenga, no significa que pueda ser usada para fines distintos a los que tú autorizaste.



Tabla 3.1 Sector público vs. sector privado

Aspecto	Sector público	Sector privado
¿Quién trata los datos?	Cualquier autoridad, entidad, órgano y organismo de los poderes Legislativo, Ejecutivo y Judicial, órganos autónomos, fideicomisos, fondos públicos y partidos políticos del estado de Nuevo León, que deciden y determinan los fines, medios y demás cuestiones relacionadas con determinado tratamiento de datos personales.	Empresas, comercios, asociaciones, profesionistas y sindicatos y cualquier otra persona física o moral que reciba y ejerza recursos públicos o realice actos de autoridad en el ámbito federal, estatal y municipal.
¿Para qué los usa?	Para ejercer atribuciones legales, prestar servicios públicos y garantizar derechos.	Para ofrecer bienes o servicios, celebrar contratos y cumplir obligaciones legales.
¿Qué ley aplica?	Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Nuevo León.	Ley Federal de Protección de Datos Personales en Posesión de los Particulares.



Aspecto	Sector público	Sector privado
¿Qué debe hacer?	Cumplir con los principios, deberes y demás obligaciones de acuerdo al marco normativo en la materia, así como tratar los datos personales que tienen en su posesión para finalidades determinadas y vinculadas con sus atribuciones.	Cumplir los principios, deberes y demás obligaciones previstas por la ley de la materia, incluido informar sobre el tratamiento mediante el aviso de privacidad.



Idea clave

Aunque el sector público y el privado se rigen por normas distintas, ambos deben proteger los datos personales, limitar su tratamiento a información adecuada y necesaria para las finalidades correspondientes, adoptar medidas de seguridad y respetar los derechos de las personas titulares. La diferencia está principalmente en quién trata los datos, con qué finalidad y bajo qué régimen jurídico.



Ejemplo

Dar tu nombre, domicilio y CURP a un hospital público (sector público) y a una aseguradora privada (sector privado) implica dos regímenes legales distintos, pero en ambos casos existe la obligación de proteger tu información.



3.2 ¿Cuándo pueden compartir tus datos?

Tus datos personales no pueden compartirse libremente. Una transferencia debe cumplir los requisitos establecidos por la ley y, cuando corresponda, contar con tu consentimiento. Sin embargo, existen casos en los que la legislación permite transferir datos sin solicitarlo.

Tabla 3.2 Ejemplos de casos en los que la ley permite compartir datos

Situación	¿Con qué finalidad pueden comunicarse?
Atención médica	Para dar continuidad al tratamiento o cumplir obligaciones sanitarias.
Procedimientos administrativos	Cuando una autoridad debe remitir un expediente a otra institución competente.
Procesos judiciales	Cuando una autoridad jurisdiccional o ministerial lo requiera conforme a sus atribuciones.
Contratación de servicios	Cuando es necesario comunicar datos a proveedores que participan en el servicio.





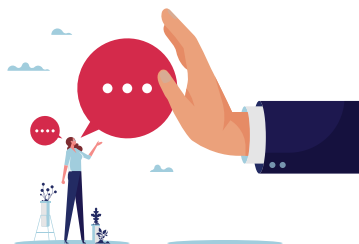
Qué hacer

El aviso de privacidad debe indicar si tus datos podrían compartirse y con qué finalidad. Si no lo dice, pregunta.

3.3 ¿Qué autoridad puede ayudarte?

Tabla 3.3 A quién acudir según el caso

Si el problema es con...	¿Quién puede ayudarte?
Una dependencia del Gobierno Federal	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.
Una dependencia estatal, un municipio, por ejemplo, Poder Ejecutivo, Poder Legislativo, Poder Judicial, fideicomisos y sindicatos.	El Instituto Estatal de Transparencia, Acceso a la Información y Protección de Datos Personales (INFONL).
Una empresa o un particular	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.





Qué hacer

Si consideras que alguna institución pública o privada, profesionista u organización particular vulnera tus derechos, primero identifica cuál es el problema, reúne la información y los documentos que pueden ayudarte a demostrar la situación. Presenta tu solicitud o reclamación ante la dependencia pública o el particular que trató tu información. Si no la resuelve o no responde a tiempo, acude a la autoridad competente (el procedimiento completo se desarrolla en los capítulos 9 y 10).

Ejemplo

María pidió a una empresa de telefonía corregir su domicilio y acompañó los documentos necesarios para demostrar que la información registrada era incorrecta; sin embargo, la empresa se negó sin explicar por qué. Posteriormente acudió a la autoridad competente y, con esa orientación, pudo continuar defendiendo sus derechos. Las autoridades no solo intervienen cuando hay un conflicto, también orientan sobre cómo actuar.



Capítulo 4.

Protege tus datos en el mundo digital



Lo esencial

La mayoría de los riesgos digitales no vienen de la tecnología, sino de decisiones cotidianas como: qué compartimos, qué permisos aceptamos y a quién le creemos. Este capítulo te comparte una tabla de riesgos, una *checklist* de hábitos y qué hacer si algo ya salió mal.

4.1 Situaciones que pueden comprometer tus datos personales

Gran parte de nuestra vida ocurre en medios digitales, donde diariamente hacemos trámites, compras, pagos y conversaciones desde el teléfono. Cada una de esas actividades implica compartir datos personales y la tecnología no siempre es el problema, sino que, con frecuencia lo es la forma en que la usamos.



Idea clave

No es necesario ser experto en tecnología para protegerte. Basta con reconocer las situaciones cotidianas que representan un riesgo y detenerte un momento antes de actuar.



Tabla 4.1 Riesgos cotidianos y cómo prevenirlos

Situación	¿Qué puede ocurrir?	¿Qué puedes hacer?
Publicar fotografías de documentos oficiales en redes sociales.	Otras personas utilicen tu información y hacer mal uso de ellos.	Evita compartir imágenes de documentos que contengan tus datos personales.
Instalar aplicaciones sin revisar los permisos.	La aplicación accede a información que no necesita para funcionar.	Lee los avisos de privacidad y, principalmente, los permisos que otorgas antes de aceptar la descarga de aplicaciones.
Usar la misma contraseña en varias cuentas.	Si una cuenta se ve comprometida, las demás también quedan en riesgo.	Usa contraseñas distintas y activa la verificación en dos pasos.
Conectarte a Wi-Fi pública para pagos o apps bancarias.	Tu información puede quedar expuesta durante la conexión.	Cuando se trate siempre de datos de este tipo, usa una red privada o los datos móviles de tu teléfono.
Dar datos por llamada, mensaje o correo sin verificar quién los solicita.	Puedes entregar información a alguien que vaya a usarla de forma indebida.	Confirma la identidad de quien solicita tus datos antes de compartirlos.
Aceptar solicitudes de personas desconocidas en redes sociales.	Tu información personal, la de tus amigos y familiares pueden quedar expuestas.	Acepta solo a quien realmente conoces.



Situación	¿Qué puede ocurrir?	¿Qué puedes hacer?
Compartir tu ubicación en tiempo real.	Pueden ubicar dónde estás y con ello poner en riesgo tu integridad.	Comparte esa información después de regresar, no en el momento.
Abrir enlaces de mensajes inesperados.	Puedes poner en riesgo tu información y ser objeto de ciberataques.	Verifica el remitente y si es necesario, opta por entrar al sitio oficial.

Ejemplo

Ana instaló una app para editar fotos. Al revisar los permisos, notó que pedía acceso a su ubicación, contactos y micrófono, nada de eso era necesario para editar imágenes. Los negó todos y la app siguió funcionando igual.

4.2 Hábitos digitales básicos

Antes de compartir y para proteger tu información, recuerda:

- Usa contraseñas distintas para todas tus cuentas y activa la verificación en dos pasos.
- Nunca compartas contraseñas ni códigos de seguridad, aunque te los pidan “para confirmar tu identidad”.
- Mantén actualizado el sistema operativo de tus dispositivos y las aplicaciones que utilizas.
- Descarga aplicaciones de sitios confiables y consulta los avisos de privacidad para revisar qué permisos autorizas.



- Antes de dar clic en un enlace, detente a pensar si esperabas ese mensaje o si conoces a quien lo envió.
- Verifica siempre la identidad de quien solicita tus datos al utilizar canales oficiales, no el contacto que te dejaron en el mensaje.
- Revisa la configuración de privacidad de tus redes sociales periódicamente.
- Destruye documentos con datos personales antes de desecharlos.



Idea clave

Ninguna institución seria (apps bancarias, gubernamentales o de otro tipo) te pedirá jamás una contraseña, NIP o código de seguridad por teléfono, mensaje o correo. Si te lo piden de esta manera, es una señal de alerta.

4.3 ¿Qué hacer si algo ya ocurrió?

No siempre es posible evitar un incidente. Si crees que tus datos pudieron quedar expuestos, lo que importa es actuar rápido, no ignorar el problema.





Qué hacer

- Cambia tus contraseñas de inmediato, comienza por las cuentas más sensibles (correo, apps bancarias).
- Cierra las sesiones abiertas en tus cuentas desde otros dispositivos.
- Activa medidas de seguridad adicionales si están disponibles (verificación en dos pasos).
- Comunícate directamente con la institución correspondiente a través de sus canales oficiales.
- Revisa los movimientos recientes de tus cuentas.
- Conserva los mensajes, correos o evidencias relacionados con el incidente.
- Pide orientación sobre los pasos que correspondan a tu caso.

4.4 Casos ilustrativos



Ejemplo 1

Sofía publicó una foto de su identificación oficial recién obtenida. Aunque cubrió algunos datos, se veían su nombre completo, parte de su CURP y

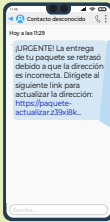
el código QR. Al notar el riesgo, eliminó la publicación.

¿Qué aprendemos?

Un documento oficial contiene más datos de los que parece a primera vista; revisa la imagen completa de cualquier



identificación oficial antes de publicarlo, no solo lo que quieres mostrar. Sofía nunca tendrá la certeza de si alguien, en ese poco tiempo que la publicó, guardó esa información.



¡URGENTE! La entrega de tu paquete se retrasó debido a que la dirección es incorrecta. Dirígete al siguiente link para actualizar la dirección: <https://paquete-actualizar.z39xi8k...>

Ejemplo 2

Laura recibió un mensaje de texto sobre un paquete “pendiente de entrega” con un enlace para confirmar su domicilio. No había hecho ninguna compra reciente, así que no lo abrió. Después supo que otras personas habían recibido el mismo mensaje.

¿Qué aprendemos?

No todo mensaje urgente es real; verificar antes de actuar evita la mayoría de estos intentos de fraude.



Para profundizar

La versión extendida “*Protección de datos personales. Herramientas para conocer y proteger tu información*” de este capítulo incluye dos casos adicionales sobre reutilización de contraseñas y permisos de aplicaciones con el mismo desarrollo que encontrarás en la Tabla 4.2 “Buenas prácticas para proteger tus datos en redes sociales e internet”.



Capítulo 5.

Tus datos personales en la vida cotidiana



Lo esencial

En trámites, escuela, salud, finanzas o apps, la pregunta es siempre la misma a saber: ¿por qué necesitan este dato y qué relación tiene con lo que estoy haciendo? Esta tabla te da las respuestas más comunes por contexto; las tres secciones siguientes profundizan en los casos que requieren más cuidado como tu identificación, tu imagen y cuando sientes que te piden información de más.

5.1 ¿Qué te pueden pedir según el contexto?

Tabla 5.1 Qué datos esperar y qué revisar, por contexto

Contexto	¿Qué datos suelen pedirte?	¿Qué preguntar antes?	Señal de alerta
Gestión de trámites y servicios en el sector público y privado	Datos de identificación y de contacto.	¿Para qué los necesitan? ¿Qué tipo de datos van a recabar? ¿Por cuánto tiempo van a resguardar mis datos? ¿Dónde puedo consultar el aviso de privacidad?	Alguien fuera de la institución pública o privada te pide datos adicionales por WhatsApp o redes sociales “para completar el trámite”.



Contexto	¿Qué datos suelen pedirte?	¿Qué preguntar antes?	Señal de alerta
Escuela	Datos de contacto, identificación y académicos.	¿Para qué los necesitan? ¿Qué tipo de datos van a recabar? ¿Por cuánto tiempo van a resguardar mis datos? ¿Dónde puedo consultar el aviso de privacidad?	Te piden reenviar documentos escolares fuera de los canales oficiales de la escuela.
Servicios de salud	Datos de identificación, datos de contacto, datos de salud (antecedentes médicos, diagnósticos, tratamientos y, en algunos casos, información genética).	¿Quién tendrá acceso a mi expediente? ¿Cómo se protegerá esta información? ¿Para qué los necesitan? ¿Qué tipo de datos van a recabar? ¿Por cuánto tiempo van a resguardar mis datos? ¿Dónde puedo consultar el aviso de privacidad?	Te piden compartir o publicar resultados médicos completos sin una razón clara.
Servicios financieros	Datos de identificación y contacto, así como información financiera y patrimonial, según el producto o servicio: ingresos, cuentas, créditos, seguros u otra información relacionada.	¿La institución está registrada (SIPRES de la CONDUSEF)? ¿Revisé el aviso de privacidad?	Te piden un depósito para “activar” un crédito, o acceso a tus contactos, fotos o micrófono para un servicio financiero.
Aplicaciones móviles	Datos de identificación o contacto, ubicación, fotografías u otra información relacionada con el uso de la aplicación. Además, la app puede solicitar permisos para acceder a recursos del dispositivo, como la cámara, el micrófono, la ubicación o la lista de contactos.	¿Los datos y permisos solicitados guardan relación con las funciones que quiero utilizar? ¿Puedo limitar esos accesos?	Una app de función simple (clima, transporte) pide permisos que no tienen relación con lo que hace.



Ejemplo

Alguien acude a una oficina pública a realizar un trámite y entrega su identificación y comprobante de domicilio, como se le solicitó. Después recibe un mensaje de una persona que dice trabajar ahí, pidiéndole que envíe por WhatsApp una foto de su tarjeta bancaria “para completar el trámite”.

Entregar los documentos por el canal oficial es considerado seguro, pero dárselos a alguien que realmente no tienes la certeza de que labore en la oficina pública donde gestionaste dicho trámite, es un acto riesgoso.



Para profundizar

La versión extendida *“Protección de datos personales. Herramientas para conocer y proteger tu información”* desarrolla cada uno de estos cinco contextos por separado, con ejemplos adicionales y el fundamento legal específico para instituciones públicas y privadas en cada caso, que encontrarás en Capítulo 5. “Tus datos personales en la vida cotidiana”.

5.2 ¿Cuándo te solicitan más de lo necesario?

No existe una lista que determine automáticamente cuándo una solicitud es indebida, pero sí hay señales que deben hacerte preguntar antes de entregar un dato, estas se encuentran en cualquiera de los cinco contextos de la tabla 5.1.



Señales para estar atento:

- Te piden información que no está relacionada con el trámite o servicio.
- No te explican qué harán con tus datos.
- Te solicitan datos sensibles para un servicio sencillo.
- Te piden documentos adicionales sin explicar por qué.
- Te piden enviar información por un medio que no reconoces como oficial.



Idea clave

Un dato aislado puede parecer inofensivo, pero combinado con otros (nombre + teléfono + domicilio + fecha de nacimiento) puede revelar mucho más de lo que crees. No entregues información por costumbre, siempre pregunta, revisa el aviso de privacidad y decide.



Qué hacer

Si no sabes por qué te piden un dato, pregunta directamente: “¿para qué necesitan este dato?”, “¿es obligatorio para el trámite?”, “¿dónde puedo consultar el aviso de privacidad?”. Si se trata de una institución pública y tienes dudas, puedes acudir a su Unidad de Transparencia.



5.3 Copia de tu identificación oficial

Tu identificación contiene varios datos en un solo documento, como nombre, fotografía, firma, domicilio, fecha de nacimiento, CURP, huella. Por eso, antes de entregar una copia (no solo mostrarla) vale la pena detenerte.



Idea clave

Mostrar una identificación no es lo mismo que entregar una copia. Si solo necesitan comprobar quién eres, puedes preguntar si basta con mostrar el original.

Tabla 5.2 Antes de entregar una copia de tu identificación

Situación	Pregúntate
Te solicitan una copia.	¿Realmente es necesaria o basta con mostrarla?
Te dicen que es requisito.	¿Dónde está establecido ese requisito?
Te piden enviarla por internet.	¿El sitio o medio es oficial?
No te explican para qué la quieren.	¿Cuál es la finalidad?
Ya no necesitas continuar el trámite.	¿Qué sucederá con los datos que ya entregaste?





Qué hacer

Si debes entregar datos personales, primero pide que te muestren el aviso de privacidad, verifica quién la recibirá, usa un medio oficial, pregunta la finalidad y, si quieres una precaución adicional, puedes escribir sobre la copia una leyenda como “Copia entregada exclusivamente para el trámite de _____, ante _____, con fecha _____”.

Esto no sustituye las obligaciones legales de quien la recibe, pero ayuda a dejar constancia del propósito.

Ejemplo

A Carlos le pidieron una copia de su identificación oficial en una institución, para un trámite oficial, él preguntó para qué la necesitaban, se le explicó y la entregó por el medio indicado. En otra ocasión, alguien le pidió una foto de su identificación oficial por una app de mensajería personal; sin poder explicar por qué, Carlos no la envió hasta confirmar quién era esa persona y para qué la necesitaba.



5.4 Cámaras de seguridad, fotografías y videograbaciones

Tu imagen es un dato personal cuando permite identificarte. Las cámaras de seguridad pueden estar en oficinas de gobierno, escuelas, hospitales, bancos, comercios o espacios públicos, y quien sea responsable de ellas debe usar las imágenes solo para la finalidad por la que fueron obtenidas.



Idea clave

Que exista una cámara no es, por sí mismo, una violación a tus datos. Las instituciones públicas y privadas que realizan tratamientos de datos personales mediante videovigilancia, deben contar con un aviso de privacidad que informe sobre el uso de estos datos. El problema surge cuando una grabación se comparte o publica, sin ser una institución autorizada para ello.

Antes de publicar una fotografía o video donde aparecen personas:

- ¿Se puede identificar a las personas en la imagen?
- ¿Dónde fue tomada? ¿Revela dónde vives o qué haces habitualmente?
- ¿Aparecen niñas, niños o adolescentes? Su información requiere cuidado especial.
- ¿Tienes una razón real para hacerla pública?
- ¿Quién podrá verla una vez publicada?



Ejemplo

En un comercio ocurrió un incidente y el encargado publicó en redes sociales el video de la cámara de seguridad para pedir ayuda a la ciudadanía. El video también mostraba a otras personas presentes que no tenían relación con lo ocurrido, sus imágenes quedaron expuestas sin necesidad. Si el establecimiento considera que la grabación puede ser útil para esclarecer un hecho, debe entregarla a las autoridades competentes, en lugar de hacerla pública por cuenta propia. La difusión pública de imágenes para apoyar una investigación corresponde a las autoridades facultadas para ello y debe realizarse conforme a las disposiciones aplicables. Antes de hacer pública una grabación, hay que pensar en todas las personas que aparecen en ella, no solo en el propósito original.



Capítulo 6.

Protección de datos para grupos de atención prioritaria



Lo esencial

Niñas, niños y adolescentes, personas adultas mayores y personas en situación de mayor vulnerabilidad no pierden sus derechos por su condición; al contrario, requieren de sistemas de apoyo que permitan garantizar la protección de sus datos personales. Necesitar apoyo para ejercer un derecho no es lo mismo que perder el control sobre tus propios datos.

6.1 Niñas, niños y adolescentes

Antes de publicar una fotografía o compartir información de un menor, pregúntate:

- ¿Se puede ver su rostro, su escuela (uniforme, letrero) o su ubicación en la imagen?
- ¿Revela dónde vive?, ¿dónde estudia o su rutina diaria (horario)?
- ¿Realmente es necesario hacerla pública o basta con compartirla de forma privada?
- ¿Aparecen otros menores en la imagen?





Idea clave

Ninguna de estas preguntas busca prohibir compartir momentos familiares. Simplemente pretenden evitar que, al combinar varios datos “aparentemente inofensivos” (nombre, escuela, horario, ubicación, etc.); alguien pueda construir una imagen completa de la vida de un menor y con ello ponerlo en riesgo. En Nuevo León se reconoce el derecho de niñas, niños y adolescentes a la protección de sus datos personales y privacidad, con el interés superior de la niñez como criterio rector, acorde con la Ley de los Derechos de Niñas, Niños y Adolescentes para el Estado de Nuevo León.



Qué hacer

En lugar de “no uses internet”, enseña “antes de compartir algo, piensa quién podrá verlo”. Un menor puede aprender frases simples (“no quiero compartir esa información”, “voy a preguntarle primero a mi mamá o papá”, “no conozco a esa persona”); y debe saber que puede acudir a un adulto de confianza si algo en internet le genera incomodidad, sin sentir que hizo algo malo por pedir ayuda.



Nota

Las escuelas manejan expedientes, calificaciones, fotografías e información médica de sus estudiantes. Las familias pueden preguntar qué datos tienen de su hija o hijo, para qué los usan y dónde consultar el aviso de privacidad; eso también es parte de proteger sus datos.

6.2 Personas adultas mayores**Idea clave**

El reto no es la edad ni la falta de habilidad tecnológica; actualmente muchas personas adultas mayores usan aplicaciones y redes sociales sin problema. El reto es reconocer cuándo una llamada, mensaje o correo busca presionar para obtener información antes de que la persona pueda verificar.

Señales de una comunicación fraudulenta

- Te dicen que actúes de inmediato (“su cuenta será cancelada hoy”, “no cuelgue”).
- Te piden contraseñas, NIP, códigos de seguridad o datos completos de tarjetas: ninguna institución legítima los solicita así.
- Usan un tono de urgencia o de premio inesperado (“ganó un premio”, “confirme sus datos para no perder su beneficio”).



- Te dicen “no le diga a nadie” o “no cuelgue mientras verifica”.



Qué hacer

Cuelga y comunícate directamente con la institución usando el número oficial de tu tarjeta, estado de cuenta o sitio institucional, nunca el número que te dieron en la misma llamada o mensaje.



Idea clave

Ayudar con un trámite a un familiar no es lo mismo que decidir por la persona. Siempre que sea posible, tu familiar debe saber qué información está dando, para qué y a quién, y eso aplica también entre familiares o personas cercanas, no se deben compartir datos médicos, financieros o contraseñas de otras personas sin necesidad.



Qué hacer

Si ya se compartió información personal, no entres en pánico. Cambia contraseñas, comunícate con quien corresponda, revisa o bloquea lo conducente y conserva mensajes o comprobantes del incidente como evidencia.



6.3 Grupos de atención prioritaria

Esto incluye, entre otras situaciones, a personas con discapacidad, que no saben leer o escribir, que cuentan con alguna dificultad para usar herramientas digitales, que se encuentran en alguna situación económica difícil, en una emergencia, que hablan una lengua indígena sin que la traducción del trámite esté disponible en ella, que se encuentre en situación de calle, sea migrante o bien, se encuentre privada de la libertad.



Idea clave

Vulnerabilidad no significa incapacidad. Una persona puede necesitar apoyo para ejercer un derecho sin perder su capacidad de decisión sobre su propia información. La diferencia importa, no es “hay que decidir por esta persona”, es “hay que darle los apoyos para que pueda decidir”.



Tabla 6.1 Qué debe procurarse según la situación

Situación	¿Qué debe procurarse?
Persona con discapacidad	Que pueda realizar el trámite con los apoyos necesarios.
No sabe leer o escribir	Que reciba la información de forma comprensible y accesible.
Dificultad para usar internet	Que tenga alternativas o apoyo para el trámite.
Necesita ayuda de otra persona	Que sepa qué datos está dando, para que un intermediario no se apropie de sus datos.
Situación de emergencia	Que solo se le pidan los datos necesarios para atenderla.
Grupos indígenas	Que tenga alternativas en su lengua.



Qué hacer

Si necesitas apoyo, pregunta qué dato te piden, para qué lo necesitan, quién tendrá acceso, si es realmente necesario entregarlo y si necesitas ayuda para el trámite, pídelo, procurando conservar el control sobre tus decisiones e información. Si no entiendes, solicita que te expliquen en un lenguaje claro el aviso de privacidad.



Capítulo 7. Tecnologías emergentes y protección de datos personales



Lo esencial

La inteligencia artificial, el perfilamiento y las tecnologías que analizan señales cerebrales tienen algo en común, usan tus datos para conocerte, predecir tu comportamiento o personalizar lo que ves. Ninguna de estas tecnologías vuelve tus datos “sin dueño”, ya que, las mismas obligaciones de protección siguen resultando aplicables.

7.1 ¿Cómo utiliza la inteligencia artificial tus datos personales?

No toda inteligencia artificial usa datos personales, pero muchas herramientas sí reciben fotografías, grabaciones de voz, textos, ubicación o documentos que tú les proporcionas. Antes de usar esta herramienta, conviene hacerte una pregunta sencilla, ¿qué información les estoy dando?



Idea clave

Incluso una tarea simple como “edita esta fotografía” implica que la herramienta recibe la imagen original. La pregunta que importa no es solo qué le compartes, sino qué ocurre con esa información después, cuánto tiempo se conserva, con qué finalidad y quién más puede acceder a ella.



Ejemplo

Si durante varios días buscas información sobre bicicletas y luego empiezas a ver anuncios y videos relacionados, no es casualidad, es resultado de que una plataforma registró esa actividad y la usó para personalizar el contenido que te muestra.



Antes de compartir información con una herramienta de inteligencia artificial, pregúntate:

- ¿Qué datos me pide y realmente los necesita para la tarea?
- ¿Puedo obtener el mismo resultado al quitar nombres, domicilios o datos de otras personas del documento?
- Si el documento o fotografía contiene información de alguien más, ¿tengo permitido compartirla?
- Si se usa para apoyar una decisión sobre una persona, ¿sé quién toma la decisión final y qué pasa si la información es incorrecta?



Idea clave

La inteligencia artificial no convierte tus datos personales en información “sin dueño”. Si proporcionas información personal, siguen existiendo las mismas obligaciones legales sobre su tratamiento. En el caso de México, conforme a la LGPDPPSO y, en Nuevo León, a la LPDPPSONL.



7.2 ¿Qué es el perfilamiento y por qué influye en lo que ves en internet?

El perfilamiento consiste en usar información sobre ti para identificar intereses, hábitos o preferencias y construir un perfil; este luego se usa para personalizar un servicio, hacer recomendaciones o mostrarte determinado contenido.

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 la atención



Idea clave

Una sola actividad dice poco, pero muchas actividades juntas pueden revelar un patrón; por ejemplo, que una persona está interesada en viajar, aunque nunca lo haya dicho directamente. Por eso lo que ves en internet no siempre representa “todo lo que existe”. La plataforma se limita al contenido que pondrá a tu disposición según tus actividades anteriores.



Ejemplo

Pedro buscó información sobre cámaras fotográficas durante varios días y después empezó a recibir recomendaciones de cámaras, cursos y accesorios. No es que su teléfono lo escuche, simplemente es que la plataforma identificó un interés de Pedro a partir de sus búsquedas y navegación.



Qué hacer

No siempre puedes evitar el perfilamiento por completo, pero sí reducirlo. Procura revisar tus opciones de privacidad, limitar permisos innecesarios, evitar compartir datos que no hacen falta, consultar distintas fuentes de información y, antes de aceptar una solicitud de datos, pregúntate si de verdad es necesaria.

7.3 Neurodatos: cuando la tecnología puede conocer lo que piensas



Existen tecnologías —en materia de salud, investigación científica, entre otras— capaces de registrar señales relacionadas con la actividad cerebral. La información que obtienen se llama neurodatos.



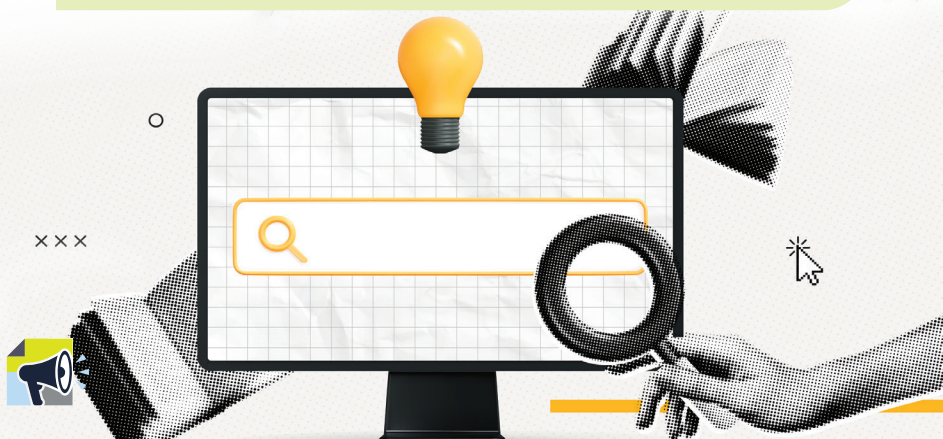


Idea clave

Esto no significa que una máquina pueda “leer tus pensamientos” como si fueran palabras escritas. Pero sí significa que, bajo ciertas condiciones, es posible registrar señales cerebrales y analizarlas para identificar patrones relacionados con determinadas respuestas o estados y esa información merece un nivel de protección particularmente alto, porque el cerebro forma parte de la esfera más íntima de una persona.

Ejemplo

Una tecnología que permite mover un cursor mediante señales cerebrales necesita registrar esas señales para funcionar. El problema aparece si esos mismos datos se usaran después para una finalidad distinta, sin que la persona lo supiera. Por esa razón la finalidad para la que se obtiene un dato siempre importa, incluso cuando la tecnología es muy nueva.





Para profundizar

Si alguna vez usas una tecnología que registra actividad cerebral, es razonable preguntar qué información obtiene, para qué la necesita, quién tendrá acceso, cuánto tiempo la conservará y cómo está protegida. Las mismas preguntas de siempre, aplicadas a un tipo de dato todavía en desarrollo. La legislación en materia de protección de datos personales en Nuevo León exige que estas finalidades sean concretas, lícitas, explícitas y legítimas.

Si deseas conocer más, te invitamos a consultar nuestra versión extendida *“Protección de datos personales. Herramientas para conocer y proteger tu información”*.



Capítulo 8.

Tus derechos sobre tus datos personales (ARCOP)



Lo esencial

Tienes cinco derechos sobre tus datos personales, acceder a ellos para conocerlos, corregirlos, cancelarlos, oponerte a su uso y, en ciertos casos, portarlos o trasladarlos de un sistema a otro; es decir de un sujeto obligado a otro sujeto obligado o de particular a particular, cumpliendo los requisitos que establece la ley. No son favores que una institución o un particular concede, se tratan de derechos que puedes ejercer.

Nota

En este libro usamos “ARCOP” para agrupar cinco derechos (Acceso, Rectificación, Cancelación, Oposición y Portabilidad). La legislación en materia de protección de datos personales identifica como “ARCO” a los primeros cuatro y regula la “Portabilidad” de forma específica.



8.1 Los cinco derechos ARCOP

Tabla 8.1 Los cinco derechos ARCOP

Letra	Derecho	En pocas palabras	Pregunta que respondes
A	Acceso	Te permite conocer y consultar datos personales que una institución o un particular tiene sobre ti y saber cómo los utiliza.	¿Qué datos personales tienen sobre mí?
R	Rectificación	Permite solicitar que tus datos sean corregidos o actualizados cuando sean inexactos, incompletos o se encuentren desactualizados.	¿Puedo solicitar que corrijan o actualicen mis datos personales?
C	Cancelación	Te permite solicitar que tus datos dejen de ser tratados y sean eliminados cuando sea posible.	¿Puedo pedir que se eliminen mis datos personales?
O	Oposición	Te permite solicitar que tus datos sean utilizados para determinados fines, cuando exista una causa legítima.	¿Puedo pedir que dejen de utilizar mis datos personales para ciertos fines?
P	Portabilidad	Te permite que puedas obtener tus datos personales y transmitirlos de un responsable a otro, o recibirlos en un formato que permita utilizarlos posteriormente.	¿Puedo obtener o trasladar mis datos personales para utilizarlos con otro responsable?





Idea clave

Es importante mencionar que el derecho de cancelación y portabilidad no siempre procede, ya que está sujeta a los supuestos y requisitos establecidos en la normativa aplicable.

8.2 Distinciones que conviene tener claras

Estos cinco derechos suenan parecidos, pero cada uno responde a algo distinto.

Acceso a datos personales $\neq$ acceso a la información pública

Diferenciarlos es muy sencillo, toda vez que, para ejercer el derecho a la información pública no necesitas



identificarte y para ejercerlo, basta con ingresar a la Plataforma Nacional de Transparencia y preguntar sobre asuntos como “quiero saber qué hace una institución con recursos públicos”; entre otros temas que sean de tu interés. Por otra parte, el derecho a la protección de los datos personales es personalísimo; solo tú puedes ejercerlo. Por ello, necesitas identificarte y, en caso de contar con representante, deberás acompañar carta poder simple firmada por dos testigos con identificación tuya y de la persona a quien le estás otorgando dicho poder. Este derecho permite saber qué información tiene una institución o un particular sobre ti.



Rectificar datos personales ≠ cancelar datos personales

El ejercicio del derecho de rectificación corrige un dato, no lo elimina. Por ejemplo, dato incorrecto “José Martínez”, dato correcto “José Martínez López”. Para eliminar, existe el derecho a la cancelación de datos personales.

Cancelar datos personales ≠ oponerse

El ejercicio del derecho a la cancelación de datos personales busca que los mismos dejen de ser tratados y cuando legalmente proceda, sean suprimidos porque ya no son necesarios para la finalidad concedida por el titular o no existe una razón legal para conservarlos. Por su parte, el ejercicio del derecho a la oposición de datos personales, busca que estos dejen de ser utilizados para determinado tratamiento o finalidad, cuando legalmente proceda, aunque los datos pueden quedar registrados.

Portabilidad de datos personales ≠ acceso a datos personales

El ejercicio del derecho de acceso a datos personales responde a “quiero saber qué tienen de mí”. Mientras que la portabilidad responde a “quiero obtener mis datos de forma que pueda usarlos o transmitirlos”, cuando la ley lo permita. Por ejemplo, si usaste una plataforma digital durante años y quieres obtener o trasladar tus datos en un formato utilizable, siempre y cuando esto sea posible.



Importante

No siempre se pueden cancelar o eliminar todos los datos personales. Que exista el derecho a la cancelación de estos, no significa que puedas eliminar cualquier registro con solo pedirlo. Una institución puede tener obligación legal de conservar cierta información por un tiempo determinado (razones fiscales, administrativas, judiciales, etc.). El derecho existe, pero convive con otras obligaciones legales.



Para profundizar

Si deseas conocer más, te invitamos a consultar nuestra versión extendida *“Protección de datos personales. Herramientas para conocer y proteger tu información”*, la cual desarrolla cada uno de estos derechos por separado, con ejemplos adicionales y el fundamento legal de cada caso, que podrás encontrar en Capítulo 8. *“Tus derechos sobre tus datos personales”*.

8.3 ¿Cuándo pueden limitarse estos derechos?

Los derechos ARCOP no son absolutos. En algunos casos previstos por la ley, una institución puede limitar o negar su ejercicio; por ejemplo, cuando sea necesario cumplir con una obligación legal, proteger los derechos de otras personas o atender razones de interés público previstas legalmente.



Tabla 8.2 Ejemplos de posibles límites

Situación	¿Por qué podría limitarse?
Pides cancelar información que debe conservarse por ley.	La institución no puede eliminar o suprimir la información mientras tenga la obligación legal de conservarla.
Pides acceso a información que también contiene datos de otra persona.	Corresponde a la institución pública y privada proteger los datos personales y derechos de terceros y en todo caso, elaborar una versión pública de la información solicitada.
Pides información de una investigación o procedimiento en curso.	No se te podría entregar, ya que se considera información reservada y su entrega podría obstaculizar o afectar el desarrollo de la investigación o procedimiento en curso.
Te opones a un tratamiento que la institución está obligada a realizar.	Puede existir una obligación legal que lo impida y eso limitaría a que ejerzas el derecho de oposición.

Capítulo 9.

¿Cómo ejercer tus derechos ARCOP paso a paso?



Lo esencial

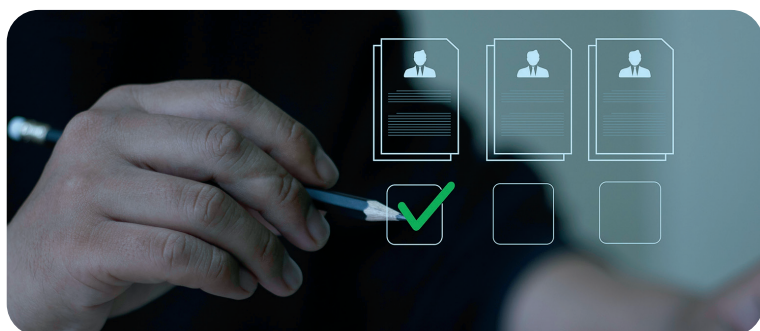
Ejercer un derecho ARCOP no requiere ser abogado. Son 5 pasos, con plazos legales concretos que debes conocer para saber si tu solicitud avanza en tiempo.



9.1 Ruta para ejercer tus derechos ARCOP

PASO 1	PASO 2	PASO 3	PASO 4	PASO 5
Identifica quién tiene tus datos	Presenta tu solicitud	Espera la respuesta (dentro del plazo legal)	Revisa la respuesta	Si no te responden o no estás de acuerdo → Capítulo 10

Paso 1: Identifica quién tiene tus datos



Piensa a quién y cuándo le has entregado tu información personal al realizar un trámite, una consulta médica, una inscripción escolar, etc. No necesitas saber el nombre técnico de la base de datos personales, basta con identificar la institución pública o privada. Si no estás seguro, identifica el aviso de privacidad del trámite o documento que conserves; si tus datos están en varias instituciones, la solicitud debe dirigirse a cada una por separado.



Paso 2: Presenta tu solicitud de derechos ARCOP

No necesitas utilizar un lenguaje jurídico. Una solicitud puede ser tan simple como “solicito ejercer mi derecho de acceso respecto de los datos personales (especificar a qué datos personales te refieres) que esa institución tiene registrados a mi nombre o de tu representado”.

Antes de enviarla, revisa lo siguiente:

- 1) Identificaste correctamente a la institución pública o privada.
- 2) Explicaste qué datos buscas.
- 3) Señalaste qué derecho quieres ejercer.
- 4) Proporcionaste los elementos necesarios que permitan tu identificación.
- 5) Recuerda guardar siempre tu comprobante.

Requisitos para ejercer tus derechos ARCOP

- El nombre del titular y su domicilio o cualquier otro medio para recibir notificaciones.
- Los documentos que acrediten la identidad del titular y, en su caso, la personalidad e identidad de su representante.
- De ser posible, el área responsable que trata los datos personales y ante el cual se presenta la solicitud.
- La descripción clara y precisa de los datos personales respecto de los que se busca ejercer alguno de los derechos ARCO, salvo que se trate del derecho de acceso.



- La descripción del derecho ARCO que se pretende ejercer, o bien, lo que solicita el titular.
- Cualquier otro elemento o documento que facilite la localización de los datos personales, en su caso.



Qué hacer

Usa esta fórmula sencilla, y describe lo siguiente:

quién soy + qué necesito + sobre qué datos.

Ejemplo para rectificación:

“Solicito la rectificación del domicilio registrado en mis datos, ya que actualmente aparece como ____ y el domicilio correcto es ____.”

Crea una pequeña carpeta (física o digital) con tu solicitud, el comprobante de recepción, cualquier comunicación que recibas y la respuesta final. Te será útil si necesitas defender tu solicitud de derechos ARCOP más adelante.



Para profundizar

La versión extendida *“Protección de datos personales. Herramientas para conocer y proteger tu información”* desarrolla cada uno de estos contextos por separado, con ejemplos adicionales, que encontrarás en el Capítulo 9. *“Cómo ejercer tus derechos paso a paso”*.



Paso 3: Espera la respuesta, dentro del plazo legal

Tabla 9.1 Plazos que debes conocer

Momento	Plazo general
Respuesta a tu solicitud	20 días hábiles
Cumplimiento de la respuesta (cuando procede)	15 días hábiles después de la respuesta
Ampliación del plazo	Son 10 días adicionales, cuando exista causa justificada



Idea clave

Para el cómputo de los plazos se toman en cuenta días hábiles, no naturales; es decir, no cuentan fines de semana ni días inhábiles. Es importante tomar en cuenta que todas las solicitudes deberán ser analizadas conforme al marco legal en materia de protección de datos personales; por tanto, la respuesta en algunos casos procederá y en otros no, dependiendo del caso específico. Revisa siempre si de verdad respondieron lo que pediste y si te explicaron por qué.



Paso 4: Revisa la respuesta enviada por la institución pública o privada sobre tu solicitud.

Paso 5: Si no te respondieron o no estás de acuerdo con la respuesta dada, te lo explicaremos a continuación, en el capítulo 10.

Capítulo 10.

¿Qué hacer si tus derechos ARCOP no son respetados por sujetos obligados en materia de protección de datos personales de Nuevo León?



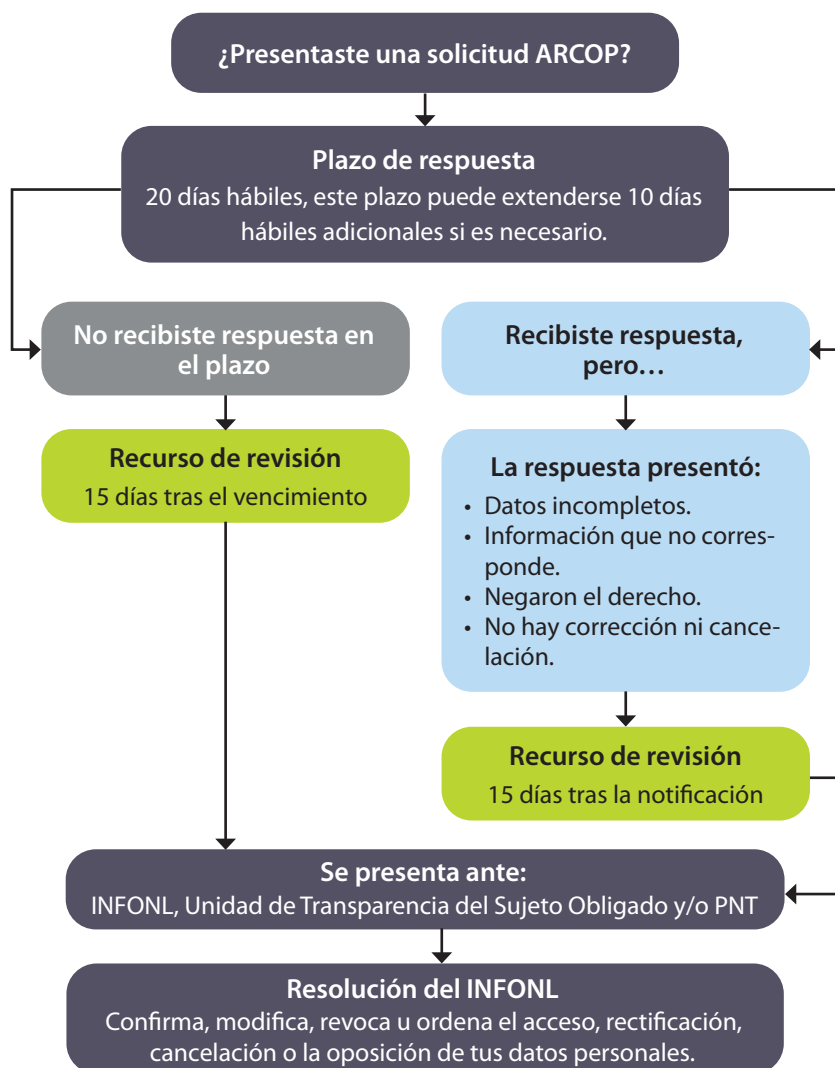
Lo esencial

Presentar una solicitud para ejercer tus derechos ARCOP no es el final del camino. Si la institución pública no responde dentro del plazo establecido, responde de manera incompleta o no estás de acuerdo con su respuesta, puedes presentar un recurso de revisión en materia de protección de datos personales.

En Nuevo León, cuando se trata de sujetos obligados estatales o municipales, como los poderes Ejecutivo, Legislativo y Judicial; los municipios; los organismos autónomos; los partidos políticos; los fideicomisos y fondos públicos, entre otros previstos por la legislación, el INFONL es la autoridad garante competente para conocer y resolver estos procedimientos, en el ámbito de sus atribuciones.



10.1 ¿Qué hago si un sujeto obligado en materia de protección de datos personales de Nuevo León no me responde o no estoy de acuerdo?





Idea clave

Interponer un recurso de revisión permite que una autoridad imparcial, autónoma y especializada en materia de protección de datos personales, como el INFONL, analice tu solicitud y la respuesta que te fue brindada para resolver tu caso, conforme a derecho, privilegiando en todo momento los principios y deberes que rigen el derecho a la protección de tus datos personales.

10.2 ¿Qué necesitas para presentar el recurso de revisión en materia de protección de datos personales?



Una vez que identifiques el motivo de tu inconformidad, el recurso de revisión debe contener determinados datos que permitan al instituto conocer qué sucedió, qué respuesta o actuación estás impugnando y qué solicitas que se revise.



De acuerdo con el artículo 119 de la LPDPPSONL, los requisitos exigibles en el escrito de interposición del recurso de revisión serán los siguientes:

- El área responsable ante quien se presentó la solicitud para el ejercicio de los derechos ARCO;
- El nombre completo del titular que recurre o su representante y, en su caso, del tercero interesado, así como el domicilio o medio que señale para recibir notificaciones;
- La fecha en que fue notificada la respuesta al titular, o bien, en caso de falta de respuesta la fecha de la presentación de la solicitud para el ejercicio de los derechos arco;
- El acto que se recurre y los puntos petitorios, así como las razones o motivos de inconformidad;
- En su caso, copia de la respuesta que se impugna y de la notificación correspondiente; y
- Los documentos que acrediten la identidad del titular y, en su caso, la personalidad e identidad de su representante.

También puedes acompañar al recurso las pruebas y demás elementos que consideres pertinentes para que el instituto valore tu inconformidad.





Para profundizar

La versión extendida *“Protección de datos personales. Herramientas para conocer y proteger tu información”*, desarrolla cada uno de estos temas por separado, con ejemplos adicionales y el fundamento legal específico para cada caso, que podrás encontrar en Capítulo 10. *“Qué hacer si tus derechos no son respetados”*.

10.3 ¿Cómo redacto un recurso de revisión en materia de protección de datos personales?

Para la redacción adecuada de la solicitud de un recurso de revisión, te recomendamos explicar los hechos de forma simple, no necesitas lenguaje jurídico. Puedes usar 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.



Formato para presentar el recurso de revisión

PRESENTE. –

LOS PUNTOS MARCADOS CON ASTERISCO (*) SON OBLIGATORIOS				
Esta sección deberá ser llenada por la Unidad de Transparencia del Sujeto obligado				
Fecha y hora de la presentación	Día	Mes	Año	Hora
1.- Área responsable ante quien se presentó la solicitud de derechos ARCO. * <i>"Art. 119, Fracción I LDPDDPPSONL."</i>				
2.- Nombre completo del titular de los datos personales que recurre. * <i>"Art. 119, Fracción II LDPDDPPSONL."</i>				
Nombre (s)		Apellido paterno		Apellido materno
2.1.- En su caso, el nombre completo del representante:				
Nombre (s)		Apellido paterno		Apellido materno
Nota: En el supuesto de que la interposición del presente recurso sea mediante un representante deberá anexar el poder simple o notarial con la firma de dos testigos.				
3.- Indique si los datos personales son de una persona: <i>En el supuesto de que los datos personales correspondan a una persona diferente al titular, enlistadas en las opciones que a continuación se mencionan; a título orientativo, se recomienda ver el apartado relativo a "Información general" (disponible al final del presente instrumento), para conocer los requisitos aplicables a cada caso.</i>				
☐ Titular (persona física a quien pertenecen y refieren los datos personales)		☐ Menor de edad (niña, niño, adolescente)		
☐ Persona en estado de interdicción		☐ Persona fallecida		
4.- Medio para oír y recibir notificaciones. * <i>"Art. 119 Fracción II LDPDDPPSONL."</i>				
☐ Correo electrónico		<i>En el supuesto de haber seleccionado este medio, favor de ingresar su correo electrónico.</i>		
☐ Personalmente en el recinto oficial del INFONL (Avenida Constitución Pte. 1765-1 Edificio Maldonado, Zona Centro Monterrey, Nuevo León, México, C.P. 64000)				
☐ Plataforma Nacional de Transparencia				
☐ Domicilio en el Estado de Nuevo León, en caso de seleccionar domicilio, favor de precisar:		<i>En el caso de haber seleccionado este medio, ingresar: Calle, Número exterior, Número interior, Colonia, Municipio, Estado y Código Postal.</i>		
☐ Número telefónico de contacto (opcional)		<i>Se hace de su conocimiento que "no es obligatorio", sin embargo, en el supuesto de haber seleccionado este medio adicional de contacto, Usted podrá ingresar el número fijo o bien celular.</i>		



5.- En el supuesto de existir un tercero interesado (persona distinta al titular que pudiera tener un interés jurídico o legítimo respecto al presente recurso de revisión) señale los datos que a continuación se refieren.

Ahora bien, si no existiera, se recomienda dejar este apartado sin llenar, (en blanco).

"Art. 119 Fracción II LDPDDPPSONL."

Nombre o denominación social:

Domicilio:

Calle

No. exterior e interior

Colonia

Municipio

Entidad Federativa

C.P.

(Nota: En el supuesto de que la interposición del presente recurso sea mediante un representante, deberá anexar el poder simple o notarial con la firma de dos testigos).

6.- Fecha en la que se le notificó la respuesta al ejercicio de sus derechos ARCO, día/mes/año, en caso de no haber recibido respuesta, favor de especificar la fecha en la que presentó la solicitud de derechos ARCO. *

Art. 119 Fracción III LDPDDPPSONL.

a). - Fecha en la que fue presentada la solicitud de ejercicio de derechos ARCO. *

•

Día

•

Mes

•

Año

b). - Fecha en la que fue notificada la respuesta al titular. *

•

Día

•

Mes

•

Año

7.- Acto recurrido (Anexar copia de los documentos) *

"Art. 119 Fracción IV LDPDDPPSONL."

Si requiere más espacio marque la siguiente casilla ☐ y especifique número de hojas.

Anexo 0 hojas.

8.- Razones o motivos de la inconformidad (Descripción de los hechos en que se funda el recurso) *

"Art. 119 Fracción IV LDPDDPPSONL."



Si requiere más espacio marque la siguiente casilla ☐ y especifique número de hojas.

Anexo 0 ☐ hojas.

9.- Puntos petitorios. * (Describir lo que solicita mediante este recurso de revisión)
"Art. 119 Fracción IV LDPDDPPSONL."

Si requiere más espacio marque la siguiente casilla ☐ y especifique número de hojas.

Anexo 0 ☐ hojas.

10.- Documentos que se acompañan en el presente recurso de revisión en materia de protección de datos personales. *

"Art. 119, fracción V de la LDPDDPPSONL."

- | | |
|--|--|
| ☐ Copia de la Solicitud de derechos ARCO. * | ☐ Copia de la respuesta que se impugna en el supuesto de que la hubiera emitido el responsable. |
| ☐ Acuse de recibo. * | ☐ Copia de la notificación de la respuesta, en caso de que se haya emitido. * |
| ☐ Documentos anexos (si es el caso, favor de especificar que documentos anexa).
a)
b) | |

11.- Documentos que acrediten la identidad del titular y, en su caso, la personalidad e identidad de su representante.

"Art. 119 Fracción VII LDPDDPPSONL."

- | | |
|---|---|
| ☐ Identificación oficial del titular o representante. | ☐ Carta Poder Simple firmada por dos testigos. |
| ☐ Acto o resolución emitida por el sujeto obligado. | ☐ Copias de traslado (en su caso). |
| ☐ Otras pruebas que consideren procedentes. (Detallar otras pruebas y elementos que se consideren procedentes o necesarias hacer del conocimiento al Instituto).
a)
b) | |



Por lo anteriormente expuesto y fundado, atentamente solicito a ese H. Instituto:

PRIMERO: Se admita a trámite el presente recurso de revisión y se notifique al sujeto obligado ante quien se ejercieron los derechos ARCO.

SEGUNDO: Se cite al Sujeto Obligado a las audiencias conciliatorias a que hace referencia la Ley de Protección de Datos Personales en Posesión de los Sujetos Obligados del Estado de Nuevo León.

TERCERO: Suplir las deficiencias del recurso de revisión, atento a lo dispuesto en los artículos 109 de la Ley de Protección de Datos Personales en Posesión de los Sujetos Obligados del Estado de Nuevo León.

PROTESTO LO NECESARIO EN DERECHO

Monterrey, Nuevo León a ____/____/____

ATENTAMENTE,

Nombre (s)

Apellido paterno

Apellido materno

El formato de recurso de revisión en materia de protección de datos personales del INFONL, lo puedes descargar en el siguiente enlace:



<https://tinyurl.com/3m4whbjv>



10.4 El Instituto Estatal de Transparencia, Acceso a la Información y Protección de Datos Personales (INFONL) protege tus datos personales

El INFONL es un organismo autónomo que garantiza la debida protección de tu información personal, que se encuentra bajo tratamiento de los diversos sujetos obligados en materia de protección de datos personales en Nuevo León. Esto significa que vigila que tu información personal sea usada de manera adecuada y conforme a la ley. Por otra parte, esta institución también se encarga de resolver los recursos de revisión en materia de datos personales cuando exista una inconformidad relacionada con el ejercicio de los derechos ARCOP, así como de sustanciar los procedimientos de verificación y denuncias que derivan de un presunto uso indebido de información personal conforme a lo dispuesto en la ley.

El INFONL no sustituye a la institución que tiene tus datos, sino que supervisa que esta cumpla con sus deberes y obligaciones para protegerlos de una manera adecuada y segura.

En pocas palabras, si una institución pública de Nuevo León tiene tus datos personales, puedes acudir ante el INFONL para recibir orientación y, cuando corresponda, solicitar que revise tu caso particular.



Capítulo 11.

Herramientas para protegerte



Lo esencial

En esta sección encontrarás un modelo para ejercer tus derechos ARCOP y un modelo para presentar una denuncia ante los sujetos obligados del Estado de Nuevo León, así como un directorio para identificar a qué autoridad acudir según tu caso y una lista de verificación antes de compartir tus datos personales.



11.1 Modelo para ejercer tus derechos ARCOP

Si deseas ejercer tus derechos de Acceso, Rectificación, Cancelación, Oposición o Portabilidad, puedes utilizar el siguiente modelo como guía para elaborar tu solicitud.

Formato Único Solicitud de Acceso, Rectificación, Cancelación, Oposición y/o Portabilidad de Datos Personales

*Los puntos marcados con asterisco al final son obligatorios.

Este espacio debe ser llenado exclusivamente por la Unidad de Transparencia:			
Folio número:		Fecha y hora de recepción ____/____/____ : ____ Hrs Día Mes Año	
1. Datos del Responsable (Sujeto Obligado) del tratamiento de los datos personales al que solicita su Derecho de Acceso, Rectificación, Cancelación, Oposición, y/o Portabilidad.			
2. Datos del Titular del Dato Personal o de su Representante			
Solicitante _____			
(Titular del dato)	Apellido Paterno	Apellido Materno	Nombre(s)
Datos de identificación oficial _____ (del que acompaña copia), mayor de edad, con domicilio en la calle _____ Número ____ Colonia _____ Municipio _____ Código Postal _____.			
Representante Legal _____			
(En su caso)	Apellido Paterno	Apellido Materno	Nombre(s)
Datos de identificación oficial _____ (del que acompaña copia), mayor de edad, con domicilio ubicado en: Calle _____ Número ____ Colonia _____ Municipio _____ Código Postal _____.			
3. En su caso, indique si los datos son de una persona:			
☐ Menor de edad ☐ En estado de interdicción o incapacidad ☐ Fallecido (a)			
Nota: Si seleccionó algunas de las opciones anteriores, véase “Información general”, para los requisitos aplicables a cada caso			
4. Indique el derecho que desea ejercer (puede ser uno o más)			
☐ Acceso ☐ Rectificación ☐ Cancelación ☐ Oposición ☐ Portabilidad			



5. Describa con claridad su solicitud y los datos personales respecto de los cuales requiere el ejercicio del derecho ARCOP (en el caso de una solicitud de acceso, no será indispensable especificar los datos personales. Para las solicitudes de rectificación, se sugiere incluir los documentos que avalen la modificación solicitada. Para el ejercicio de cancelación, deberá señalar las causas que lo motivan a solicitar el borrado o eliminación de los datos personales. Para el ejercicio del derecho de oposición, deberá señalar la situación que lo lleva a solicitar que concluya el tratamiento (uso) de los datos, así como el daño que le causaría que se continuara con el mismo, o bien, deberá indicar las finalidades específicas respecto de las cuales solicita que se concluya el tratamiento):*

En caso de que cuente con información que facilite la búsqueda y eventual localización de los datos personales, como la unidad administrativa que considera que trata sus datos y documentos que sean de utilidad, por favor proporciónela (opcional):

6. Lugar o medio para recibir la información solicitada y las notificaciones correspondientes

- ☐ Correo electrónico
☐ Domicilio

Calle

No. Exterior

No. Interior

Colonia

Municipio

Código Postal

- ☐ Acudir a la Unidad de Transparencia
☐ Sistema Electrónico habilitado para ello

En caso de que no se indique algún medio para recibir notificaciones, éstas se realizarán por estrados de la Unidad de Transparencia.

Las notificaciones se harán a través del sistema electrónico establecido por el Sujeto Obligado o correo electrónico proporcionado por el solicitante.

*Correo electrónico para recibir notificaciones.

Si no se utiliza el sistema electrónico o no se proporciona un correo electrónico, las notificaciones serán personales, practicándose en el domicilio que el interesado señale. Este domicilio deberá estar dentro del municipio de residencia del sujeto obligado al que se le requiere la solicitud de Acceso, Rectificación, Cancelación, Oposición y/o Portabilidad de los datos, de lo contrario se harán por tabla de avisos.

Calle

No. Exterior / No. Interior

Colonia o Fraccionamiento

Código Postal

Municipio

7. Opcionalmente, la modalidad en la que se prefiere se otorgue el acceso a datos personales, indique cómo requiere el acceso o reproducción de los datos:



- ☐ Consulta directa (**sin costo**)
- ☐ Copias simples (**sin costo** las primeras 20 hojas)
- ☐ Disco compacto (**sin costo**, si éste es proporcionado por el solicitante)
- ☐ Copias certificadas (**sin costo** las primeras 20 hojas)
- ☐ Dispositivo de almacenamiento (**sin costo**, si éste es proporcionado por el solicitante)

8. Documentos Anexos

- a) Copia de la Identificación del Titular del Dato.
- b) Carta Poder Simple, firmada por dos testigos (en caso de ser por Representante)
- c) Copia de la identificación del Representante del Titular del Dato.
- d) Cualquier otro documento que facilite el numeral 3.

9. Medidas de accesibilidad opcional.

Lengua indígena (para facilitar la traducción, indique el nombre de la lengua y/o el lugar donde habla dicha lengua el solicitante):

Formato accesible y/o preferencia de accesibilidad:

- ☐ Equipos de cómputo con tecnología adaptada, escritura braille y lectores de texto
 - ☐ Lenguaje de señas o cualquier otro medio o modo de comunicación
 - ☐ Lugar de estacionamiento para persona con discapacidad
 - ☐ Asistencia de intérpretes oficiales de la lengua que señala Brindar las facilidades para el acceso de perros guías o animales de apoyo
 - ☐ Apoyo de lectura de documentos
 - ☐ Rampa para personas con discapacidad
 - ☐ Otras (indique cuáles):
-

Aviso de Privacidad Simplificado. La Comisión de Transparencia y Acceso a la Información del Estado de Nuevo León es el responsable del tratamiento de los datos personales que proporcione en este formato, los cuales serán tratados exclusivamente para dar atención a su solicitud de ejercicio de derechos ARCOP, y de ser el caso, para el Recurso de Revisión, así como con fines estadísticos. Para esto último, requerimos de su consentimiento, por lo que le solicitamos que indique a continuación si autoriza que sus datos personales sean utilizados con fines estadísticos, a fin de contar con información valiosa para mejorar nuestros servicios e implementar las medidas que resulten pertinentes para impulsar el ejercicio del derecho de protección de datos personales en nuestro estado. Es importante señalar que las estadísticas que se generen no vincularán la información general con datos que hagan identificables a los titulares:

- ☐ Consiento que mis datos personales se utilicen con fines estadísticos.
- ☐ No consiento que mis datos personales se utilicen con fines estadísticos.

En caso de no consentir el tratamiento, le solicitamos no llenar las secciones 10 y 11 de este formato.

Asimismo, le informamos que sus datos personales podrán ser transferidos, cuando sea necesario para atender requerimientos de información de una autoridad competente, que estén debidamente fundados y motivados.

Usted podrá consultar nuestro Aviso de Privacidad Integral en
<https://infonl.mx/proteccion-de-datos-personales/avisos-de-privacidad/>



Bajo protesta de decir verdad manifiesto que los datos asentados en el presente son ciertos, incluyendo los que acrediten la identidad del titular.

 Nombre y firma del Titular del Dato o de su Representante

10. Información para fines estadísticos (opcional)

Sexo: ☐ Masculino ☐ Femenino Nacionalidad _____

Ocupación (Seleccione por favor una opción):

- ☐ Ámbito Empresarial ☐ Ámbito Gubernamental ☐ Ámbito Académico ☐ Medios de Comunicación
☐ Organización no gubernamental Comerciante ☐ Empleado
☐ Otro (Especifique) _____

11. Escolaridad

☐ Sin estudios ☐ Primaria ☐ Secundaria ☐ Preparatoria ☐ Licenciatura ☐ Posgrado ☐ Doctorado ☐ Técnica

12. Instructivo

- o Llenar letra de molde legible o en electrónico.
- o El sujeto obligado le auxiliará en la elaboración de la presente solicitud.
- o En caso de requerir diversos Derechos ARCOP, deberá solicitar cada una en un formato independiente.
- o En caso de presentar esta solicitud mediante un representante, se acreditará dicha representación mediante una carta simple firmada ante dos testigos (carta poder simple). En caso de que los datos personales requeridos no fuesen localizados en los sistemas de datos personales del sujeto obligado, dicha circunstancia se comunicará al interesado vía resolución.
- o El sujeto obligado no estará obligado a dar trámite a solicitudes de Acceso, Rectificación, Cancelación, Oposición, y/o Portabilidad, ofensivas o cuando se haya ejercido los mencionados derechos referentes a datos sustancialmente idénticos como respuesta a una solicitud de la misma persona.
- o Mientras más clara y precisa sea su solicitud de Acceso, Rectificación, Cancelación, Oposición, y/o Portabilidad a datos personales será más rápida la localización.

13. Información General

- o Los formatos de solicitudes de Acceso, Rectificación, Cancelación, Oposición, y/o Portabilidad que proporcionen los sujetos obligados serán gratuitos.
- o Usted puede reproducir este formato en papel bond blanco.
- o Podrán solicitarse más documentos que los señalados en este formato, siempre y cuando sean necesarios para ejercer la solicitud de los derechos ARCOP.
- o Los plazos de contestación de la solicitud de derechos ARCOP, serán de 20 días hábiles.

Documentación que se debe presentar:

- o La identidad del titular de los datos personales y, en su caso, de su representante legal deberán ser acreditadas previo al ejercicio del derecho ARCOP que corresponda, a través de la presentación, en original para su cotejo y copia simple, de un documento de identificación oficial vigente, entre ellos: Credencial para Votar, Pasaporte, Cartilla Militar, Cédula Profesional, Licencia para Conducir y/o Documento Migratorio.
- o La identidad de los menores de edad se podrá acreditar mediante su acta de nacimiento, Clave Única de Registro de Población, credenciales expedidas por instituciones educativas o instituciones de seguridad social, pasaporte, o cualquier otro documento oficial utilizado para tal fin.
- o La identidad de personas en estado de interdicción o incapacidad declarada por ley se podrá acreditar mediante su acta de nacimiento, Clave Única de Registro de Población, pasaporte o cualquier otro documento o identificación oficial expedida para tal fin.
- o Además de lo anterior, en el caso del representante, se deberá presentar el documento en el que consten sus facultades de representación: instrumento público o carta poder simple firmada ante



dos testigos, anexando copia simple de las identificaciones oficiales de quienes intervengan en la suscripción del mismo o la declaración en comparecencia personal del titular.

- o Asimismo, previo al ejercicio del derecho ARCOP que corresponda, deberá presentar el original del acuse de presentación de su solicitud.
- o Para el ejercicio de derechos ARCOP de una persona menor de edad, en estado de interdicción o incapacidad, o fallecida, se deberá presentar la siguiente documentación, según sea el caso:
 - a) **Menores de edad**
 - o En el caso de que los padres tengan la patria potestad del menor y sean los que pretendan ejercer el derecho ARCOP, además de acreditar la identidad del menor deberán presentar los siguientes documentos:
 - o Acta de nacimiento del menor de edad;
 - o Documento de identificación oficial del padre o de la madre que pretenda ejercer el derecho;
 - o Carta en la que se manifieste, bajo protesta de decir verdad, que el padre o madre, según sea el caso, ejerce la patria potestad del menor, y que no se encuentra dentro de alguno de los supuestos legales de suspensión o limitación de la misma.
 - o **Si la patria potestad la ejerce una persona distinta a los padres, y ésta es quien pretenda ejercer el derecho ARCOP, además de acreditar la identidad del menor deberán presentar los siguientes documentos:**
 - o Acta de nacimiento del menor de edad;
 - o Documento legal que acredite la posesión de la patria potestad;
 - o Documento de identificación oficial de quien ejerce la patria potestad y presenta la solicitud.
 - o Carta en la que se manifieste, bajo protesta de decir verdad, que ejerce la patria potestad del menor, y que no se encuentra dentro de alguno de los supuestos legales de suspensión o limitación de la misma.
 - o **Cuando el derecho ARCOP lo pretenda ejercer el tutor del menor de edad, además de acreditar la identidad del menor deberán presentar los siguientes documentos:**
 - o Acta de nacimiento del menor de edad;
 - o Documento legal que acredite la tutela;
 - o Documento de identificación oficial del tutor;
 - o Carta en la que se manifieste, bajo protesta de decir verdad, que ejerce la tutela, y que no se encuentra dentro de alguno de los supuestos legales de suspensión o limitación de la misma.
 - b) **Personas en estado de interdicción o incapacidad:**
 - o Instrumento legal de designación del tutor;
 - o Documento de identificación oficial del tutor, y
 - o Carta en la que se manifieste, bajo protesta de decir verdad, que ejerce la tutela, y que no se encuentra dentro de alguno de los supuestos legales de suspensión o limitación de la misma.
 - c) **Personas fallecidas:**
 - o Acta de defunción;
 - o Documento(s) que acrediten el interés jurídico de quien pretende ejercer el derecho, y
 - o Documento de identificación oficial de quien solicita el ejercicio del derecho.

Para conocer más, consulta y descarga el formato oficial del INFONL:



<https://tinyurl.com/2dw69dcc>





Qué hacer

Antes de enviar cualquier solicitud, revisa si identificaste a la institución correcta, explicaste qué necesitas, señalaste el derecho que ejerces, diste elementos para localizar tus datos, acreditaste tu identidad si es necesario, y conservaste una copia con tu comprobante.

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 del 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).



La denuncia podrá presentarse a través de los formatos proporcionados, medios electrónicos, escrito libre o cualquier otro medio o tecnología que el Instituto establezca para dicho efecto.

Pasos para presentar tu denuncia

1. Elabora tu denuncia en el formato que se proporciona a continuación (de preferencia).
2. Imprime tu denuncia.
3. Fírmala de manera autógrafa, o bien puedes plasmar tus huellas dactilares.
4. Escanea tu denuncia.
5. Anexa tu denuncia firmada de manera autógrafa.
6. Anexa los documentos con la información que consideres pertinente.
7. Envía tu denuncia al correo denuncia.datospersonales@infonl.mx

A continuación te compartimos nuestro formato base para presentar denuncia en materia de protección de datos personales ante el Instituto Estatal de Transparencia, Acceso a la Información y Protección de Datos Personales (INFONL) en términos de la Ley de Protección de Datos Personales en Posesión de los Sujetos Obligados del Estado de Nuevo León.



Formato de denuncia en materia de protección de datos personales

PRESENTE. –

En cumplimiento a lo dispuesto por el artículo 136 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Nuevo León, se pone a su disposición el presente formato de denuncia.

Adicionalmente se le hace de su conocimiento que ésta plantilla deberá llenarse con letra legible.

Hoja 1/1.- En caso de requerir más hojas, especifique aquí el número total de hojas del presente escrito, sirviéndose firmar cada hoja adicional: _____

Los puntos marcados con asterisco (*) son obligatorios

Fecha y hora de la presentación

Día

Mes

Año

Hora

1.- Nombre del denunciante, o en su caso, de su representante: *

"Art. 136, Fracción I LDPDDPPSONL."

Nombre (s)

Apellido paterno

Apellido materno

2.- Medio para oír y recibir notificaciones: *

"Art. 136 Fracción II LDPDDPPSONL."

☐

Correo electrónico

En el supuesto de haber seleccionado este medio, favor de ingresar su correo electrónico

☐

Personalmente en el recinto oficial del INFONL (Avenida Constitución Pte. 1765-1 Edificio Maldonado, Zona Centro Monterrey, Nuevo León, México, C.P. 64000)

☐

Domicilio en el estado de Nuevo León:

En el caso de haber seleccionado este medio, ingresar: Calle, Número exterior, Número interior, Colonia, Municipio, Estado y Código Postal.

☐

Número telefónico de contacto (opcional)

Se hace de su conocimiento que "no es obligatorio", sin embargo, en el supuesto de haber seleccionado este medio adicional de contacto, Usted podrá ingresar el número fijo o bien celular.

3.- Relación de los hechos en que se basa la denuncia: *

"Art. 136 Fracción III LDPDDPPSONL."



Si requiere más espacio marque la siguiente casilla ☐ y especifique número de hojas
Anexo 0 hojas.

4.- Elementos con los que cuente para acreditar su dicho. (Anexar copia de los documentos)
"Art. 136 Fracción III LDPDDPPSONL."

- a) .
b) .

5.- El responsable denunciado y su domicilio, o en su caso, los datos para su identificación y/o ubicación. *
"Art. 136 Fracción IV LDPDDPPSONL."

Nombre del sujeto obligado: .

Domicilio: .

Ingresar: Calle, Número exterior, Numero interior, Colonia, Municipio, Estado y Código Postal.

En caso de no contar con los
datos anteriores, plasme aquí
los datos para su
identificación y/o ubicación:

6.- Firma del denunciante o en su caso, del representante. (Si no sabe firmar, sírvase estampar su huella digital) *
"Art. 136 Fracción V LDPDDPPSONL."

FIRMA DEL DENUNCIANTE

HUELLAS DIGITALES (de ser el caso)

7.- CARÁCTER DEL DENUNCIANTE.

☐ **Afectado principal:** Cuando las presuntas violaciones a la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Nuevo León y demás ordenamientos aplicables, recaen a su persona.

☐ **Tercero:** Cuando el particular no está directamente involucrado en el asunto respecto de la o las personas implicadas en el mismo, es decir, las violaciones a Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Nuevo León, recaen sobre otras personas.



Su denuncia puede ser presentada a través del correo electrónico denuncia.datospersonales@infonl.mx o físicamente en la unidad de correspondencia común del Instituto Estatal de Transparencia, Acceso a la Información y Protección de Datos Personales con domicilio ubicado en Av. Constitución, número 1465-1, colonia Centro, Municipio de Monterrey, Nuevo León, C.P.64000, en un horario de lunes a viernes de 9:00 a 17:00 horas.

IMPORTANTE: Bajo protesta de decir verdad, manifiesto que los datos asentados en el presente son ciertos, incluyendo los que acreditan la identidad del denunciante, conociendo las penas en que incurrir las personas que declaran falsamente ante una autoridad distinta a la judicial.

Aviso de privacidad simplificado

El Instituto Estatal de Transparencia, Acceso a la Información y Protección de Datos Personales (INFONL), es el responsable del tratamiento de los datos personales que nos proporcione.

Finalidades del tratamiento de datos personales;

Sus datos personales serán utilizados para las siguientes finalidades:

Recibir, registrar y tramitar denuncias en materia de protección de datos personales en posesión de sujetos obligados del sector público, de conformidad con Ley de Protección de Datos Personales en Posesión de los Sujetos Obligados del Estado de Nuevo León.

De manera adicional, los datos personales que nos proporcione podrán ser utilizados para contar con datos de control y estadísticos.

Mecanismos para el ejercicio de los derechos ARCO;

Usted podrá ejercer sus derechos ARCO directamente ante la Unidad de Transparencia de este Instituto, ubicada en Avenida Constitución 1465-1, colonia Centro, C.P. 64000, Monterrey, Nuevo León, o bien, a través de la Plataforma Nacional de Transparencia (<http://www.plataformadetransparencia.org.mx/>).

Si desea conocer el procedimiento para el ejercicio de estos derechos puede acudir a la Unidad de Transparencia o comunicarse al Tel: 10017800.

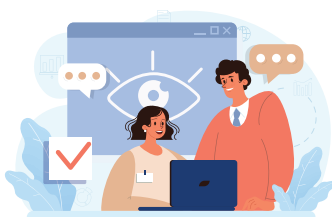
Sitio dónde consultar el aviso de privacidad integral;

Quien así lo requiera, podrá consultar el aviso de privacidad en su modalidad integral, de acuerdo con lo establecido en el artículo 30 de la Ley de Protección de Datos Personales en Posesión de los Sujetos Obligados del Estado de Nuevo León en la liga <https://infonl.mx/proteccion-de-datos-personales/avisos-de-privacidad/>

En este enlace podrás descargar el formato para presentar la denuncia en datos personales:



<https://tinyurl.com/4xhahcuf>



11.3 Directorio de autoridades competentes

Tabla 11.1 ¿A quién acudo?

Si tus datos están en manos de...	Acude a...
Una institución pública del Estado de Nuevo León	El Instituto Estatal de Transparencia, Acceso a la Información y Protección de Datos Personales (INFONL).
Una institución pública federal	La 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.
Una institución privada	La 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.



Herramienta adicional

Lleva un pequeño control de dónde has entregado tus datos (institución, qué datos, para qué, fecha aproximada). No requiere ningún trámite y te ayuda a identificar rápidamente a quién dirigir una futura solicitud.



Antes de confiar en un sitio web...

Verifica quién lo publica, que la dirección corresponda realmente a la institución, que la información esté actualizada y no proporciones datos personales en páginas a las que llegaste por enlaces desconocidos o mensajes inesperados.

11.4 Micrositios del INFONL

El INFONL cuenta con espacios especializados en su sitio institucional que ofrecen información y herramientas para que la ciudadanía conozca y ejerza sus derechos en materia de protección de datos personales. En ellos puedes consultar información sobre protección de datos personales, derechos de las personas y avisos de privacidad, así como recursos para saber qué hacer cuando necesitas ejercer algún derecho relacionado con tus datos.

Estos espacios pueden ser especialmente útiles para pasar de la información a la acción, lo que incluye conocer tus



derechos, identificar qué información debe proporcionarte una institución y saber dónde acudir cuando necesites ejercerlos.

Recomendación: Los sitios institucionales pueden cambiar de diseño, nombre o dirección de sus secciones. Si un enlace deja de funcionar, lo recomendable es ingresar directamente al sitio oficial del INFONL y utilizar su buscador o menú de navegación para localizar nuevamente la información. Además de facilitar la consulta, esto ayuda a reducir el riesgo de ingresar a páginas falsas que imitan a instituciones públicas.

Consulta el sitio oficial del INFONL:



<https://infonl.mx/proteccion-de-datos-personales/>

11.5 Lista de verificación antes de compartir tus datos personales

Antes de proporcionar tus datos personales, pregúntate:

- ¿Quién me está solicitando esta información?
- ¿Para qué la necesitan?
- ¿Realmente necesitan todos estos datos?



- ¿Qué tipo de datos son? (De identificación, laborales, patrimoniales, financieros, médicos, biométricos, etc.).
- ¿Dónde puedo consultar el aviso de privacidad?
- ¿Qué harán con mi información después?
- ¿La compartirán con alguien más?
- ¿Quién puede tener acceso a mi información?
- ¿Estoy usando un sitio o canal oficial confiable?
- ¿Estoy seguro de que es necesario compartir mis datos personales?

El mensaje más importante de esta publicación es que no necesitas memorizar leyes para proteger tus datos personales. Antes de compartirlos, basta con preguntarte: ¿quién los solicita?, ¿para qué los necesita?, y si realmente es necesario proporcionarlos. Esa pequeña pausa, en el fondo, hace toda la diferencia, ya que te permite reflexionar y decidir sobre el uso que se dará a tu información personal.

Recuerda: Tus datos personales son tuyos y tienes derecho a saber cómo, cuándo, para qué y por quién son utilizados. La protección de datos personales es un derecho que permite a cada persona mantener control sobre su información y decidir sobre su tratamiento.

En el INFONL, trabajamos para garantizar este derecho, promover una cultura de protección de datos personales y brindar a la ciudadanía las herramientas necesarias para



ejercer sus derechos. Infórmate, conoce tus derechos y participa activamente en la protección de tu información personal.



Para profundizar

Por último, te recordamos que la versión extendida de esta obra *“Protección de datos personales. Herramientas para conocer y proteger tu información”*, desarrolla cada uno de estos temas por separado, con ejemplos adicionales y el fundamento legal específico para cada caso, misma que podrás encontrar en el sitio oficial del INFONL.





Referencias

- 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>
- Congreso del Estado de Nuevo León. (2019). Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Nuevo León [LPDPPSONL]. 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. (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/
- Constitución Política de los Estados Unidos Mexicanos. (1917). Texto vigente. <https://www.diputados.gob.mx/LeyesBiblio/pdf/CPEUM.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://sidof.segob.gob.mx/notas/docFuente/5752569>
- 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. (s. f.). Sitio oficial del INFONL. <https://infonl.mx/>





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



Ediciones
DeLaurel®

ISBN 978-968-9780-06-9



9 789689 780069