MANUAL DE PROTECCIÓN DE DATOS PERSONALES PARA EL SECTOR PÚBLICO SALVADOREÑO

Textos de Lectura Fácil

Instituto de Acceso a la Información Pública

Instituto de acceso a la información pública de la República de El Salvador

Lic. Carlos Adolfo Ortega Umaña
Comisionado Presidente

Lic. Mauricio Antonio Vásquez López
Comisionado Propietario

Lic. Jaime Mauricio Campos Pérez
Comisionado Propietario

Lic. María Herminia Funes de Segovia
Comisionada Propietaria

Lic. Max Fernando Mirón Alfaro
Comisionado Propietario

Coordinación de la producción:
Unidad de Capacitaciones del IAIP

Coordinación:
Área de institucionalidad democrática de EUROsociAL
Fernando de la Cruz (Fundación CEDDET)

Revisión:
Iñaki Pariente de Prada (Director de la Agencia Vasca de Protección de Datos)
Ana Isabel Martín Ramos (Experta internacional de EUROsociAL)

Adaptación a Lectura Fácil:
Laia Vidal
Ana Crespo

Ilustraciones, diseño y maquetación:
Judit Canela

Edición: Junio 2015

La presente publicación ha sido elaborada con la asistencia de la Unión Europea. El contenido de la misma es responsabilidad exclusiva de los autores y en ningún caso se debe considerar que refleja la opinión de la Unión Europea.

ÍNDICE

Introducción.....4
¿Para qué sirve este Manual?.....5
La sociedad de la información 5

Datos personales
¿Qué es un dato personal?.....8
¿Dónde pueden aparecer mis datos?.....9

Protección de datos personales..... 10

La ley de acceso a la información pública
¿Qué regula esta Ley?..... 11
¿Qué dice esta Ley sobre la protección de datos personales?..... 11
¿En qué principios se basa?..... 11
El Instituto de Acceso a la Información Pública..... 15
¿Cómo se protegen los datos personales?.....16
Niveles de seguridad.....17
Bases de datos.....18
El registros de las bases de datos..... 19
Datos sensibles.....21
Datos para fines policiales.....22
¿Cuándo se pueden tratar los datos personales?.....22
¿Quién puede tratar los datos personales?.....23
¿Qué derechos tiene la ciudadanía sobre sus datos?..... 24
¿Cómo ejercer estos derechos?..... 25
¿Dónde dirigirse?..... 25
¿Cuándo se obtiene respuesta?..... 26
¿Cuánto cuesta?..... 26
¿Cómo apelar?..... 27
Infracciones y sanciones..... 29

Introducción

En muchas de las actuaciones que realizamos durante el día intercambiamos información personal: al pagar con un tarjeta de crédito, al aportar información por teléfono, al contratar un servicio, al comprar a través de internet, al realizar trámites en un organismo público o al realizar un ingreso hospitalario, entre otras muchas actividades cotidianas.

Desde que nacemos generamos una gran cantidad de datos: partida de nacimiento, escolarización, seguro de salud, contratos de trabajo…

Con la llegada de internet y las nuevas tecnologías el intercambio y almacenamiento de datos ha aumentado, y son más accesibles para todos. Es decir, nos pueden controlar más a través de nuestros datos. Eso puede generar injerencias ilegítimas en la vida privada de las personas.

Para proteger nuestros derechos y nuestra privacidad existen contenidos normativos que regulan el uso de los datos personales, entre ellas las previsiones sobre protección de datos contenidos en la Ley de Acceso a la Información Pública (en adelante, LAIP).

¿Para qué sirve este Manual?

El objetivo de este Manual es explicar qué son datos personales, la importancia de su adecuada protección, y cómo garantizar el derecho a la privacidad de las personas.

También servirá para dar a conocer qué establece la Ley de Acceso a la Información Pública sobre la protección de los datos personales.

La sociedad de la información

El interés por proteger el derecho a la intimidad y la privacidad frente a la creciente recogida y gestión de información personal surgió a finales de los años 70.

En aquel momento en que la tecnología no estaba tan avanzada, la preocupación se centraba en la capacidad de los Estados para utilizar esa información como arma de poder.

La legislación de la época se basaba en la regulación de los bancos de datos públicos y en la creación de organismos de control que mediaran entre el Estado y la ciudadanía.

Esa situación cambió radicalmente a partir de la década de los 90.
La llegada de Internet y todos los servicios que la nueva tecnología
incorporaba (navegación web, correo electrónico, etc.)
revolucionaron los modelos tradicionales de comunicación
y multiplicaron exponencialmente los intercambios de información.

Desde un punto de vista tanto público como privado,
los datos personales se convirtieron en una mercancía de gran valor
que las herramientas informáticas permitían recopilar
y procesar con el objetivo de utilizarlos para fines muy variados,
algunos de dudosa legalidad.

Es entonces cuando se planteó por primera vez la necesidad
de regular jurídicamente la protección de datos personales
para garantizar algunos derechos fundamentales que empezaban
a verse amenazados por la nueva sociedad de la información,
en especial el derecho a la intimidad y la privacidad.

Hoy en día, ya no somos capaces de concebir nuestra sociedad
sin la presencia de las nuevas tecnologías.
La circulación e intercambio de datos personales sigue creciendo
debido al sostenido desarrollo tecnológico, el uso masivo de Internet
y la consolidación de las redes sociales.
Y es la gestión de estos datos la que permite la elaboración
de perfiles y patrones de comportamiento que ponen en peligro
libertades y derechos fundamentales de la ciudadanía.

Sin lugar a dudas, esta situación se acentuará en el futuro
con la irrupción de nuevos dispositivos tecnológicos
en nuestra vida cotidiana.
El reto consiste, pues, en desarrollar una legislación
lo bastante amplia y exhaustiva como para proteger
los derechos de la ciudadanía en todos los ámbitos
en que éstos se ven amenazados
por el procesamiento de sus datos personales.

Datos personales

¿Qué es un dato personal?

Cualquier información concerniente a una persona
que permite identificarla o hacerla identificable
al cruzar diferentes datos aislados.

Existen datos que de forma fácil se reconocen como personales;
es el caso de la imagen o el nombre y apellidos.
Y existen otros que son más difíciles de identificar
como datos personales; es el caso de los datos de salud,
biométricos, genéticos, de empleo, bancarios, datos vinculados
a la personalidad como la orientación sexual, las creencias religiosas
o la ideología política y afiliación sindical,
u otros como el origen étnico, currículums,
datos de consumo y preferencias de compra, la voz o la firma.

A los efectos de la LAIP, esta norma entiende por datos personales
la nacionalidad, domicilio, patrimonio, dirección electrónica,
número telefónico u otros análogos, así como datos personales sensibles
como el credo, religión, origen étnico, filiación o ideologías políticas,
afiliación sindical, preferencias sexuales, salud física
y mental, situación moral y familiar y otras informaciones íntimas
de similar naturaleza o que puedan afectar el derecho al honor,
a la intimidad personal y familiar y a la propia imagen.

Los datos personales son muy importantes porque
nos identifican y nos describen.
Pero también porque pueden influir
en cómo nos pueden tratar o evaluar, gestionando,
cruzando o analizando la información personal
que ofrecemos por distintos medios.

Las leyes de protección de datos controlan el uso que se hace
de ellos para que nadie los pueda utilizar de forma indebida.
Las personas físicas tienen derecho a gestionar
su propia información y a controlar cómo pueden tratarla
otras personas o instituciones.
También tienen derecho a poder acceder a su propia información.

¿Dónde pueden aparecer nuestros datos?

Los datos pueden estar guardados en diferentes formatos:
pueden ser digitales, imagen, voz, documentos en papel
o distintos soportes como un CD, un DVD o una computadora.

Los entes públicos poseen gran cantidad
de datos personales de la ciudadanía.
Pero lo Ley protege estos datos, para que no se puedan usar
con finalidades distintas a aquélla para la que han sido recabados.

Protección de datos personales

Intimidad y privacidad son conceptos diferentes
aunque estén relacionados.

La protección de datos personales hace referencia a la privacidad,
entendida como toda la información que pertenece a una persona.

Por el contrario, el derecho a la intimidad se limita a proteger
los aspectos más reservados de la vida de la persona,
aspectos que se mantienen al margen
del conocimiento generalizado de los demás.

La Ley de Acceso a la Información Pública

¿Qué regula esta Ley?

La Ley de Acceso a la Información Pública (LAIP) se aprobó
por el Decreto Legislativo número 534 de fecha 3 de marzo de 2011,
publicado el 8 de abril de 2011.

Esta ley garantiza que la ciudadanía acceda a la información pública
y pueda conocer cómo actúan las instituciones del Estado.
También regula el acceso, la difusión y uso de los datos personales.

¿Qué dice esta Ley sobre la protección de datos personales?

El derecho a la protección de datos de carácter personal en la LAIP
otorga a las personas el derecho a que se protejan sus datos,
así como el derecho a saber si se están utilizando, por quién
y para qué, a obtener una copia inteligible o comprensible
y sin demora de los datos que están siendo utilizados,
a modificarlos y actualizarlos y a conocer
qué información personal poseen los entes públicos.

¿En qué principios debe basarse la protección de datos personales?

Los principios de la protección de datos personales
son un conjunto de reglas que indican cómo deben tratarse
dichos datos para garantizar la privacidad de las personas
desde que se obtienen hasta que se eliminan.

Dichos principios son los que a continuación se indican:

- **Licitud**
  Obtener los datos personales de acuerdo con la ley.
  Además, los datos personales deben recopilarse
  con fines determinados, expresos y legítimos.

- **Calidad**
  Sólo se pueden tratar datos personales que sean adecuados,
  pertinentes y no excesivos en relación con finalidades lícitas.
  Se deben eliminar los datos que dejen de cumplir
  estas características.

  Cada institución debe poseer sólo aquellos datos personales
  que necesite para ejercer su función.
  Por ejemplo, un hospital puede tener
  datos personales relacionados con la salud
  de sus pacientes, pero no sobre sus estudios académicos.

- **Exactitud**
  Los datos deben ser correctos, veraces y estar actualizados.

- **Acceso, corrección y supresión o eliminación**
  Todas las personas pueden ejercer los derechos de acceso,
  corrección, y supresión o eliminación sobre sus datos personales
  para consultarlos, revisarlos y cancelarlos,
  en los casos en que sean falsos, inexactos o excesivos.

  Pero existen excepciones, por ejemplo, para cancelar
  datos personales. Si una persona solicita suprimir sus datos
  puede ocurrir que esos datos deban permanecer
  durante determinado tiempo para atender
  posibles responsabilidades derivadas del tratamiento de esos datos.

- **Información**
  Al recabar datos personales se debe informar de forma expresa
  a la persona titular de dichos datos la finalidad
  para la que se van a utilizar.

- **Seguridad**
  Los datos deben guardarse de forma que se evite su alteración
  y pérdida, así como su transmisión o acceso no autorizados.

- **Custodia y cuidado**
  Los datos deben estar conservados,
  y se debe garantizar que cualquier persona
  que los consulte lo haga de forma cuidadosa y diligente.

- **Consentimiento para transmitir o comunicar datos**
  La persona titular debe autorizar la comunicación
  de sus datos a terceras personas ajenas a ella
  o a la organización que los posea de manera legítima.

- **Consentimiento informado**

  Al recabar datos se debe informar de forma clara a su titular sobre:
  - La existencia y denominación de una base de datos personales.
  - La finalidad para la que se solicitan y recaban.
  - Los destinatarios de la información.
  - Quién los puede consultar.
  - Si es obligatorio o no suministrarlos, y qué consecuencias se derivan de suministrarlos o no hacerlo.
  - Qué se va a hacer con los datos personales recabados.
  - Sus derechos sobre sus datos personales, y cómo ejercerlos.
  - Quién es el responsable de la base de datos: Identidad y dirección.

El titular debe dar su consentimiento para que se recopilen sus datos.
Una vez prestado el consentimiento la persona puede revocarlo.
Esta revocación impedirá que se sigan tratando los datos personales;
pero no podrá evitar los efectos que ya haya tenido el tratamiento de sus datos hasta el momento de la revocación.

No será necesario el consentimiento de la persona titular de los datos personales si se trata de datos de acceso público o si su tratamiento está ordenado por una Ley.

El consentimiento de la persona titular de los datos personales debe ser libre, específico, informado e inequívoco.

- **Confidencialidad**

  Se debe garantizar que únicamente las personas autorizadas puedan acceder a los datos personales para tratarlos.
  Las personas autorizadas deberán guardar obligación de secreto.
  Esta obligación se mantendrá aún después de finalizar su vínculo profesional con las organizaciones responsables del tratamiento de tales datos.

El Instituto de Acceso a la Información Pública

Es una institución pública, con autonomía administrativa y financiera. Entre sus funciones está:

- Hacer cumplir la Ley de Acceso a la Información Pública (LAIP).
- Decidir sobre transparencia y acceso a la información pública.
- Garantizar la protección y el correcto tratamiento de los datos personales que recopilan los entes públicos.
- Definir los procedimientos de inscripción y registro de bases de datos y atender las denuncias presentadas por los particulares.
- Elaborar un manual de protección de datos para el Sector Público.
- Elaborar recomendaciones de seguridad para proteger los datos personales.
- Elaborar un plan de capacitación sobre datos personales para el sector público.

Síntesis de las atribuciones del Instituto en materia de protección de datos personales:

- Difundir, asistir y promocionar:
  - Dar a conocer las leyes y reglamentos. sobre la protección de datos.
  - Asistir a los titulares de los datos y a los responsables que los tratan.
  - Promocionar la profesionalización de los servicios públicos sobre la protección de datos.
- Registrar: Debe llevar un control de las bases de datos que tienen los entes públicos. Éstos deben comunicar al Instituto si crean, modifican o eliminan algún sistema de datos.
- Crear normas: Posee facultades normativas en esta materia.
- Revisar: Tiene la capacidad de revisar sus propios actos, siendo la resolución que adopte definitiva y obligatoria.

Los entes públicos deben permitir al Instituto acceder a los lugares
donde se encuentran y se operan sus bases de datos,
para que pueda comprobar que se realiza de forma correcta.

¿Cómo se protegen los datos personales?

Los entes públicos están obligados a adoptar medidas de seguridad
para garantizar la integridad, exactitud y calidad de los datos
que recopilan. Estas medidas deben evitar la alteración, pérdida,
transmisión y acceso no autorizado a los datos personales.

Se debe crear un documento de seguridad para proteger
los datos personales. Como mínimo, debe contener:

- El ámbito de aplicación.
- Las medidas, normas, procedimientos de actuación, reglas
  y estándares utilizados.
- Las funciones y obligaciones del personal en relación
  con el tratamiento de los datos de carácter personal.
- La estructura de los sistemas de datos personales
  que contengan datos de carácter personal y la descripción
  de los sistemas de información que los tratan.
- El procedimiento de notificación, gestión y respuesta
  ante incidencias.
- Los procedimientos para realizar copias de respaldo
  y de recuperación de los datos en los ficheros
  o tratamientos automatizados.
- Las medidas para el transporte de soportes y documentos,
  su destrucción o la reutilización.
- Debe mantenerse actualizado y revisados.

Niveles de seguridad

Existen tres niveles (básico, medio y alto)
y se sugieren las siguientes medidas para cada uno de ellos:

Nivel básico

Documento de seguridad: Los entes público deben elaborar un documentos
de seguridad que refleje las medidas y procedimientos de seguridad
que garanticen la seguridad de los datos personales que tratan.
Estos documentos los deberían realizar los responsables
de las bases de datos, y deberían contener:

- **Registro de incidencias:**
  Donde quede reflejado quién, cuándo y por qué ha tenido acceso
  a la base de datos y en qué consistió su intervención.
- **Sistema de identificación:**
  Herramientas tecnológicas de la información (encriptación, uso de claves
  y firmas digitales) que identifique quién accede a los datos personales.
- **Organigrama de la institución** y manuales de puestos:
  Las tareas de seguridad deberían realizarlos funcionarios concretos,
  así se puede controlar si se cumplen estas tareas.
- **Copias de seguridad y recuperación**: Garantizar protocolos
  de recuperación de los datos ante una incidencia
  o acto vandálico para recuperar la base de datos.

Nivel medio

- **Responsable de seguridad:** Establecer un responsable a quien corresponde
  tomar medidas, darles seguimiento y mantener estándares de calidad
  de manera periódica.
- **Auditorías:** Internas y externas, para verificar que se cumplen las normativas.
  Los informes de estas auditorías se deberían entregar al IAP, y éste realizar
  un análisis en un plazo razonable (unos 20 días)
  y proponer medidas de mejora.

Nivel alto

- Uso intensivo de claves de acceso y encriptación.
- **Registro de acceso:** El acceso a las bases de datos está limitado al personal autorizado.
  Se controla la identificación, hora, fichero, tipo de acceso, autorizado o denegado, y se guardan los datos durante 2 años.
- **Telecomunicaciones:** Las transmisiones de los datos deben producirse de manera cifrada, para que no se puedan manipular ni en el lugar de origen ni en el origen de llegada.

Bases de datos

Los datos deben almacenarse en una base de datos organizada, que permita ejercer los derechos de acceso, rectificación y eliminación.

Los entes públicos deben establecer políticas de seguridad que permitan tramitar y procesar los datos de forma ágil y segura.
Así, la ciudadanía se siente confiada en cómo el Estado gestiona los datos.
Estas políticas de protección de datos deben tener en cuenta:

- La finalidad de la base de datos personales y sus usos.
- Las personas o grupos de personas sobre los que obtener datos o que resulten obligados a suministrarlos.
- El procedimiento para recopilarlos.
- La estructura básica de la base de datos y la descripción de los tipos de datos incluidos.
- La cesión de las que pueden ser objeto los datos.
- Las instancias responsables de tratar la base de datos.
- La unidad administrativa para ejercer los derechos de acceso, rectificación o eliminación.
- El nivel de protección.

Si se suprime una base de datos, se debe indicar dónde van almacenar los datos que contiene, o cómo se van a destruir.
En este caso se debe documentar qué tipo de datos se van a destruir, sus titulares y quien es la persona encargada de hacerlo y quien supervisa la destrucción.

El registro de las bases de datos

El IAIP es responsable de llevar un registro de los sistemas de datos personales de los entes públicos.
Éstos deben notificarle al IAIP si crean, modifican o suprimen datos personales.
Así, cualquier persona podrá conocer las bases de datos existentes en las dependencias administrativas, y podrá ejercer sus derechos.

Tanto la creación de una base de datos como los registros deben contener la siguiente información:

- Nombre de la base de datos personales, indicando normativa aplicable, finalidad y usos.
- Nombre del sistema.
- El origen de los datos, indicando el colectivo de personas sobre las que se pretende obtener datos, o que resulten obligados a suministrarlos; su procedencia y cómo se han obtenido.
  - Nombre, cargo, teléfono y correo electrónico del responsable.
  - La estructura básica del sistema, con descripción detallada de datos identificativos y, en su caso, de los especialmente protegidos, las restantes categorías de datos de carácter personal; modo de tratamiento utilizado en su organización (manual o automatizado).
    En su caso, señalar los datos de carácter obligatorio y facultativo.

- Identificación del sistema, finalidades, usos y soporte.
- Las cesiones previstas, los destinatarios o categorías de destinatarios.
- La categoría de los datos, cómo se han recopilado y cómo se van actualizar.
- La unidad administrativa a la que corresponde el sistema y el cargo del responsable.
- Unidad administrativa en la que se encuentra el sistema.
- Domicilio oficial y dirección electrónica de la Oficina de Información Pública.
- Destino y personas físicas o morales a las que se pueden transmitir.
- Nivel de seguridad: básico, medio o alto.
- Modo de interrelacionar la información y el plazo de conservación.
- Normativa aplicable.

Cuando los entes públicos recopilan información sobre una persona, deben informarla sobre:

- La existencia de una base de datos, cómo se van a tratar, la finalidad y los destinatarios de la información.
- El carácter obligatorio o facultativo de responder a las preguntas.
- Las consecuencias de obtener datos personales, de negarse a suministrarlos o de su inexactitud.
- La posibilidad para que estos datos sean difundidos: De ser así, debe constar el consentimiento expreso del interesado, salvo si son públicos.
- La posibilidad de ejercitar los derechos de acceso, rectificación y eliminación y oposición.
- El nombre del responsable de la base de datos y los destinatarios.

Si los datos no se han obtenido directamente de la persona interesada, el ente público debe informarla en un plazo prudencial, que suelen ser 3 meses.

El ente público debe informar a la persona interesada cuando se recopilan sus datos, pero existen excepciones:

- Que se haya le informado con anterioridad.
- Que así lo prevea expresamente una Ley.
- Cuando los datos provengan de fuentes públicas.
- Cuando resulte imposible o exija un esfuerzo desproporcionado a la persona interesada. En el caso de sistemas muy grandes deberían proveerse medios de comunicación vía web.

Datos sensibles

Es necesario el consentimiento de la persona para utilizar los siguientes datos:

- Origen étnico o racial
- Características morales o emocionales
- Ideología y opiniones políticas
- Creencias
- Convicciones religiosas
- Ideas filosóficas
- Preferencia sexual

Está prohibido crear bases de datos para almacenar estos datos, excepto si:

- Existen razones de interés general.
- Lo dispone una ley.
- Lo consiente expresamente la persona interesada.
- Tiene fines estadísticos o históricos, pero deben ser datos disasociados.

La difusión de este tipo de datos puede provocar que se rechace o se discrimine a la persona.

Datos personales para fines policiales

El derecho de la protección de datos personales no limita
que se recopilen datos para investigaciones penales o administrativas.
Pero se deben tomar medidas de seguridad reforzadas
y contar con una autorización judicial.

¿Cuándo se pueden tratar los datos personales?

Cuando la persona interesada da su consentimiento
de forma libre, inequívoca, específica e informada.

Existen excepciones, pero siempre se deben tener en cuenta
los principios antes mencionados en este Manual
y analizar cada caso en concreto.

Algunos ejemplos de excepciones al consentimiento:

- Cuando se esté en presencia del ejercicio de las atribuciones legales atribuidas a los entes públicos. Ejemplo: recaudación de impuestos.
- Datos estrictamente necesarios para el desarrollo de la actividad laboral. Ejemplo: tarjeta de control horario.
- Ámbito de la salud: cuando el estado de salud del paciente no permite recabar su consentimiento, en medidas de urgencia para detener un brote o epidemia.
- Ámbito electoral: los padrones electorales, las listas de partidos y electores.
- Cuando hay transmisión de datos entre organismos con fines estadísticos, históricos o científicos.
- La cesión de datos personales de un ente público a un tercero prestador de un servicio.
- Cuando media una orden judicial.
- Cuando los datos figuren en registros públicos, el tratamiento sea necesario, y no se vulneren sus derechos y libertades.

La persona interesada puede revocar su consentimiento
si existe una causa justificada.
No se le atribuyan efectos retroactivos.
Deberá presentar una solicitud a la Oficina pertinente,
a través de los formatos emitidos por el Instituto.

¿Quién puede tratar los datos personales?

El titular del ente público es el responsable del tratamiento
de las bases de datos personales.

Este responsable debe adoptar las medidas necesarias
para proteger los datos y asegurarse
que cualquier persona que acceda a la base de datos aplique
y respete los principios relativos a la protección de datos.

El encargado de tratamiento es la persona o entidad
que accede a los datos de carácter personal
para prestar algún tipo de servicio al responsable del fichero.
Un ejemplo es la videovigilancia en la que una empresa ajena
a la organización accede a la imagen de las personas
para desarrollar este servicio.
O el mantenimiento del hardware o software informático.
O incluso la realización de sercicios de limpieza
para la organización por cuenta de una empresa externa
ya que puede tener disponibilida a los datos.

Este acceso a los datos debe formalizarse
en un contrato específico que, como mínimo,
recoja lo siguiente:

- Que los datos serán tratados por el encargado conforme a las instrucciones del responsable.
- Que nos se utilizarán para una finalidad distinta a la contratada.

- Que no se comunicarán a otras personas.
- Que se adoptarán las medidas de seguridad legalmente exigidas.
- Que se devolverán al responsable o se destruirán una vez finalizada la relación contractual de servicios.

¿Qué derechos tiene la ciudadanía sobre sus datos?

Cualquier persona tiene derecho a:

- Acceder a sus datos
- Rectificarlos
- Cancelarlos
- Oponerse a su tratamiento

Toda persona tiene, además, derecho a que se le informe de forma gratuita del origen de sus datos y a saber a qué otras personas o entidades han sido comunicados.

Se podrán denegar estos derechos si existe una causa legal o justificada.

Derecho	Descripción
Acceso	Permite obtener información de los datos, la finalidad, su origen y las comunicaciones.
Rectificación	Permite solicitar que se modifiquen los datos inexactos o incompletos.
Eliminación	Permite eliminarlos si son: • Inadecuados • Excesivos • No se ajustan a la Ley o a los Lineamientos
Oposición	Permite oponerse a que se cedan los datos.

¿Cómo ejercer estos derechos?

Para poder ejercer estos derechos la persona interesada, o su representante legal, debe identificarse con la credencial para votar, el pasaporte vigente o la cédula profesional.

Debe presentar una solicitud a la oficina encargada en el ente:

- Por correo postal o mensajería
- Por correo electrónico
- De forma verbal. El responsable deberá recogerla en el formato correspondiente

La solicitud debe contener:

- Ente público al que se dirige la solicitud.
- Nombre completo y, en su caso, el de su representante legal.
- Descripción clara y precisa de los datos personales requeridos.
- Cualquier otro elemento que facilite su localización.
- El domicilio, u otro medio para recibir notificaciones.

Además de estos requisitos, existen otros específicos
según lo que se solicita:

- **Derecho de acceso:** Indicar la modalidad de respuesta:
  presencial, copias simples o certificadas.
- **Derecho de rectificación:** Señalar el dato erróneo
  y la corrección que deba realizarse, acompañado
  de la documentación que lo avale.
- **Derecho de eliminación:** Indicar las razones por las cuales
  se considera que el tratamiento de los datos no se ajusta a la normativa.

¿Dónde dirigirse?

A la oficina competente en la materia de que se trate.
Todos los entes públicos deben tener una oficina
donde la ciudadanía pueda ejercer sus derechos.

¿Cuándo se obtiene respuesta?

El plazo máximo para la respuesta es de 10 días hábiles
contados a partir de la fecha de la solicitud

La respuesta debe estar suscrita y firmada
por la persona responsable del ente público.
Puede ser:

- Procedente: Respuesta positiva a la petición.
- No procedente: Se deniega la petición.
  Se deben especificar las razones.

¿Cuánto cuesta?

El trámite es gratuito, pero la persona solicitante debe pagar
los costos de reproducir los datos solicitados.
Se debe pagar antes de recibir los datos.

¿Cómo apelar?

La persona solicitante tiene derecho a presentar un recurso
de apelación ante el Instituto de Acceso a la Información Pública.
Al hacer la solicitud, se debe informar sobre este derecho,
del modo de hacerlo y del plazo establecido.

Si el recurso se presenta por falta
de respuesta del ente público, el plazo empieza
a contar desde que concluye el período
que tenía el ente para contestar.

En el recurso se debe indicar:

- La dependencia o entidad dónde se presentó la solicitud.
- El nombre de la persona que recurre y el lugar o medio
  para recibir notificaciones.
- La fecha en que se notificó a la persona que recurre.
- El acto y los puntos a recurrir.

Si la persona que recurre no cumple algún requisitos,
el Instituto, en un plazo no mayor de 3 días hábiles
debe informarle y concederle 3 días hábiles más
para que corrija las irregularidades.

Una vez presentado el recurso,
el Instituto tiene 15 días hábiles para emitir
una resolución a través del siguiente procedimiento:

1. Revisa y emite un acuerdo, en un plazo de 3 días hábiles.

2. En caso de no cumplir con alguno
   de los requisitos establecidos, puede solicitar
   que se corrijan en un plazo de 3 días hábiles.

3. Si se admite el recurso, una comisión lo analiza
   y en 15 días presenta un proyecto de resolución
   que presenta al pleno del Instituto.
   Este comisionado no participa en las decisiones del pleno.

4. Si se admite el recurso, se debe comunicar la resolución
   tanto a la persona interesada, como al ente
   y a la persona responsable si también ha sido denunciada.
   El ente y la persona responsable debe hacer
   un informe en un plazo de 7 días hábiles.

5. Las partes pueden ofrecer pruebas hasta el día
   que se celebre la audiencia oral.

6. El Instituto celebrará una audiencia oral con las partes.

7. Si existe una causa justificada, el pleno del Instituto
   puede ampliar, 10 días el plazo para celebrar la audiencia.
   Las resoluciones del Instituto se pueden recurrir
   ante la Sala de lo Contencioso Administrativo
   de la Corte Suprema de Justicia.

Infracciones y sanciones

La Ley de Acceso a la Información Pública establece
una serie de infracciones por el mal uso
de la información pública por parte
del personal empleado de los entes públicos.
Su infracción está castigada con sanciones de tipo económico,
sin perjuicio de las responsabilidades penales, civiles,
administrativas o de otra índole en que incurra el responsable.

EUROsocIAL
PROGRAMA PARA LA COHESIÓN SOCIAL EN AMÉRICA LATINA

Con apoyo de:

FIIAPP
COOPERACIÓN ESPAÑOLA

FUNDACIÓN CEDDET

RED IBEROAMERICANA DE PROTECCION DE DATOS

Con la participación de:

LF
Asociación Lectura Fácil