PROTECCIÓN DE DATOS PERSONALES

info

VISIÓN FEDERALISTA DEL RÉGIMEN DE PROTECCIÓN DE DATOS PERSONALES: ÁMBITOS VARIOS EN EL EJERCICIO DE LA PDP

Gabriela Magdaleno del Río
Directora de Datos Personales del INFO CDMX

Planteamiento del problema:

El desarrollo tecnológico ha traído consigo nuevos tipos de interacciones en la red que implican que todos los días expongamos información relacionada con nuestra vida privada. Esto a su vez ha desarrollado nuevos tipos de delitos y, por ende, nuevos retos para resguardar nuestra privacidad.

Antecedentes del derecho a la protección de los datos personales:

- **A partir del siglo XVIII, los derechos humanos comenzaron a ser reconocidos en la normativa constitucional.**
- **Su reconocimiento constitucional implicó que fueron alcanzando su consolidación como prerrogativas inherentes a todo ser humano.**
- **Como parte de estos derechos humanos, se incorporó el derecho a la intimidad de la persona.**
- **Con el avance tecnológico este derecho ha ido alcanzando nuevos matices.**

Antecedentes del derecho a la protección de los datos personales:

- ***Los datos personales se han convertido en una práctica habitual de control y almacenamiento por parte de los sectores tanto públicos como privados.***
- ***El derecho a la intimidad ha tenido que ir redireccionando su ámbito de protección.***

Objetivo:

- ***Hacer un análisis respecto al reconocimiento que se ha venido realizando a este derecho derivado del derecho a la intimidad.***

Objetivo:

- ***Hacer un análisis respecto al reconocimiento que se ha venido realizando a este derecho derivado del derecho a la intimidad.***

Las generaciones de los derechos humanos

- ***La aparición de generaciones de derechos no constituye la sustitución global de un catálogo de derechos por otro.***

- ***Implica el reconocimiento de nuevos derechos que intentan dar respuesta a las nuevas necesidades históricas.***

Las generaciones de los derechos humanos

	Primera generación de derechos humanos	Segunda generación de derechos humanos	Tercera generación de derechos humanos
Época	Siglo XVIII	Siglo XIX	Siglo XX y XXI
Definición	La defensa de la persona cuya exigencia consistía en la autolimitación y la no injerencia de los poderes públicos en la esfera privada de la persona.	Matiz ideológico de las propias libertades individuales. Completar el catálogo de derechos y libertades de la primera generación.	Una respuesta al fenómeno de lo que se ha denominado "contaminación de las libertades" que implica la erogación y degradación que aqueja a los derechos fundamentales ante las nuevas tecnologías.
Tipo de derechos	Derecho al honor, a la vida, a la integridad personal, reconocimiento a la intimidad…	Derechos económicos, sociales y culturales. Derechos de participación para una política activa de los poderes públicos (Estado social de derecho)	Surgimiento de nuevos perfiles del derecho a la intimidad: derechos a la libertad informática, derecho a la autodeterminación informativa, derechos a la PDP.

Del derecho a la intimidad a la PDP

Derecho a la intimidad	Derecho a la privacidad	Derecho a la protección de datos personales
Abarca aquello que se considera más propio y oculto del ser humano (la información que mantiene para si mismo).	Una garantía del individuo a la protección de su persona y su seguridad frente a cualquier invasión a su vida privada.	La intimidad a perdido su carácter individual y privado, para asumir una significación pública y colectiva, consecuencia del cauce tecnológico.
Derecho del individuo a la soledad y a tener una esfera reservada sin que la indiscreción ajena tenga acceso a ella.	Proteger las creencias, los pensamientos, las emociones y sensaciones de la persona.	Tiene la función dinámica de controlar la circulación de informaciones relevantes para cada sujeto y ya no solo la defensa de la vida privada del conocimiento ajeno.
La intimidad de la persona ha encontrado su justificación y fundamento en el derecho.	Garantizar a los ciudadanos la seguridad de su persona, de su domicilio y de sus efectos frente a cualquier intromisión indebida del gobierno.	El control sobre las informaciones que nos conciernen. No es sólo la falta de información por parte de los demás.
La intimidad se justifica como un medio para promover la libertad individual.		Un derecho activo de control sobre el flujo de informaciones que afectan a cada sujeto.
Idea de libertad como autonomía individual.		Es necesario el reconocimiento de la información relativa a la persona. Pero, además el establecimiento de mecanismos de protección que puedan hacer frente a su uso y manejo.
Derecho a una absoluta independencia, puesto que el individuo es soberano sobre su cuerpo y mente.		

El derecho fundamental a la protección de datos personales

- ***Los datos de toda persona deben ser objeto de protección para que éstos puedan ser tratados o elaborados, y finalmente ser convertidos en información y, en consecuencia, sólo ser utilizados para los fines y personas autorizadas.***

- ***La PDP es aquella parte de la legislación que protege el derecho fundamental de la libertad, en particular, el derecho individual a la intimidad respecto del procesamiento manual o automático de datos.***

- ***En el ámbito europeo se entiende por datos personales: toda aquella información sobre una persona física identificada o identificable (el interesado).***

- ***Se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación, o uno o varios elementos específicos, características de su identidad física, psíquica, social, etc.***

El estudio de la protección de los datos personales

- ***Conviene iniciar el estudio de la protección de datos personales, desde el primer desafío de las nuevas tecnologías de la información con respecto a la recolección, procesamiento y transmisión de datos personales.***

- ***El derecho a la protección de datos refleja más que una idea individualista de protección a la intimidad, puesto que engloba los intereses de grupo contra el procesamiento, almacenamiento y recolección de información.***

El estudio de la protección de los datos personales

- ***Las nuevas tecnologías ha permitido tratar, elaborar y transmitir informaciones, como la han sido los datos relativos a la persona, lo que en consecuencia ha supuesto la aparición de nuevos derechos y libertades, o bien, el replanteamiento de su contenido.***

- ***La delimitación conceptual del derecho a la intimidad como facultad de aislamiento, ahora se ha convertido en un poder de control sobre las informaciones que son relevantes para cada sujeto.***

- ***El peligro para la privacidad del individuo no radica en que se acumule la información sobre él, sino, más bien, en que pierda la capacidad de disposición sobre ella y respecto a quién y con qué objeto se transmite.***

El estudio de la protección de los datos personales

- ***En la era tecnológica, a cada individuo le corresponde conocer cuál será el uso de los datos personales inscritos en ficheros, que puedan ser objeto de un tratamiento automatizado, y podrá exigir que su almacenamiento y control sea adecuado para que no se vea vulnerado en su libertad y dignidad.***

La protección de los datos personales en México

- Desde la Constitución Política de los Estados Unidos Mexicanos de 1917 se han establecido derechos relativos a la libertad individual, entre los que destacan la inviolabilidad de correspondencia y domicilio y el secreto de las comunicaciones privadas.
- Con el creciente avance tecnológico en este país, fue necesario dar respuesta a las nuevas pretensiones individuales, consecuencia de los cambios sociales que el avance tecnológico ha introducido.
- En 2002 se aprobó la Ley Federal de Transparencia y Acceso a la Información Pública, en esta se estipulo la primera definición de datos personales:

"La información concerniente a una persona física, identificada o identificable, entre otra, la relativa a su origen étnico o racial, o que esté referida a las características físicas, morales o emocionales, a su vida afectiva y familiar, domicilio, número telefónico, patrimonio, ideología y opiniones políticas, creencias o convicciones religiosas, los estados de salud físicos o mentales, las preferencias sexuales, u otras análogas que afecten su intimidad.

Visión federalista en el régimen de protección de datos personales

datos personales

Un dato personal es cualquier información relacionada a una persona.

Nombre

Fecha de nacimiento

Número telefónico

ADN

RFC

Huellas dactilares

Ingresos

Domicilio

Cédula profesional

Dirección de correo electrónico

Cuentas bancarias

Nacionalidad

CURP

Estado de salud

Fotografía

Estado Civil

Edad

Firma

También son datos personales:

Preferencia sexual

Religión

Ideología

Origen étnico

¿Qué son datos personales?

Dato Personal. Toda información concerniente o relativa a una persona física identificada o identificable.

Dato Sensible. Tiene un régimen de garantías más reforzado que el que tiene el tratamiento cualquier otra información.

La protección de **datos personales** es un derecho fundamental de tercera generación que busca la protección de la persona en relación con el tratamiento de su información.

El DPDP ha sido relacionado con el derecho a la intimidad. Actualmente, se ha configurado un auténtico **derecho** de protección de datos personales, distinto al derecho a la intimidad.

La protección de datos personales busca controlar o defender, la **Autodeterminación Informativa,** es decir, que el uso de la información personal contenida en bases de datos sea exactamente el que el individuo autorizó.

Legislación

13 de abril de 2010	• La Cámara de Diputados aprobó la LFPDPPP
27 de abril de 2010	• El Senado de la República aprobó dicho dictamen
5 de julio de 2010	• El Poder Ejecutivo Federal publicó en el DOF la LFDPPP

Sujetos regulados

De acuerdo al artículo 2 de la LFPDPPP, todas las personas físicas o morales que para sus actividades cotidianas recaben, manejen y utilicen información personal, con excepción de:

- Las sociedades de información crediticia.

- Las personas que llevan a cabo la recolección y almacenamiento de datos personales para uso exclusivamente personal, y sin fines de divulgación o utilización comercial.

Principios de la Protección de Datos Personales

Licitud. Se refiere al compromiso que deben asumir los entes privados que traten información del titular cuando solicitan la prestación de un bien o servicio.

Calidad. Los datos de salud, deberán ser exactos, adecuados, pertinentes y no excesivos, para lograr la finalidad por la cual fueron recabados.

Responsabilidad. Quienes traten datos personales deben asegurar que ya sea dentro o fuera de nuestro país, se cumpla con los principios esenciales de protección de datos personales, comprometiéndose a velar siempre por el cumplimiento de estos principios y a rendir cuentas en caso de incumplimiento.

Principios de la Protección de Datos Personales

Proporcionalidad. Las empresas sólo podrán recabar los datos estrictamente necesarios e indispensables para la finalidad que se persigue y que justifica su tratamiento.

Consentimiento. Toda transmisión deberá contar con el consentimiento libre, expreso e informado del titular de los mismos, salvo las excepciones legales conducentes.

Información. Se deberá hacer del conocimiento del titular el fundamento y motivo por el que se recaban los datos, así como los propósitos para los cuales se tratarán. (Los responsables deben dar a conocer esas características a través del "Aviso de Privacidad")

Aviso de privacidad

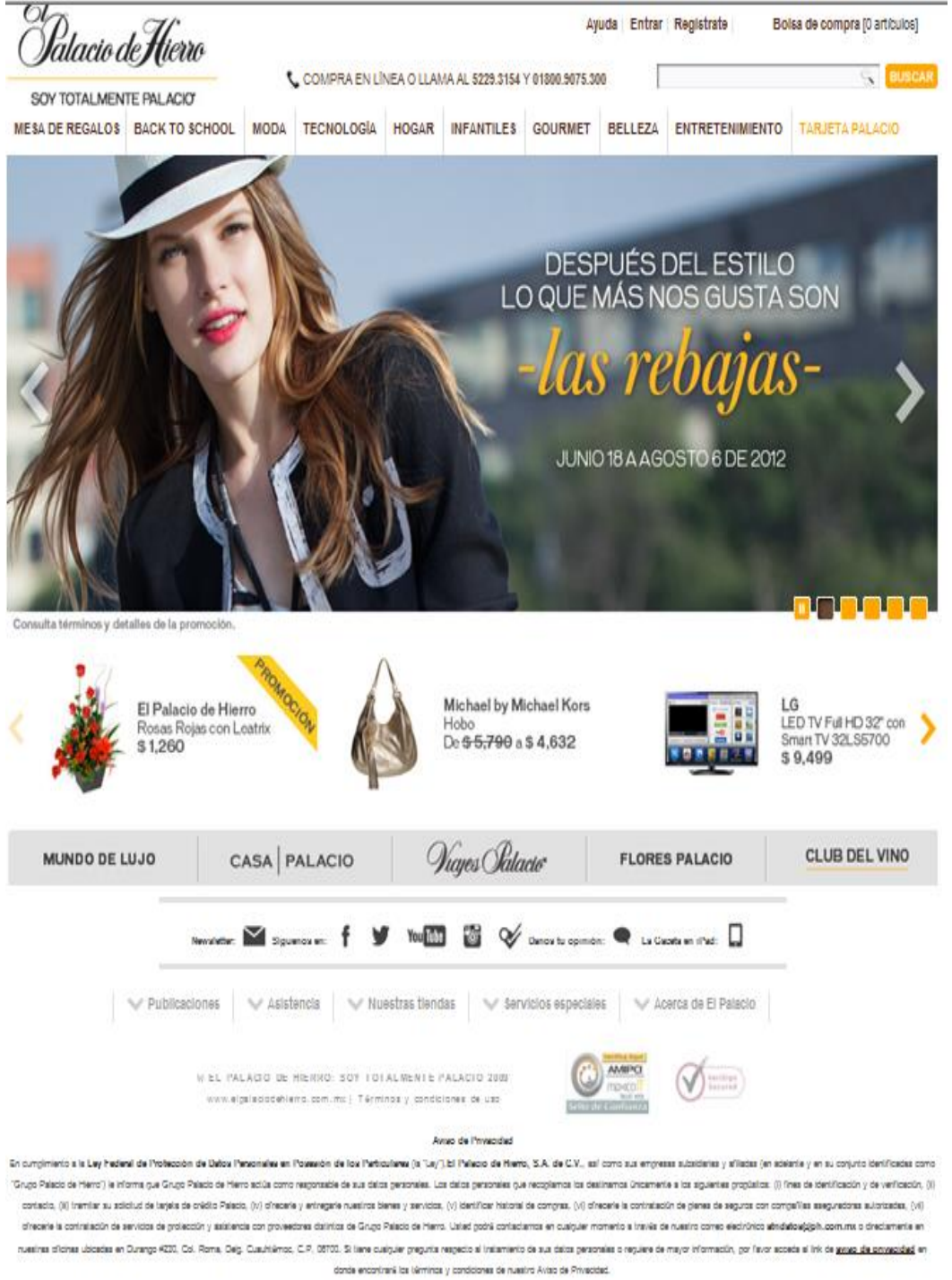
El artículo 15 de la Ley de Protección de Datos Personales en Poder de los Particulares establece:

> «El responsable tendrá la obligación de informar a los titulares de los datos, la información que se recaba de ellos y con que fines, a través del **Aviso de Privacidad**.»

El aviso de privacidad deberá contener, al menos, la siguiente información:

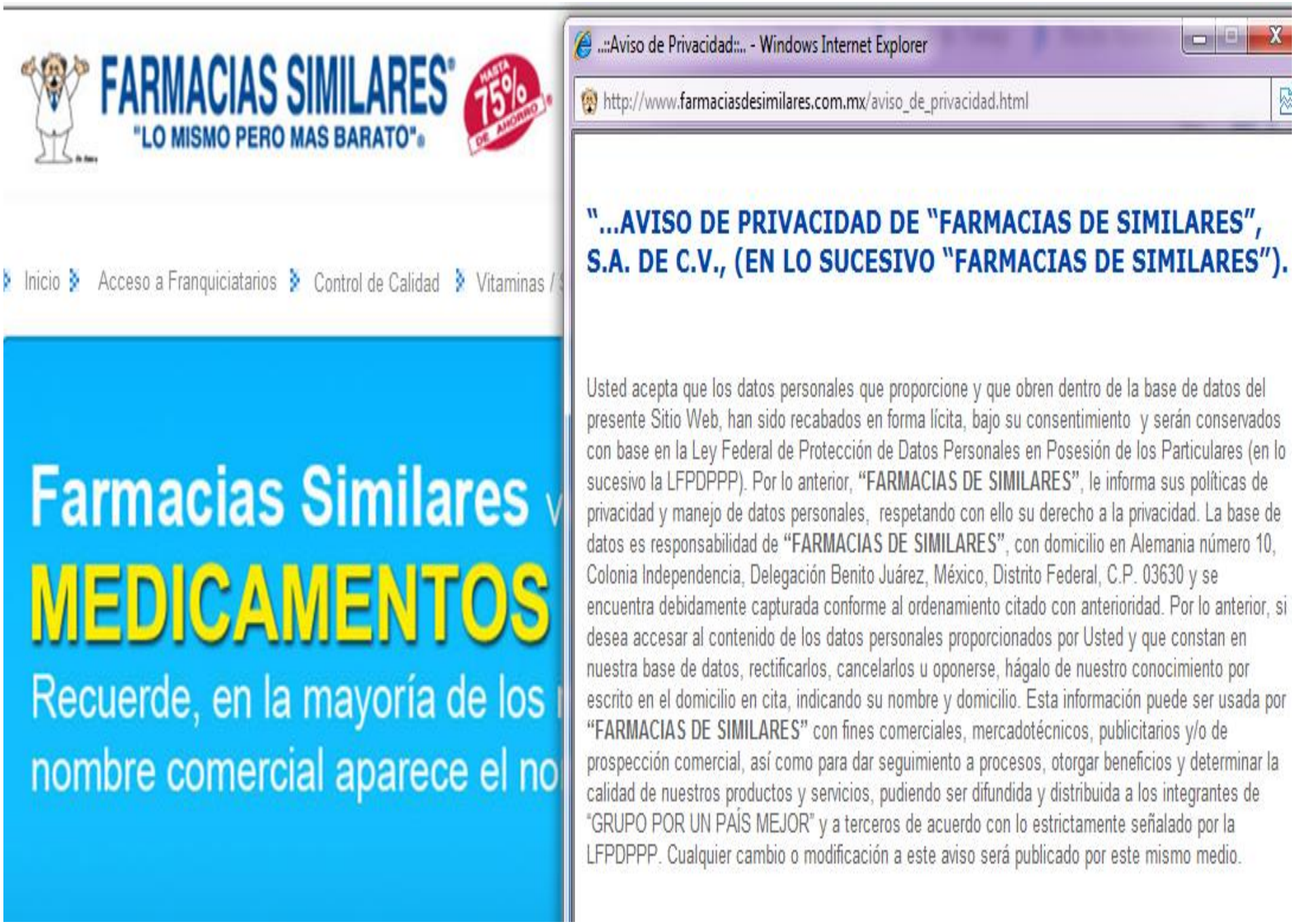
- La identidad y domicilio del responsable.
- Las finalidades del tratamiento de datos.
- Las opciones y medios que el responsable ofrezca a los titulares para limitar el uso o divulgación de los datos.
- Los medios para ejercer los derechos ARCO.
- En su caso las transferencias de datos que se efectúen.
- El procedimiento y medio por el cual el responsable comunicará a los titulares de cambios al aviso de privacidad.

En caso de los **datos personales sensibles**, el aviso de privacidad deberá señalar expresamente que se trata de este tipo de datos.



Aviso de Privacidad

En cumplimiento a la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (la "Ley"),El Palacio de Hierro, S.A. de C.V., así como sus empresas subsidiarias y afiliadas (en adelante y en su conjunto identificadas como "Grupo Palacio de Hierro") le informa que Grupo Palacio de Hierro actúa como responsable de sus datos personales. Los datos personales que recopilamos los destinamos únicamente a los siguientes propósitos: (i) fines de identificación y de verificación, (ii) contacto, (iii) tramitar su solicitud de tarjeta de crédito Palacio, (iv) ofrecerle y entregarle nuestros bienes y servicios, (v) identificar historial de compras, (vi) ofrecerle la contratación de planes de seguros con compañías aseguradoras autorizadas, (vii) ofrecerle la contratación de servicios de protección y asistencia con proveedores distintos de Grupo Palacio de Hierro. Usted podrá contactarnos en cualquier momento a través de nuestro correo electrónico atndatos@ph.com.mx o directamente en nuestras oficinas ubicadas en Durango #230, Col. Roma, Delg. Cuauhtémoc, C.P. 06700. Si tiene cualquier pregunta respecto al tratamiento de sus datos personales o requiere de mayor información, por favor acceda al link de aviso de privacidad en donde encontrará los términos y condiciones de nuestro Aviso de Privacidad.


FARMACIAS SIMILARES
"LO MISMO PERO MAS BARATO"
HASTA 75% DE AHORRO
Inicio
Acceso a Franquiciatarios
Control de Calidad
Vitaminas
Farmacias Similares
MEDICAMENTOS
Recuerde, en la mayoría de los
nombre comercial aparece el no
...:Aviso de Privacidad:... - Windows Internet Explorer
http://www.farmaciasdesimilares.com.mx/aviso_de_privacidad.html
"...AVISO DE PRIVACIDAD DE "FARMACIAS DE SIMILARES", S.A. DE C.V., (EN LO SUCESIVO "FARMACIAS DE SIMILARES").
Usted acepta que los datos personales que proporcione y que obren dentro de la base de datos del presente Sitio Web, han sido recabados en forma lícita, bajo su consentimiento y serán conservados con base en la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (en lo sucesivo la LFPDPPP). Por lo anterior, "FARMACIAS DE SIMILARES", le informa sus políticas de privacidad y manejo de datos personales, respetando con ello su derecho a la privacidad. La base de datos es responsabilidad de "FARMACIAS DE SIMILARES", con domicilio en Alemania número 10, Colonia Independencia, Delegación Benito Juárez, México, Distrito Federal, C.P. 03630 y se encuentra debidamente capturada conforme al ordenamiento citado con anterioridad. Por lo anterior, si desea accesar al contenido de los datos personales proporcionados por Usted y que constan en nuestra base de datos, rectificarlos, cancelarlos u oponerse, hágalo de nuestro conocimiento por escrito en el domicilio en cita, indicando su nombre y domicilio. Esta información puede ser usada por "FARMACIAS DE SIMILARES" con fines comerciales, mercadotécnicos, publicitarios y/o de prospección comercial, así como para dar seguimiento a procesos, otorgar beneficios y determinar la calidad de nuestros productos y servicios, pudiendo ser difundida y distribuida a los integrantes de "GRUPO POR UN PAÍS MEJOR" y a terceros de acuerdo con lo estrictamente señalado por la LFPDPPP. Cualquier cambio o modificación a este aviso será publicado por este mismo medio.

Generador de avisos de privacidad del INAI

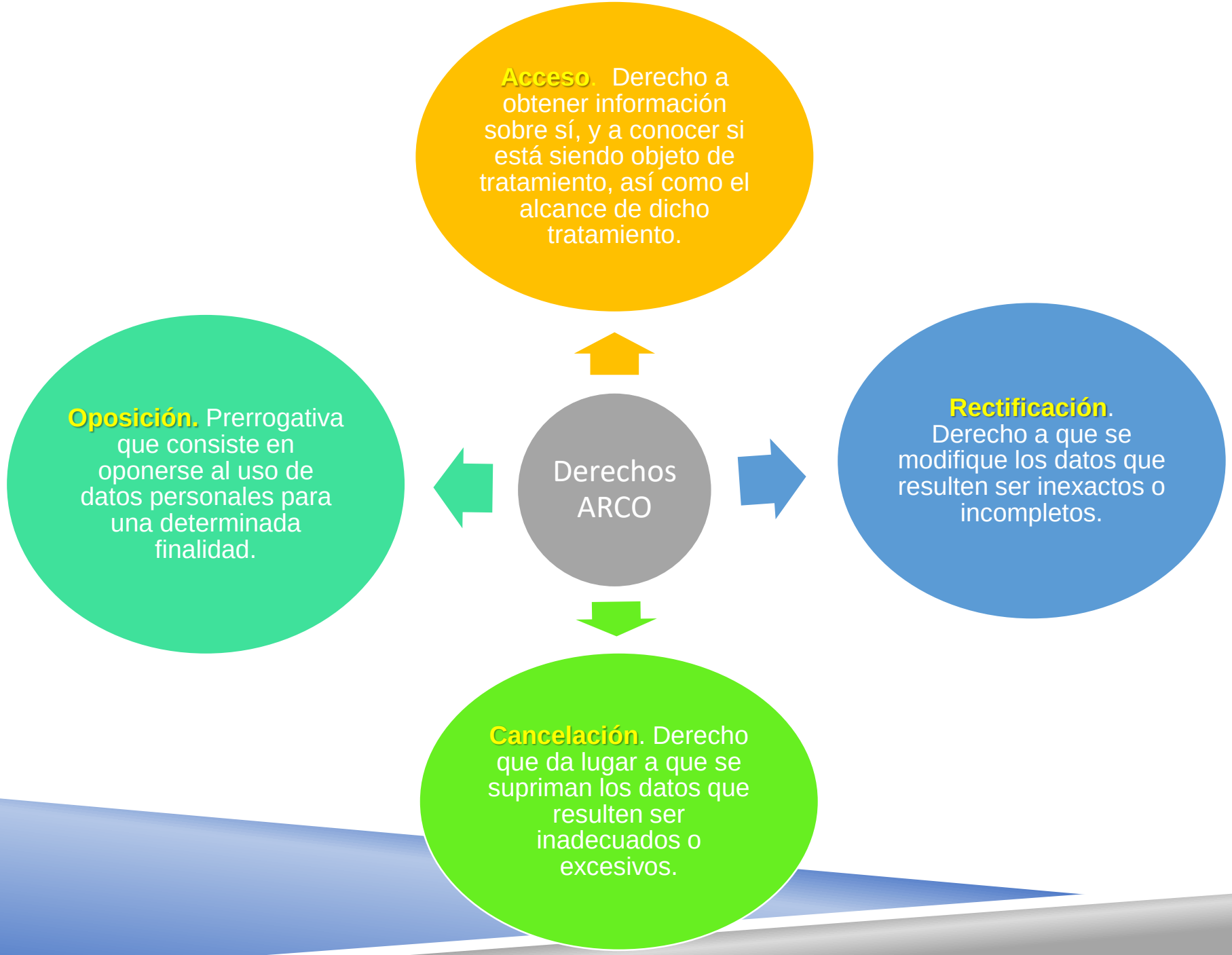
Terceros certificadores

Agentes autorizados para certificar a los responsables que cumplan con la LFPDPPP y los parámetros de autorregulación que deben:

- Ser imparciales.
- Realizar comprobación del debido cumplimiento.
- Contar con facultades de sancionar.

Del ejercicio de los derechos de Acceso, Rectificación, Cancelación y Oposición

Los titulares de los datos personales, o en su caso, un representante legal, pueden ejercer cualquiera de los derechos ARCO ante las empresas que los tengan en sus bases de datos.


Acceso. Derecho a obtener información sobre sí, y a conocer si está siendo objeto de tratamiento, así como el alcance de dicho tratamiento.
Oposición. Prerrogativa que consiste en oponerse al uso de datos personales para una determinada finalidad.
Derechos ARCO
Rectificación. Derecho a que se modifique los datos que resulten ser inexactos o incompletos.
Cancelación. Derecho que da lugar a que se supriman los datos que resulten ser inadecuados o excesivos.

¿Cómo ejercer los derechos ARCO?

De conformidad con lo dispuesto en el artículo 29 de la LFPDPPP, la solicitud de acceso, rectificación, cancelación u oposición deberá contener y acompañar lo siguiente:

[redacted]

Plazos para ejercer derechos ARCO

Una vez presentada la solicitud, la empresa que posea tus datos

Tendrá un plazo máximo de 20 días hábiles para responder

Y 15 días hábiles más para hacer efectivo el derecho que solicites

En caso de que resulten procedentes

Los plazos podrán ser ampliados por una sola vez y por un periodo igual cuando existan hechos que lo justifiquen.

Artículo 35 de la LFPDPPP

El ejercicio de los derechos **ARCO** es **gratuito** y únicamente deberá cubrir el costo por reproducción en copias u otros formatos.

En caso de que volvieras a ejercer cualquiera de los derechos en un plazo menor a **doce meses**, el costo no podrá exceder del equivalente a **tres días** de salario mínimo vigente en el Distrito Federal.

Si se realizaran modificaciones sustanciales al **Aviso de Privacidad** y surgen situaciones que ameriten nuevamente el ejercicio de un mismo derecho en menos de **12 meses**, no habrá costo.

En que casos una empresa PUEDE negar total o parcialmente el tratamiento de los mismos los derechos ARCO

- Cuando el solicitante no sea el titular de los datos personales, o el representante no esté debidamente acreditado.
- Cuando la persona física o empresa no tenga en su posesión los datos personales.
- Cuando se lesionen datos personales de un tercero.
- Cuando exista algún impedimento legal o resolución de autoridad competente que restrinja el ejercicio de alguno de los derechos ARCO.
- Cuando la rectificación, cancelación y oposición solicitada haya sido previamente realizada.

La empresa deberá comunicar y justificar cuando se actualice alguno de los anteriores supuestos y no pueda llevar a cabo la acción que le fue solicitada.

QUE hacer EN caso de que se mal utilicen LOS datos

- Si te enteras que una empresa está haciendo mal uso de tus datos personales, puedes ejercer tu derecho de oposición, a fin de que los datos no sean utilizados. La excepción a esta disposición opera cuando:
- El titular de los datos personales sea parte firmante de un contrato y el tratamiento de sus datos personales sea necesario para el cumplimiento de dicho contrato
- Exista una disposición legal que prevea su tratamiento
- La cancelación obstaculice actuaciones judiciales o administrativas vinculadas con obligaciones fiscales o la investigación y persecución de delitos
- Su tratamiento sea necesario para realizar una acción de interés público
- Su tratamiento sea necesario para cumplir con una obligación que el titular de los datos haya adquirido
- Los datos sean objeto de tratamiento para la prevención o diagnóstico médico o la gestión de servicios de salud -siempre que dicho tratamiento se realice por un profesional de la salud sujeto a un deber de secreto

Procedimiento ante el INAI

El titular puede presentar una solicitud de **protección de datos** ante el **IFAI**, ya sea por escrito o por medios electrónicos, durante los **15 días hábiles** siguientes a la fecha en que la empresa haya comunicado su respuesta; o bien, a partir de que haya vencido el plazo de respuesta, sin que ésta hubiera sido generada.

El Instituto tiene máximo para emitir la resolución **50 días hábiles**, contados a partir de la presentación de la solicitud de **protección de datos**. Si existe causa justificada, el plazo podrá ampliarse por una vez y por un periodo igual.

En caso de que la resolución que emita el Instituto sea favorable al titular, el **IFAI** notificará a la empresa que tiene los datos; ésta tendrá un plazo de **10 días hábiles** para hacer efectivos los derechos.

Si el titular no está conforme con la resolución que emita el Instituto, podrá promover un juicio de nulidad ante el **Tribunal Federal de Justicia Fiscal y Administrativa** contra la resolución, o interponer un Juicio de Amparo.

El Instituto, en su carácter de autoridad garante, tiene la facultad de imponer sanciones a aquellas empresas que incumplan alguna disposición de la Ley. A continuación se mencionan algunas de las posibles sanciones:

I. Apercibimiento

II. Multa de 100 a 160,000 días de salario mínimo vigente en el D.F., cuando la empresa actúe con negligencia o dolo con respecto a la información personal, no observe los principios de protección de datos establecidos en la Ley u omita datos en el Aviso de Privacidad

III. Multa de 200 a 320,000 días de salario mínimo general vigente en el D.F., cuando incumpla con su deber de confidencialidad en el tratamiento de los datos, cambie la finalidad del tratamiento de los mismo sin darte aviso, transfiriera tu datos a terceros sin el consentimiento del titular, obstruya los actos de verificación del Instituto o realice un uso ilegítimo de los datos

IV. En caso de que persistan las infracciones de manera reiterada, el Instituto podrá imponer una multa adicional que irá de 100 a 320,000 días de salario mínimo vigente en el Distrito Federal.
Tratándose de infracciones cometidas en el tratamiento de datos sensibles, los montos de las sanciones podrán incrementarse hasta por dos veces.

De las infracciones y Sanciones Artículo 63 y 64 de la LFPDPPP

Delitos en materia de tratamiento de datos personales.

Artículos 67, 68 y 69 de la LFPDPPP

Fue voluntad del legislador establecer tipos penales para **sancionar** hasta con 5 años de prisión a los responsables que bajo ciertas circunstancias hagan un uso ilícito de la información personal que tratan.

Tratándose de datos personales sensibles, las penas se duplicarán.

Tratamiento y protección de datos personales en el sector público de la salud

¿Qué es un expediente clínico?

- **El conjunto de información ordenada y detallada que recopila cronológicamente todos los aspectos relativos a la salud de un paciente y a la de su familia en un periodo determinado de su vida; representa una base para conocer las condiciones de salud, los actos médicos y los diferentes procedimientos ejecutados por el equipo médico a lo largo de un proceso asistencial.**

¿Qué es un expediente clínico?

- **El conjunto único de información y datos personales de un paciente, que se integra dentro de todo tipo de establecimiento para la atención médica, ya sea público, social o privado, el cual, consta de documentos escritos, gráficos, imagenológicos, electrónicos, magnéticos, electromagnéticos, ópticos, magneto-ópticos y de cualquier otra índole, en los cuales, el personal de salud deberá hacer los registros, anotaciones, en su caso, constancias y certificaciones correspondientes a su intervención en la atención médica del paciente, con apego a las disposiciones jurídicas aplicables**

¿Qué es un expediente clínico?

- **El expediente clínico constituye el documento base que proporciona al médico los elementos necesarios para realizar un diagnóstico y tratamiento; aunque también puede ser útil como documento legal en el que se evidencia el proceso de actuación del profesional de la salud y como prueba documental ante un reclamo por parte del paciente en cuanto al proceso de atención recibida por el médico.**

Contenido del expediente clínico

Descripción del individuo: nombre, sexo, edad y domicilio del paciente y los demás que señalen las disposiciones sanitarias.

Antecedentes remotos y próximos: grupo étnico, antecedentes heredo-familiares, antecedentes personales patológicos (incluido uso y dependencia del tabaco, del alcohol y de otras sustancias psicoactivas, de conformidad con lo establecido en la NOM-028-SSA2-2009, para la prevención, tratamiento y control de las adicciones) y no patológicos.

Padecimiento actual: indagar acerca de tratamientos previos de tipo convencional, alternativos y tradicionales.

Evolución de la enfermedad: Evolución y actualización del cuadro clínico.

Inspección del cadáver: Causas de la muerte acorde a la información contenida en el certificado de defunción y, en su caso, si se solicitó y se llevó a cabo estudio de necropsia hospitalaria.

Régimen de principios, excepciones, deberes y derechos que rigen el tratamiento de los datos personales contenidos en el expediente clínico

- **El ejercicio de los derechos de acceso y protección de los datos personales en el sector público de la salud en México, está íntimamente relacionado con el documento toral de la atención médica, esto es, el expediente clínico.**

- **Independientemente del tipo de soporte en que se contenga la información del paciente, ya sea impreso, audiovisual o electrónico, su tratamiento por parte del responsable deberá apegarse a las disposiciones y principios establecidos en la legislación de la materia.**

Los artículos 16 al 30 de la LGPDPPSO, 6 a 21 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP), así como 7 al 26 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público (LGPDPSP), establecen los ocho principios rectores que deberán observar los responsables en el tratamiento de los datos personales:

1.Calidad: Adoptar las medidas necesarias para mantener exactos, completos, correctos y actualizados los datos personales en su posesión, a fin de que no se altere su veracidad.
2.Consentimiento: Contar con la autorización del titular para el tratamiento de sus datos personales, salvo los casos de excepción previstos en la ley. El consentimiento deberá ser libre, específico e informado.
3.Finalidad: Limitar el tratamiento de datos personales a las finalidades concretas, lícitas, explícitas y legítimas informadas en el aviso de privacidad.
4.Información: Informar al titular, a través del aviso de privacidad, la existencia y características principales del tratamiento al que serán sometidos sus datos personales, a fin de que pueda tomar decisiones informadas al respecto.
5.Lealtad: El responsable no deberá obtener y tratar datos personales a través de medios engañosos o fraudulentos y ha de privilegiar la protección de los intereses del titular y la expectativa razonable de privacidad.
6.Licitud: El tratamiento de datos personales por parte del responsable deberá sujetarse a las facultades o atribuciones que la normatividad aplicable y vigente le confiera.
7.Proporcionalidad: Tratar únicamente los datos personales que resulten adecuados, relevantes y estrictamente necesarios para la finalidad que justifica su tratamiento.
8.Responsabilidad: Implementar los mecanismos necesarios para acreditar el cumplimiento de los principios, deberes y obligaciones establecidos en la legislación en la materia y rendir cuentas sobre el tratamiento de datos personales en su posesión al titular y a los organismos garantes.

Con relación al principio de consentimiento es importante mencionar que tratándose de datos personales sensibles, el responsable deberá obtener el consentimiento expreso y por escrito del titular para su tratamiento, a través de su firma autógrafa, firma electrónica o cualquier mecanismo de autenticación que al efecto se establezca (artículo 21, párrafo cuarto de la LGPDPPSO), salvo en los casos de excepción previstos en la Ley.

Los artículos 22 de la LGPDPPSO y 10 de la LFPDPPP, prevén los supuestos de excepción en los que el responsable no estará obligado a recabar el consentimiento del titular para efectuar el tratamiento de sus datos personales, estableciendo que cuando los datos sean indispensables para la atención médica, la prevención, diagnóstico, la prestación de asistencia sanitaria, tratamientos médicos o la gestión de servicios sanitarios, no será necesario otorgar el consentimiento mientras el titular no esté en condiciones de hacerlo, y siempre que el tratamiento de datos se realice por una persona sujeta al secreto profesional u obligación equivalente.

Con relación a los deberes en materia de PDP, tanto la LGPDPPSO como la LFPDPPP establecen en esencia las obligaciones para el responsable respecto de adoptar las medidas necesarias para mantener exactos, completos, correctos y actualizados los datos personales en su posesión, a fin de que no se altere su veracidad, así como las medidas de seguridad que permitan proteger los datos personales contra daño, pérdida, alteración o destrucción; uso, acceso o tratamiento no autorizados; así como aquellas que garanticen su confidencialidad, integridad y disponibilidad.

Al respecto, disponen tres tipos de medidas de seguridad que el responsable deberá observar, para garantizar la adecuada protección de los datos personales:

Administrativas: Comprenden las políticas y procedimientos para la gestión, soporte y revisión de la seguridad de la información a nivel organizacional, la identificación, clasificación y borrado seguro de la información, así como la sensibilización, formación y capacitación del personal, en materia de protección de los datos personales.

Físicas: Se refieren al conjunto de acciones y mecanismos para proteger el entorno físico de los datos personales y de los recursos involucrados en su tratamiento.

Técnicas: Se trata del conjunto de acciones y mecanismos que se valen de la tecnología relacionada con hardware y software para proteger el entorno

Al respecto, disponen tres tipos de medidas de seguridad que el responsable deberá observar, para garantizar la adecuada protección de los datos personales:

Administrativas: Comprenden las políticas y procedimientos para la gestión, soporte y revisión de la seguridad de la información a nivel organizacional, la identificación, clasificación y borrado seguro de la información, así como la sensibilización, formación y capacitación del personal, en materia de protección de los datos personales.

Físicas: Se refieren al conjunto de acciones y mecanismos para proteger el entorno físico de los datos personales y de los recursos involucrados en su tratamiento.

Técnicas: Se trata del conjunto de acciones y mecanismos que se valen de la tecnología relacionada con hardware y software para proteger el entorno

Ante un escenario de vulneración, el responsable está obligado a hacerles saber tal situación sin dilación alguna al titular, al igual que al organismo garante, a fin de que puedan tomar las medidas correspondientes para la defensa de sus derechos.

El responsable deberá informar: la naturaleza del incidente; los datos personales comprometidos; las recomendaciones al titular acerca de las medidas que éste pueda adoptar para proteger sus intereses; las acciones correctivas realizadas de forma inmediata; y los medios donde puede obtener más información al respecto.