

Marco constitucional

Artículo 6º constitucional



Primer párrafo

- Libre manifestación de las ideas.
- Derecho de réplica.
- Derecho a la información.

Segundo párrafo

- Derecho al libre acceso a la información plural y oportuna.
- Derecho a buscar, recibir y difundir información de ideas.

Tercer párrafo

- Derecho de acceso a las tecnologías de la información y comunicación.
- Derecho a los servicios de radiodifusión y telecomunicaciones, incluido el de banda ancha e internet.

Artículo 6º constitucional

Apartado A, fracción I

- Publicidad de la información en posesión de cualquier autoridad, órgano, organismo, partidos políticos, personas físicas que ejerzan recursos públicos, etc.
- Reserva de información por razones de interés público y seguridad nacional.
- Principio de máxima publicidad.
- Obligación de los sujetos obligados para documentar todo acto que derive de sus facultades, competencias o funciones.
- Declaración de inexistencia de la información.

Apartado A, fracción II

- Protección de la información sobre la vida privada y los datos personales.

Apartado A, fracción III

- Derecho de acceso a información pública, datos personales y rectificación de ellos.

Apartado A, fracción IV

- Establecimiento de mecanismos de acceso a la información y procedimientos de revisión ante organismos autónomos especializados.

Artículo 6º constitucional

Apartado A, fracción V

- Obligación de los sujetos obligados para preservar sus documentos en archivos administrativos.
- Obligación de los sujetos obligados de publicar la información completa y actualizada del ejercicio de recursos e indicadores.

Apartado A, fracción VI

- Remisión a la ley para que ésta señale la forma en la que se publicará la información acerca de los recursos públicos que se entreguen a personas físicas o morales.

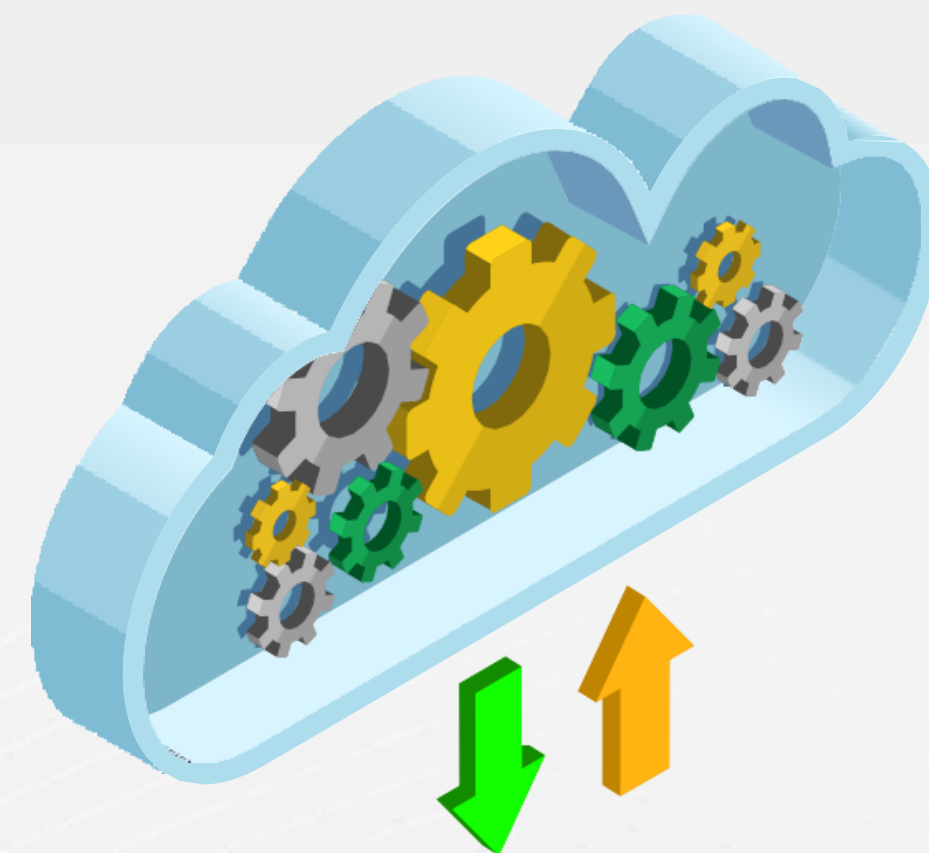
Apartado A, fracción VII

- Establece sanción en caso de incumplimiento a las disposiciones en materia de acceso a la información.

Apartado A, fracción VIII

- Fundamento del INAI, como organismo autónomo, especializado, imparcial, colegiado, con personalidad jurídica y patrimonio propio.

EVOLUCIÓN CONSTITUCIONAL DE LA PROTECCIÓN DE DATOS EN MÉXICO



INTERNACIONAL



Año	Instrumento	Artículo
1948	Declaración Universal de Derechos Humanos	Art. 12. “Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques.”
1948	Declaración Americana de los Derechos y Deberes del Hombre	Art. 5. “Toda persona tiene derecho a la protección de la Ley contra los ataques abusivos a su honra, a su reputación y a su vida privada y familiar.”
1950	Convenio para la Protección de los Derechos y las Libertades Fundamentales	Art. 8. “Derecho al respeto a la vida privada y familiar. 1 Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia. 2. No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho, sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública el bienestar económico del país, la defensa del orden y la prevención del delito, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás.”
1966	Pacto Internacional de los Derechos Civiles y Políticos	Art. 12. “Nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación. 2. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques.”
1969	Convención Americana sobre Derechos Humanos (Pacto de San José)	Art. 11, apartado 2. “Nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación.”
1981	Convenio para la Protección de las Personas con Respecto al Tratamiento Automatizado de Datos de Carácter Personal (Convenio 108)	Primer documento internacional de protección de datos personales. incorporaba el principio de no discriminación, la facultad de establecer excepciones, un control de sanciones y el flujo de datos a través de las fronteras, entre otros
2001	Protocolo adicional al Convenio para la Protección de las Personas con Respecto al Tratamiento Automatizado de Datos de Carácter Personal (Convenio 108 +)	
2007	Carta de Derechos Fundamentales de la Unión Europea	1. Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan. 2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a obtener su rectificación. 3. El respeto de estas normas estará sujeto al control de una autoridad independiente.

Evolución del Derecho de Protección de Datos Personales en la Ciudad de México

2002

Ley Federal de
Transparencia
Acceso a la
Información Pública
Gubernamental.

Capítulo IV Datos
personales

2007

Reforma el Art.
6º Constitucional
Frac. II y III.

2009

• Reforma al Art. 16
Constitucional

2014

Reforma
constitucion
al artículo
6to,
apartado A.,
F. II y III



Marco constitucional

Artículo 16° constitucional

Derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley.

Artículo 73 fracción XXIX-O

Congreso ▼

Legislar en materia de protección de datos personales en posesión de particulares.

Antecedentes de la PDP

4 ETAPAS

- Reforma al artículo 6° CPEUM.
- Reforma al artículo 73 fracción XXIX-O CPEUM.
- Reforma al artículo 16 CPEUM
- Reforma al artículo 6°

MARCO CONSTITUCIONAL EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES

Artículo 20, apartado C, fracción V, primer párrafo (Derechos de la víctima o del ofendido):

- “Al resguardo de su identidad y otros datos personales en los siguientes casos: cuando sean menores de edad; cuando se trate de delitos de violación, trata de personas, secuestro o delincuencia organizada; y cuando a juicio del juzgador sea necesario para su protección, salvaguardando en todo caso los derechos de la defensa.”

Artículo 73, fracción XXIX-O y XXIX-S, respectivamente (Facultades del Congreso):

- “Para legislar en materia de protección de datos personales en posesión de particulares.” (Reforma 2009)
- “Para expedir las leyes generales reglamentarias que desarrollen los principios y bases en materia de transparencia gubernamental, acceso a la información y protección de datos personales en posesión de las autoridades, entidades, órganos y organismos gubernamentales de todos los niveles de gobierno.” (Reforma 2014)

105, fracción II, inciso h (Sujetos facultados para interponer acciones de inconstitucionalidad)

- “El organismo garante que establece el artículo 6° de esta Constitución en contra de leyes de carácter federal y local, así como de tratados internacionales celebrados por el Ejecutivo Federal y aprobados por el Senado de la República, que vulneren el derecho al acceso a la información pública y la protección de datos personales. Asimismo, los organismos garantes equivalentes en las entidades federativas, en contra de leyes expedidas por las Legislaturas locales”.

116, fracción VIII:

- “Las Constituciones de los Estados establecerán organismos autónomos, especializados, imparciales y colegiados, responsables de garantizar el derecho de acceso a la información y de protección de datos personales en posesión de los sujetos obligados, conforme a los principios y bases establecidos por el artículo 6o. de esta Constitución y la ley general que emita el Congreso de la Unión para establecer las bases, principios generales y procedimientos del ejercicio de este derecho.”

FACEBOOK Y CAMBRIDGE ANALYTICA



La consultora *Cambridge Analytica*, fundada en 2013, fue acusada de haber obtenido información de millones de usuarios de Facebook sin permiso, violando las políticas de uso de la red social.

Con esos datos habría generado anuncios políticos dirigidos para favorecer la campaña presidencial de Donald Trump así como para el *Brexit* del Reino Unido.

Los periódicos *The New York Times* y *The Guardian* publicaron notas sobre el uso de datos de los perfiles en la red social de para generar anuncios políticos, argumentando que con ellos se buscaba *manipular las decisiones de los votantes*.

Lo anterior, mediante el uso de la aplicación *This is your digital life* que funcionaba como un test online, y que se presentaba como una herramienta de investigación para los usuarios, en la que se les ofrecía entre 2 y 5 dólares por responder un cuestionario sobre personalidad e intereses políticos, finalmente, se les solicitaba iniciar sesión en Facebook y otorgarle permisos a la *app*, como acceder a su información y actividad de usuario, su ubicación y contactos en la red.

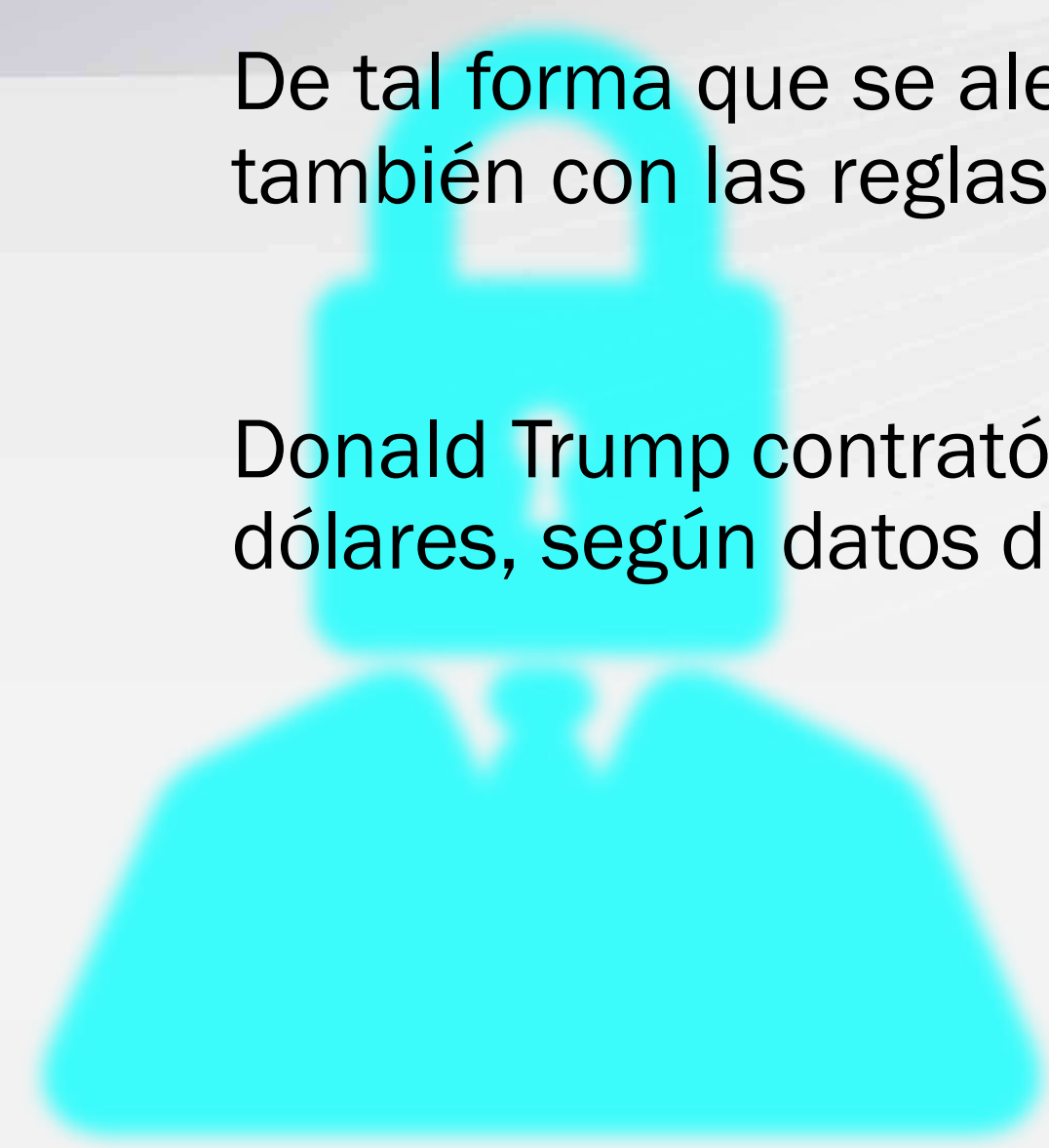
Así, la aplicación era descargada e instalada de manera voluntaria por las y los usuarios.

Alrededor de 270 mil personas que hicieron esta encuesta online, lo cual derivó en la recopilación de información de 50 millones de perfiles, toda vez que dicha aplicación solicitaba el acceso a los datos de perfiles asociados (amigos).

Esta información fue enviada a *Cambridge Analytica* sin el permiso expreso de los usuarios, ya que estos, al hacer el test, aceptaban que su información se recopilara solo para fines académicos y no con otro propósito. Máxime que también se envió la información recopilada de perfiles amigos.

De tal forma que se alegó falta de transparencia en el uso de datos sin permiso, incumpliendo también con las reglas de uso de Facebook.

Donald Trump contrató los servicios de *Cambridge Analytica* en 2016 por más de 6,2 millones de dólares, según datos de la Comisión Electoral Federal







AMAZON

En abril de 2016 la Dirección Ejecutiva del Registro Federal de Electores del INE (DERFE), tuvo conocimiento de la divulgación del listado nominal de electores en la página de internet de *Amazon*, mediante diversos correos electrónicos recibidos por el Consejero Presidente del INE y personal de la DERFE.

Esta información correspondía a la *Lista Nominal de Electores para Revisión, entregada a los Partidos Políticos en el marco del Proceso Electoral Federal 2014- 2015 y de los Procesos Electorales Coincidentes 2015* entregada al Representante propietario del Partido Movimiento Ciudadano, en dispositivos de almacenamiento USB, con su respectivo cifrado de seguridad.

La información estuvo disponible en internet de manera libre, por lo menos en el periodo del 18 de abril de 2016, al 20 de abril del mismo año

La DERFE realizó una *la verificación de correspondencia* entre de la información del sitio reportado con las marcas de rastreabilidad contenidas en el disco de ADN entregado al Partido Movimiento Ciudadano, para corroborar que fueran coincidentes.

El Partido MC aprobó la contratación de un servidor virtual en Internet con *Amazon Web Services*, única y *exclusivamente* para salvaguardar la información del Listado Nominal de Electores ejercer sus facultades legales de revisión.

INDATCOM, S.A. de C.V., en su calidad de proveedor de servicios tecnológicos del Partido MC, habilitó un sitio web con el propósito exclusivo de que en este espacio digital, fuese alojada y resguardada la base de datos con información confidencial, que la DERFE proporcionó al partido denunciado, en el marco del Proceso Electoral Federal 2014-2015.

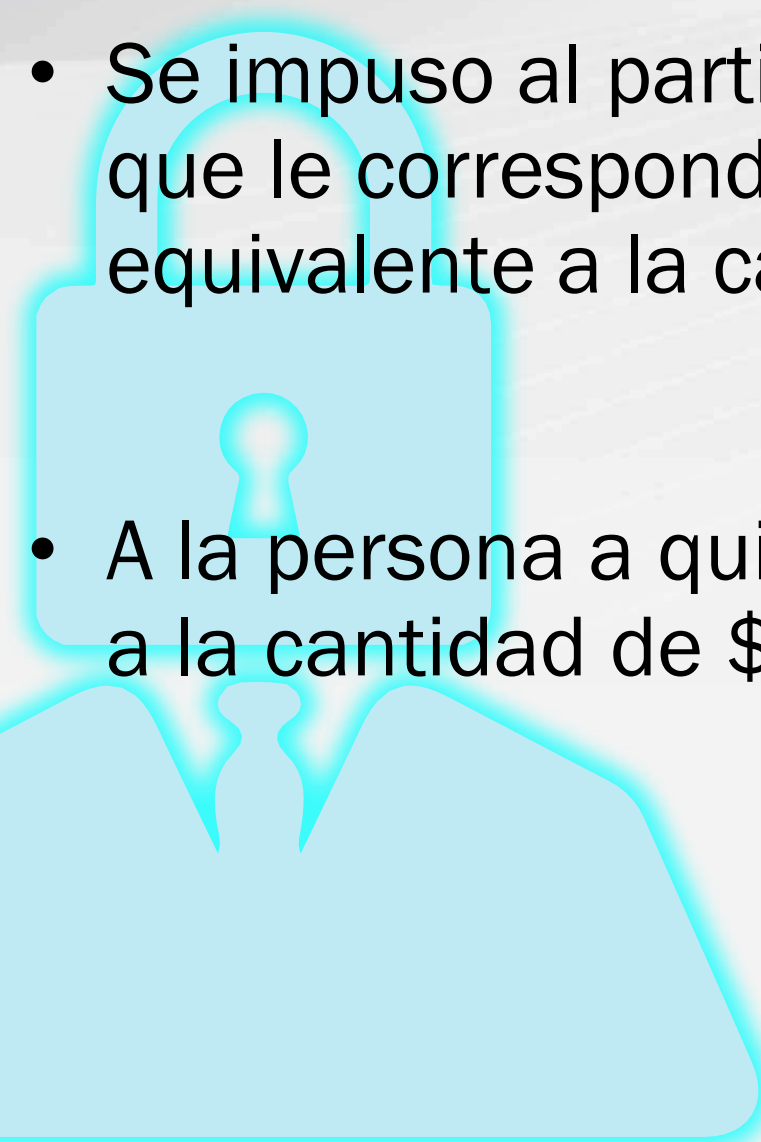
El personal de la DERFE accedió al servidor de *AMAZON* para la obtención de muestras de la información localizada, de tal forma que era accesible sin tener que violar o romper candados o medidas de seguridad.

Se determinó que el partido denunciado no tomó medidas de seguridad eficaces y eficientes para salvaguardar la información confidencial de más de 93 millones de ciudadanos, cuya exposición sí se demostró de forma total.

Asimismo, se acreditó responsabilidad de la persona designada por el Partido MC para tener acceso a la lista de electores, como el único sujeto al que se le entregó dicha información, mismo que alojó la información en un servidor en Internet; no eliminó la base de datos que conformaba el instrumento electoral, después de utilizarla; que indebidamente conservó de forma premeditada esa información por, al menos un año un mes más, y; que permitió, como consecuencia de no tomar las medidas de seguridad necesarias que garantizaran su seguridad, que la información estuviera expuesta de forma global, al haberse encontrado la información en un sitio de publicidad y exposición mundial.

En ese tenor, se impusieron como sanciones:

- Se impuso al partido la reducción del 10% de la ministración anual del financiamiento público que le correspondía para el sostenimiento de sus actividades ordinarias permanentes, por el equivalente a la cantidad de \$34,158,411.30, descontada en seis mensualidades, y
- A la persona a quien le fue entregada la lista nominal, dos multas de 308 UMAS, equivalentes a la cantidad de \$22,496., cada una, pagadas en seis exhibiciones mensuales



CONCEPTOS Y DEFINICIONES BÁSICAS



Intimidad^[1]

Lo «**íntimo**» podría pensarse como el ámbito tanto de los pensamientos de cada cual, de la formación de decisiones («lo aún no expresado y que probablemente nunca lo será»), como de aquellas acciones cuya realización no requiere la intervención de terceros y tampoco los afecta.



Privacidad^[1]

En el ámbito de lo «**privado**» se requiere necesariamente, a diferencia de lo íntimo, la presencia de por lo menos dos actores.

Se trata del ámbito donde pueden imperar exclusivamente los deseos y preferencias individuales, como condición necesaria para el «ejercicio» de la libertad individual, conformando así la «esfera personal reconocida».

Derecho a la privacidad ^[2]

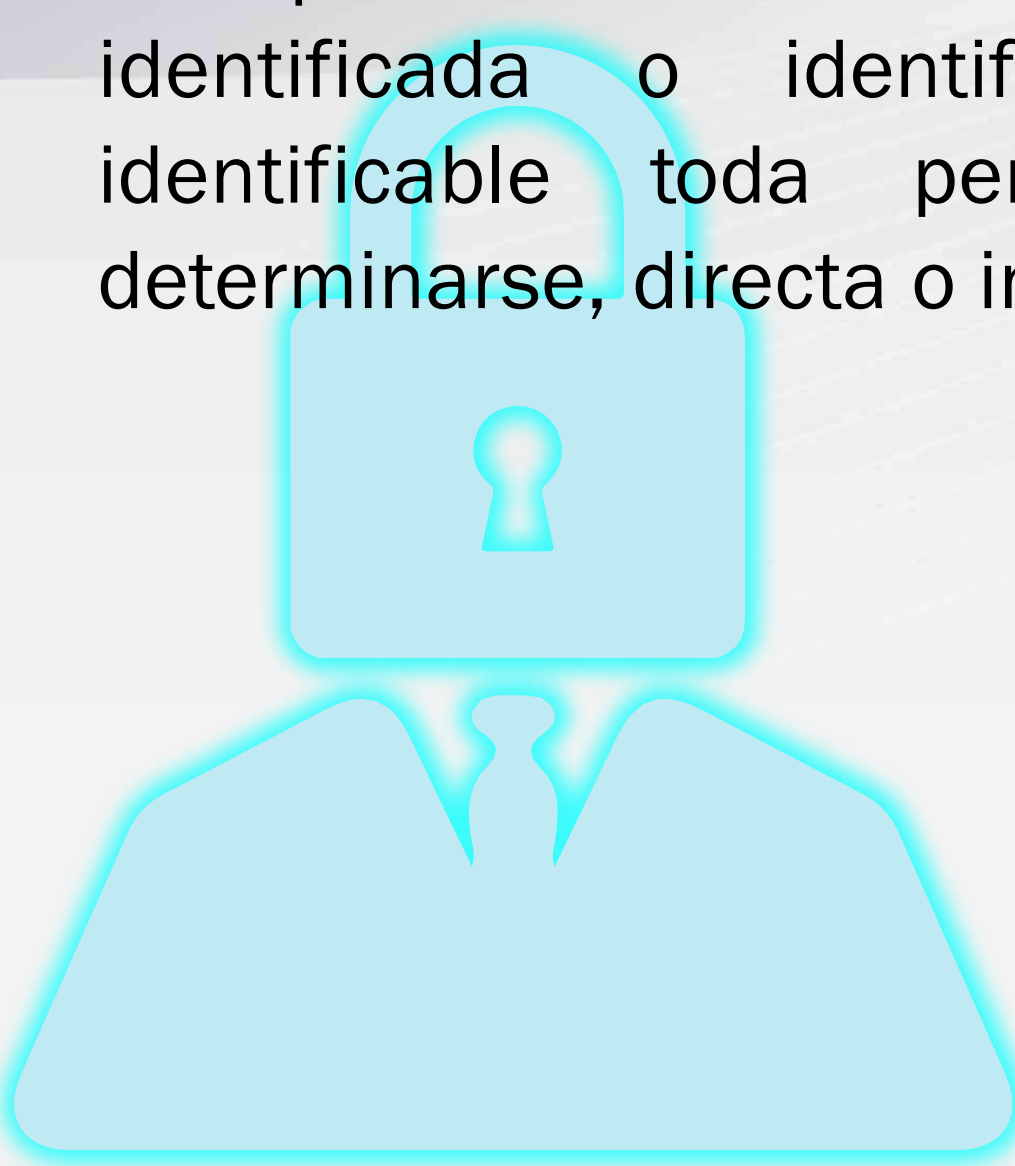
El derecho a la privacidad es aquél que todo individuo tiene a **separar** aspectos de su vida privada del escrutinio público.

^[1] Garzón Valdés, Ernesto, Lo íntimo, lo privado y lo público, Cuadernos de Transparencia # 6, INAI, 2015.

^[2] García Ricci, Diego, Artículo 16 Constitucional. Derecho a la privacidad, IIJ-UNAM, 2013.

DATOS PERSONALES

Cualquier información relativa a una persona **física** identificada o identificable, considerándose **como** identificable toda persona cuya identidad **pueda** determinarse, directa o indirectamente.



Tipos de Datos

DATOS



APELLIDOS
 NOMBRE
 DIRECCIÓN
 TELÉFONO
 POBLACIÓN



Identificativos

Nombre, edad, domicilio, estudios, etc.

Menores de edad

Financieros

Bienes, cuentas bancarias, información fiscal, reporte de buró de crédito, declaraciones de impuestos.

Datos electrónicos

La dirección IP, los correos electrónicos e incluso la geolocalización.

Sensibles

Origen racial, estado de salud, creencias religiosas, opiniones políticas, Preferencia sexual, Datos biométricos.

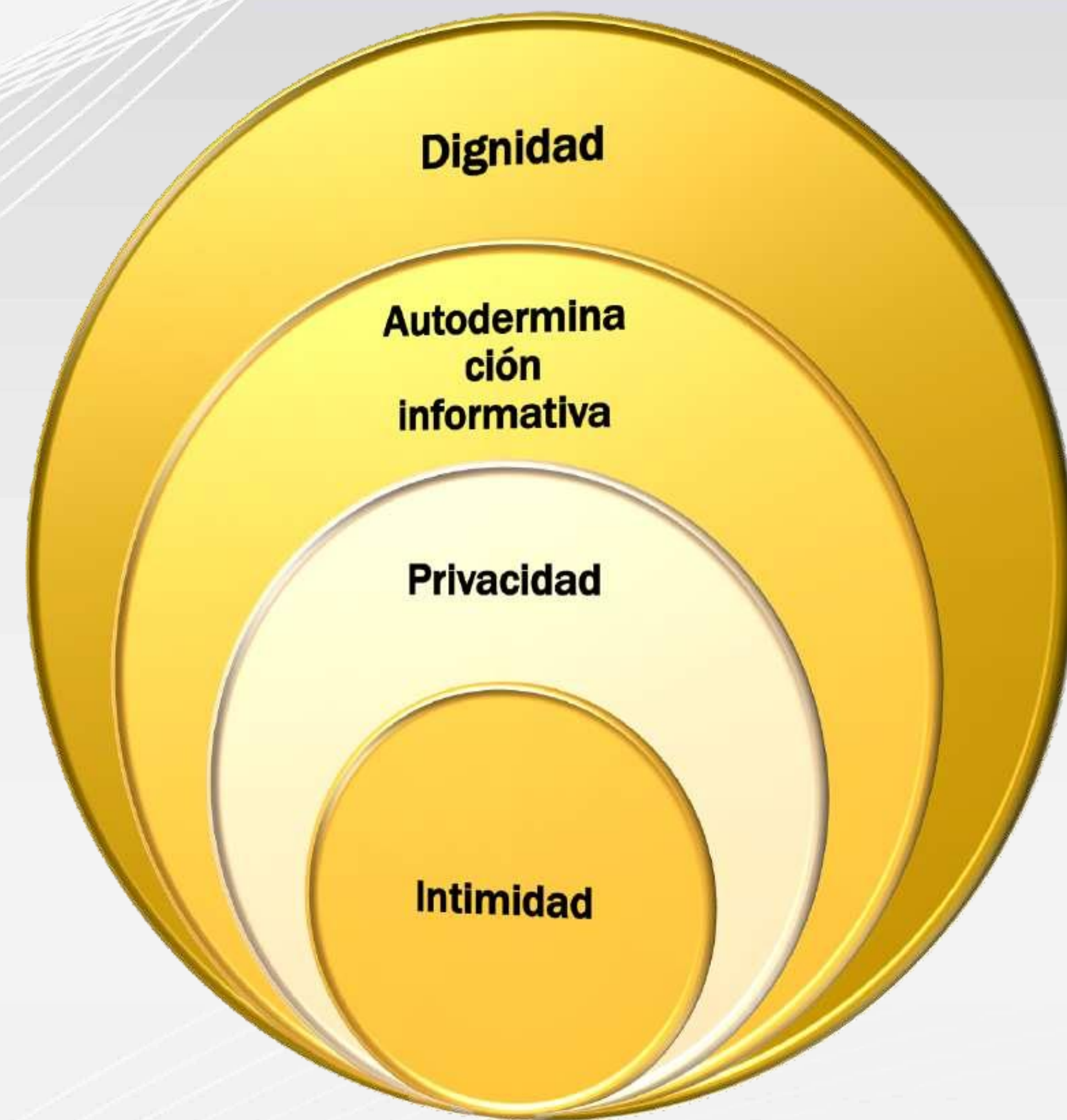
¿POR QUÉ PROTEGER LOS DATOS PERSONALES ?

La **autodeterminación informativa** es el reconocimiento al individuo de la facultad de disposición y decisión respecto a sus propios datos personales. Este derecho, reconoce al sujeto la facultad de decidir cuándo y cómo está dispuesto a permitir que sea difundida su información personal o a difundirla él mismo.

La **Protección de Datos Personales** es una prerrogativa que tiene el titular de los datos para proteger cualquier información concerniente a su persona.

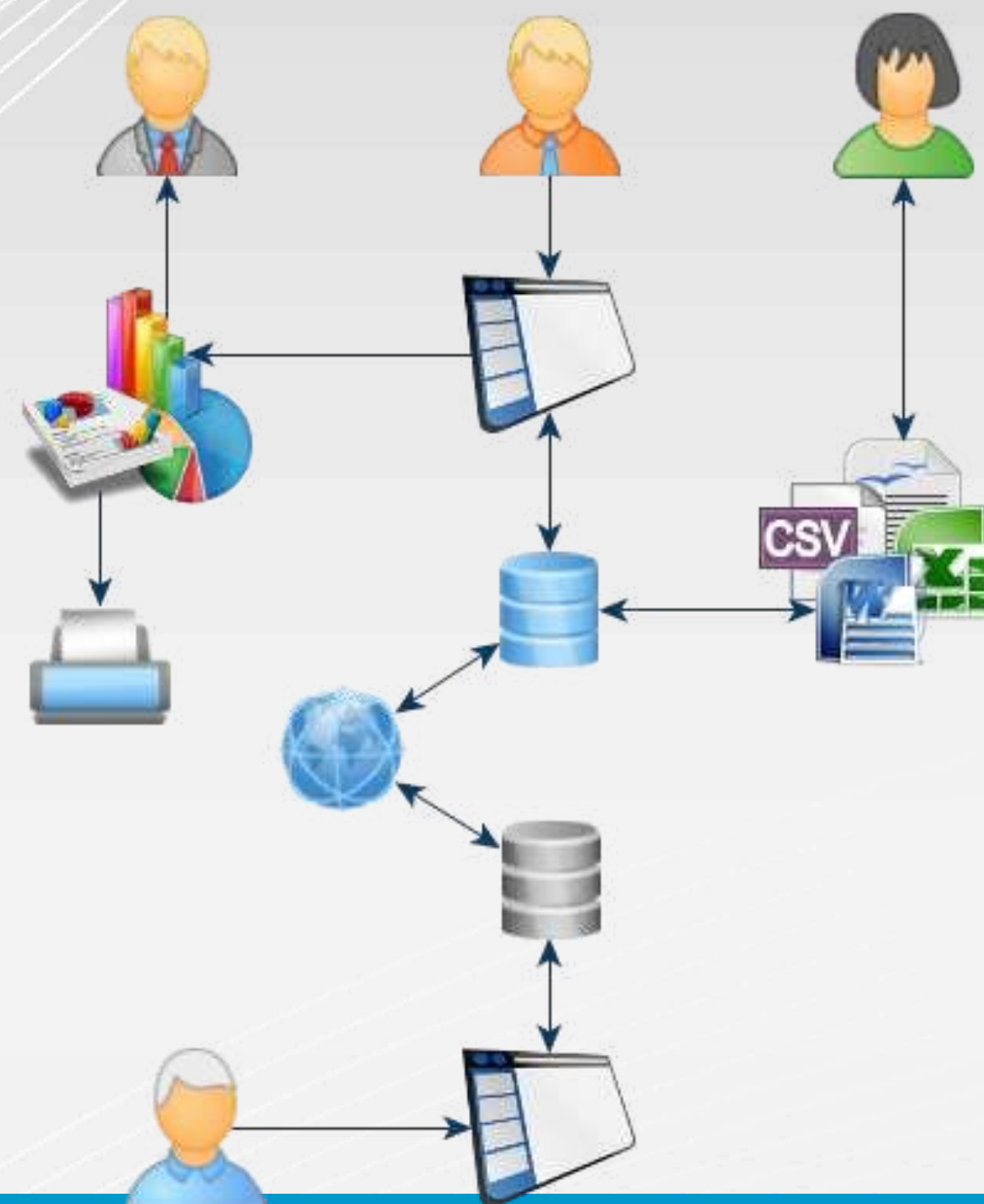


La protección de la intimidad, privacidad y autodeterminación informativa al igual que el derecho a la **protección de datos personales** buscan procurar la dignidad y la personalidad humana.



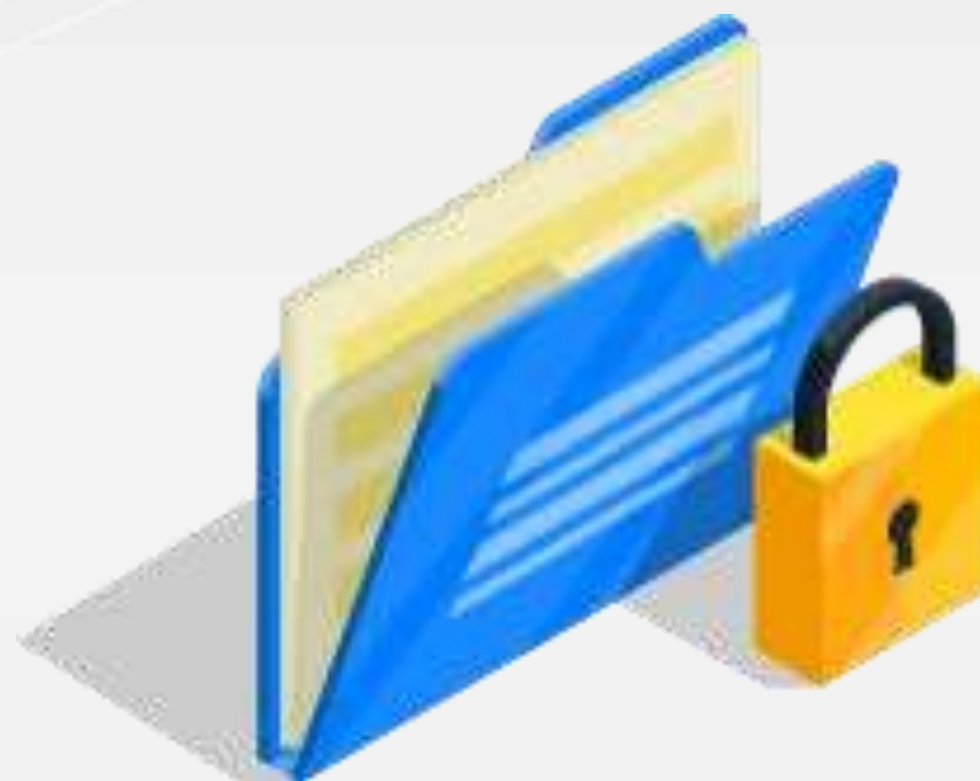
TRATAMIENTO DE DATOS PERSONALES

Cualquier operación o conjunto de operaciones efectuadas mediante procedimientos manuales o automatizados aplicados a los datos personales, relacionadas con la obtención, uso, registro, organización, conservación, elaboración, utilización, comunicación, difusión, etc.



MEDIDAS DE SEGURIDAD

Conjunto de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permitan proteger los datos personales y los sistemas de datos personales.



NIVELES DE SEGURIDAD

Básicas

Medias

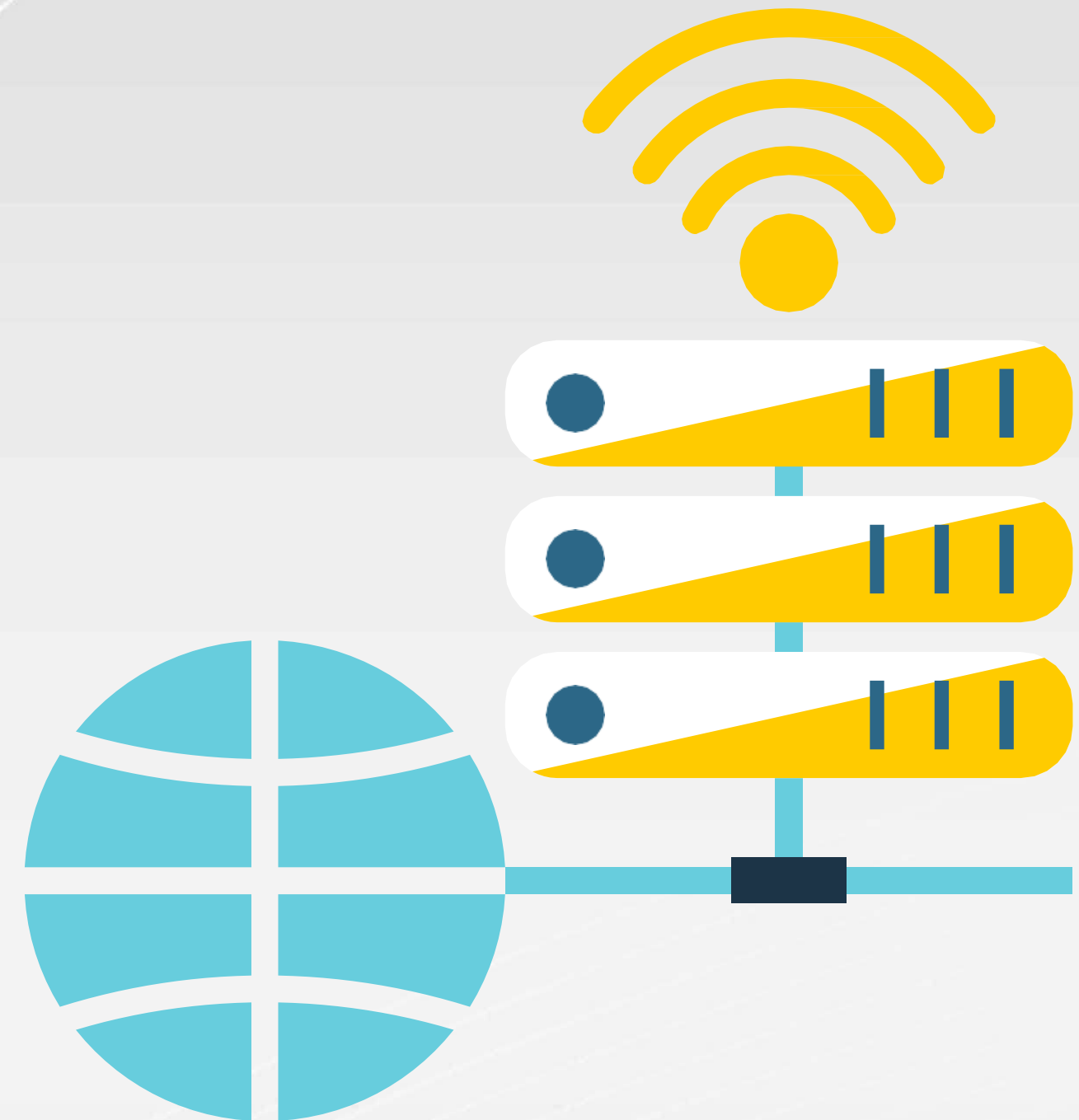
Altas
(datos sensibles)

TITULAR

La persona física a quien
corresponden los
datos personales.

RESPONSABLE

Cualquier sujeto obligado , que decida y determine
finalidad, fines, medios, medidas de seguridad y
demás cuestiones relacionadas con el tratamiento
de datos personales.



USUARIO

Persona autorizada por el responsable e integrante del sujeto obligado, que dé tratamiento y/o tenga acceso a los datos y/o sistema de datos personales.

ENCARGADO

La persona física o jurídica, pública o privada, ajena a la organización del responsable, que sola o conjuntamente con otras trate datos personales a nombre y por cuenta del responsable.



APECTOS RELEVANTES DE LA LEY

PRINCIPIOS Y DEBERES

DERECHOS DE LOS TITULARES Y SU EJERCICIO

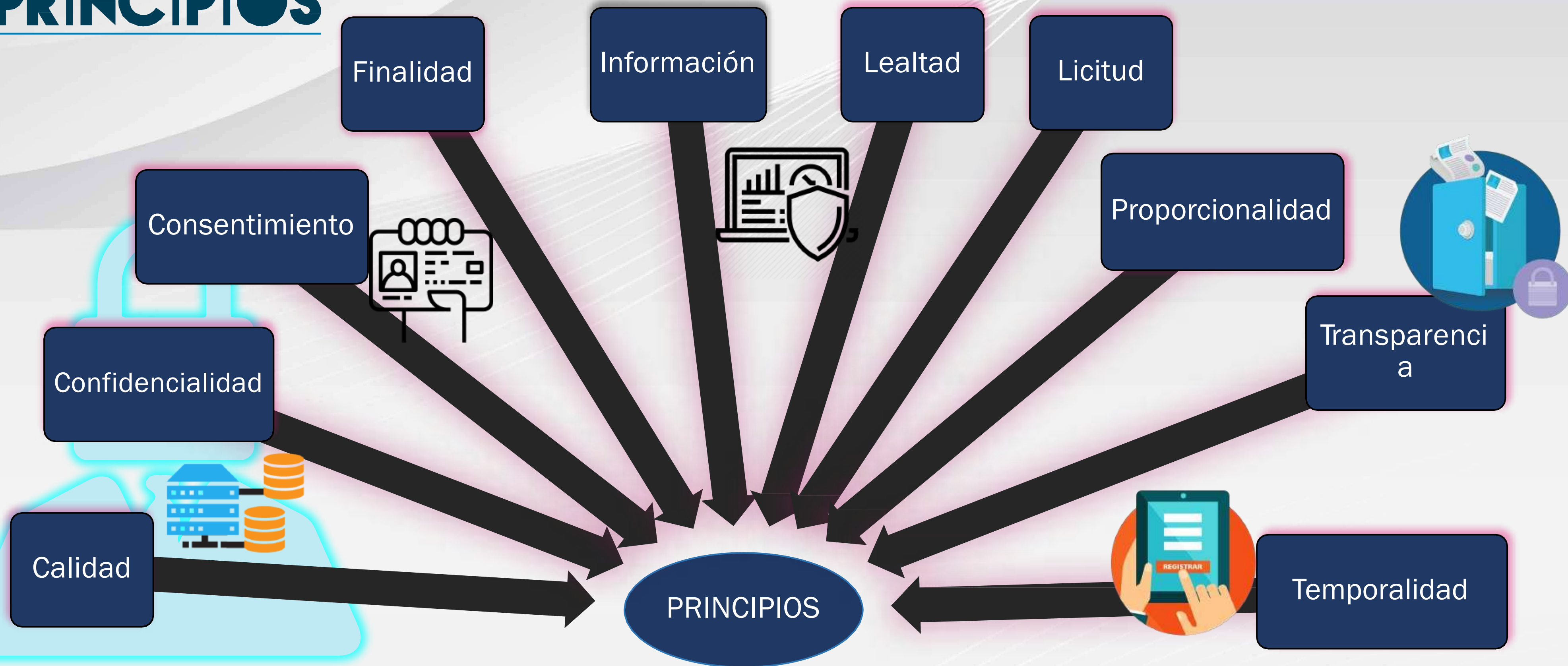
ÓRGANOS EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE SUJETOS OBLIGADOS

LA PROTECCIÓN DE DATOS PERSONALES

MEDIOS DE DEFENSA EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE SUJETOS OBLIGADOS

MEDIDAS DE APREMIO Y RESPONSABILIDADES

PRINCIPIOS



PRINCIPIOS

Calidad

Los DP deben ser ciertos, adecuados, pertinentes y proporcionales, no excesivos, en relación con el ámbito y la finalidad para la que fueron recabados..

Confidencialidad

Solo el titular, el Responsable y el usuario puedan acceder a los DP, para cumplir con las finalidades del tratamiento. Se deberá garantizar la secrecía y la no difusión de los mismos.

Consentimiento

Manifestación de la voluntad libre, específica e informada del titular de los DP para su tratamiento;

Finalidad

Los DP recabados y tratados tendrán fines determinados, explícitos y legítimos y no podrán ser tratados ulteriormente con fines distintos para los que fueron recabados

Información

El Responsable deberá informar al titular de los DP sobre las características principales del tratamiento, la finalidad y cualquier cambio del estado relacionados con sus datos personales.

Lealtad

El tratamiento de DP se realizará sin que medie dolo, engaño o medios fraudulentos, tengan un origen lícito, y no vulneren la confianza del titular.

Licitud

El tratamiento de DP será lícito cuando el titular los entregue, previo consentimiento o en cumplimiento de una obligación y no serán utilizados para otras finalidades.

Proporcionalidad

El Responsable tratará aquellos DP que resulten necesarios, adecuados y relevantes en relación con la finalidad, para la cual se obtuvieron.

Transparencia

La información relacionada con el tratamiento de DP será accesible y fácil de entender y siempre a disposición del titular.

Temporalidad

Los DP tendrán un ciclo de vida vinculado a la finalidad para la cual fueron recabados y tratados. Concluida su finalidad pueden ser destruidos.

DEBERES

El responsable del tratamiento tiene, entre otros, **los siguientes deberes en el tratamiento:**

- Garantizar a las personas, el ejercicio de los derechos de Acceso, Rectificación, Cancelación y Oposición;
- Registrar ante el Instituto los Sistemas de Datos Personales, así como la modificación o supresión de los mismos;
- Informar al titular previo a recabar sus datos personales, la existencia y finalidad de los sistemas de datos personales.

DERECHOS DE LOS TITULARES Y SU EJERCICIO

A

El derecho de Acceso se ejerce por el titular o su representante, para obtener y conocer la información relacionada con el uso, registro, fines, organización y conservación de sus DP

R

El titular tendrá derecho a solicitar por sí o por su representante, la rectificación o corrección de sus DP, cuando resulten inexactos, incompletos, erróneos o no se encuentren actualizados.

C

El titular tendrá derecho a solicitar la cancelación o eliminación de sus DP de los archivos, registros, expedientes y sistemas del responsable, a fin de que ya no estén en su posesión.

O

El titular podrá oponerse al tratamiento de sus DP o exigir que cese el mismo, cuando no se ajuste a las finalidades o a lo dispuesto por la Ley o aún siendo lícito, cause un daño o perjuicio al titular.

MEDIOS PARA PRESENTAR UNA SOLICITUD DE DERECHOS ARCO

¿Cómo puedo ejercer
mis derechos ARCO?



REQUISITOS PARA EL EJERCICIO DE LOS DERECHOS ARCO

I • Nombre del Titular

II • Documentos que acrediten la identidad del Titular

III • De ser posible, área del responsable que trata los DP

IV • Descripción clara y precisa de los DP de los que se busca ejercer alguno de los derechos ARCO

V • Descripción del derecho ARCO que se pretende ejercer



PLAZOS DE RESPUESTA

Para el ejercicio de los derechos ARCO



PLAZOS DE RESPUESTA

Para el ejercicio
de los derechos
ARCO

PLAZO DE
RESPUESTA

SI PROCEDE

Siempre y cuando existan
razones fundadas y
motivadas

AMPLIACIÓN

20 Días
hábles

10 Días
hábles



RECURSO DE REVISIÓN

Es un **medio de defensa** que puede hacer valer quien ejerza alguno de los Derechos ARCO, en contra de las respuestas u omisiones emitidas por los Sujetos Obligados.

El recurso de revisión procederá, entre otras causas, por:

- I. La inexistencia de los datos personales.
- II. La declaración de incompetencia por el sujeto obligado.
- III. La entrega de datos personales incompletos.
- IV. La entrega de datos personales que no correspondan con lo solicitado.
- V. La negativa al acceso, rectificación, cancelación u oposición de datos personales.
- VI. La falta de respuesta a una solicitud ARCO, dentro de los plazos establecidos en la presente ley.
- VII. Los costos de reproducción o tiempos de entrega de los datos personales.
- VIII. La falta de trámite a una solicitud para el ejercicio de los derechos ARCO.



Se podrá interponer dentro de los **15 días** siguientes contados a partir de la notificación de la respuesta a la solicitud de derechos ARCO o del fenecimiento del plazo para dar una respuesta.

Es el organismo autónomo, especializado, independiente, imparcial y colegiado. Facultado para dirigir y vigilar el ejercicio de los Derechos de Acceso a la Información y de **Protección de Datos Personales**. Se encuentra conformado por 3 personas comisionadas ciudadanas y una de ellas funge como presidenta.



ALGUNAS ATRIBUCIONES DEL EN MATERIA DE DATOS PERSONALES

Promover y difundir el ejercicio del derecho a la protección de datos personales.	Resolver los recursos de revisión y verificaciones en materia de datos personales.	Llevar a cabo acciones y actividades que promuevan el conocimiento del derecho a la protección de datos personales	Requerir información para darle seguimiento a los procesos de verificación.	Diseñar y aprobar los formatos de solicitudes de acceso, rectificación, cancelación y oposición de datos personales.	Coordinarse y promover el derecho a la protección de datos personales con los responsables de manera permanente.
---	--	--	---	--	--

ÓRGANOS EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE SUJETOS OBLIGADOS

- UNIDAD DE TRANSPARENCIA
- COMITÉ DE TRANSPARENCIA

UNIDAD DE TRANSPARENCIA

Son las unidades administrativas **RECEPTORAS DE LAS SOLICITUDES DE DERECHOS ARCO**

Dan trámite y atienden las solicitudes; son el vínculo directo entre los sujetos obligados y las personas. Dependerá del Titular del SO.

Debe contar con:

- Responsable y personal que designe el titular del SO
- Oficinas visibles y accesibles al público
- Buzón ciudadano

Oficial de Datos Personales

- Especializado en la materia, forma parte de la Unidad de Transparencia y asesora al Comité de Transparencia.



Algunas atribuciones que tiene son:

Auxiliar y orientar al titular con relación al ejercicio de los derechos ARCO y la protección de datos personales.	Gestionar las solicitudes para el ejercicio de los derechos ARCO.	Proponer al Comité de Transparencia los procedimientos que aseguren y fortalezcan la gestión de las solicitudes de los derechos ARCO.	Asesorar a las áreas del sujeto obligado en materia de protección de datos personales	Podrá dar aviso al superior jerárquico en caso de que algún área se niegue a colaborar.	Registrar ante el Instituto los sistemas de datos personales, así como su modificación y supresión.
--	---	---	---	---	---

COMITÉ DE TRANSPARENCIA

Órgano Colegiado al interior de cada Sujeto Obligado integrado por número impar de personas servidoras públicas, que no dependerán jerárquicamente entre sí.

Sus integrantes son designados por el titular del sujeto obligado; el titular del órgano interno de control y los titulares de las unidades administrativas que propongan la clasificación o inexistencia de información.

¿Qué funciones tiene?

Instituir procedimientos internos para asegurar la mayor eficiencia en la gestión de las solicitudes para el ejercicio de los derechos ARCO.

Confirmar, modificar o revocar la declaración de la inexistencia de los datos personales.

Supervisar, en coordinación con las áreas o unidades administrativas competentes, el cumplimiento de las medidas, controles y acciones previstas en el documento de seguridad.

VERIFICACIÓN

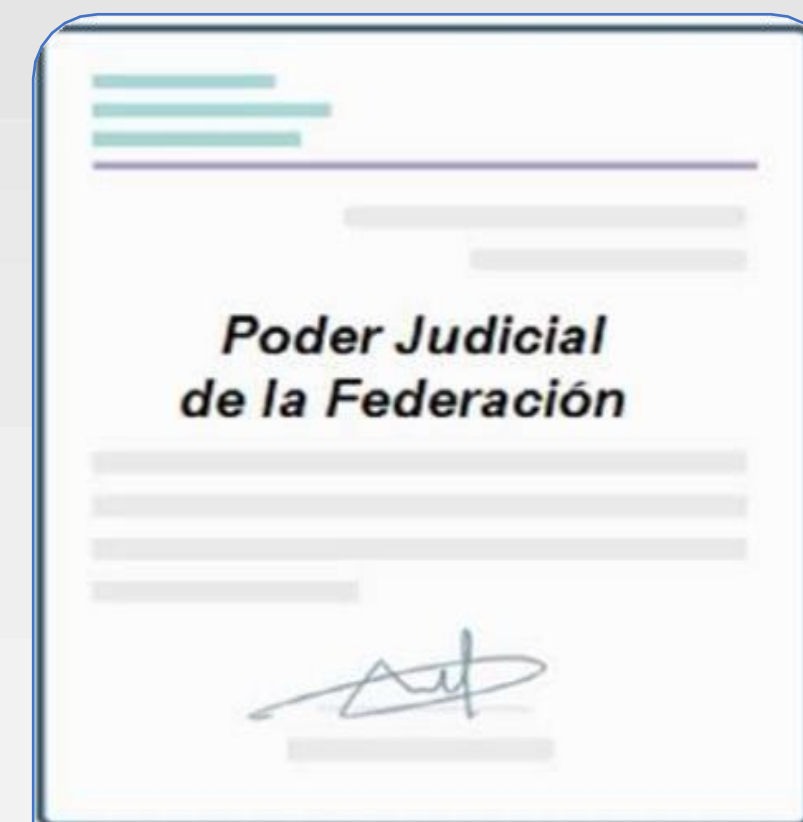
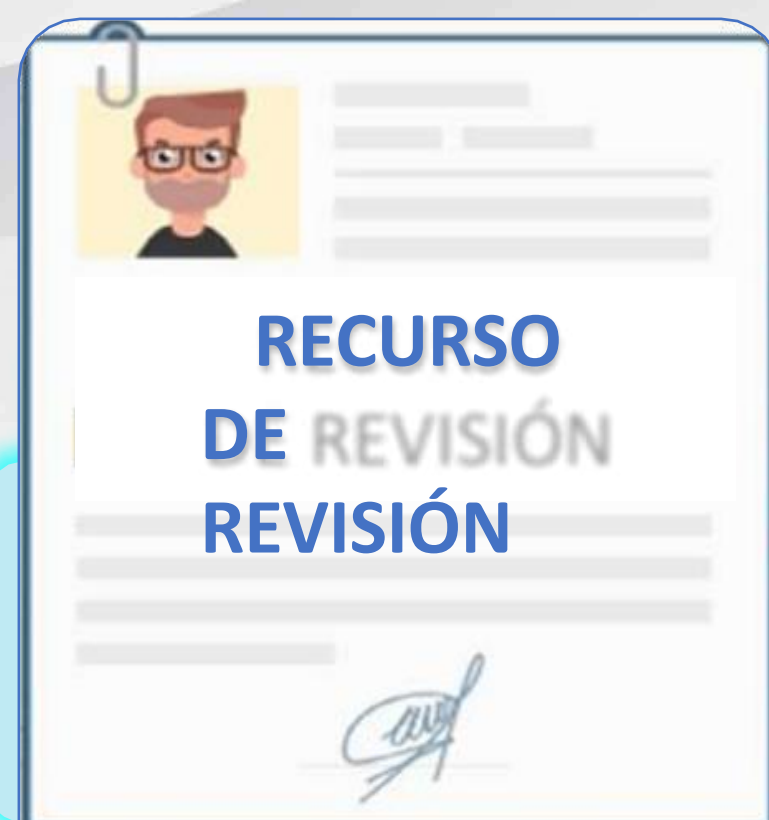
En el proceso de verificación:

• Vigila y verifica el cumplimiento de los principios y las disposiciones de la Ley. • Está obligado a guardar confidencialidad sobre la información a la que tiene acceso.	El responsable: • No podrá negar el acceso a la documentación solicitada con motivo de una verificación, ni podrá invocar la reserva o la confidencialidad de la información.
---	--

El inicio de la verificación puede ser por:

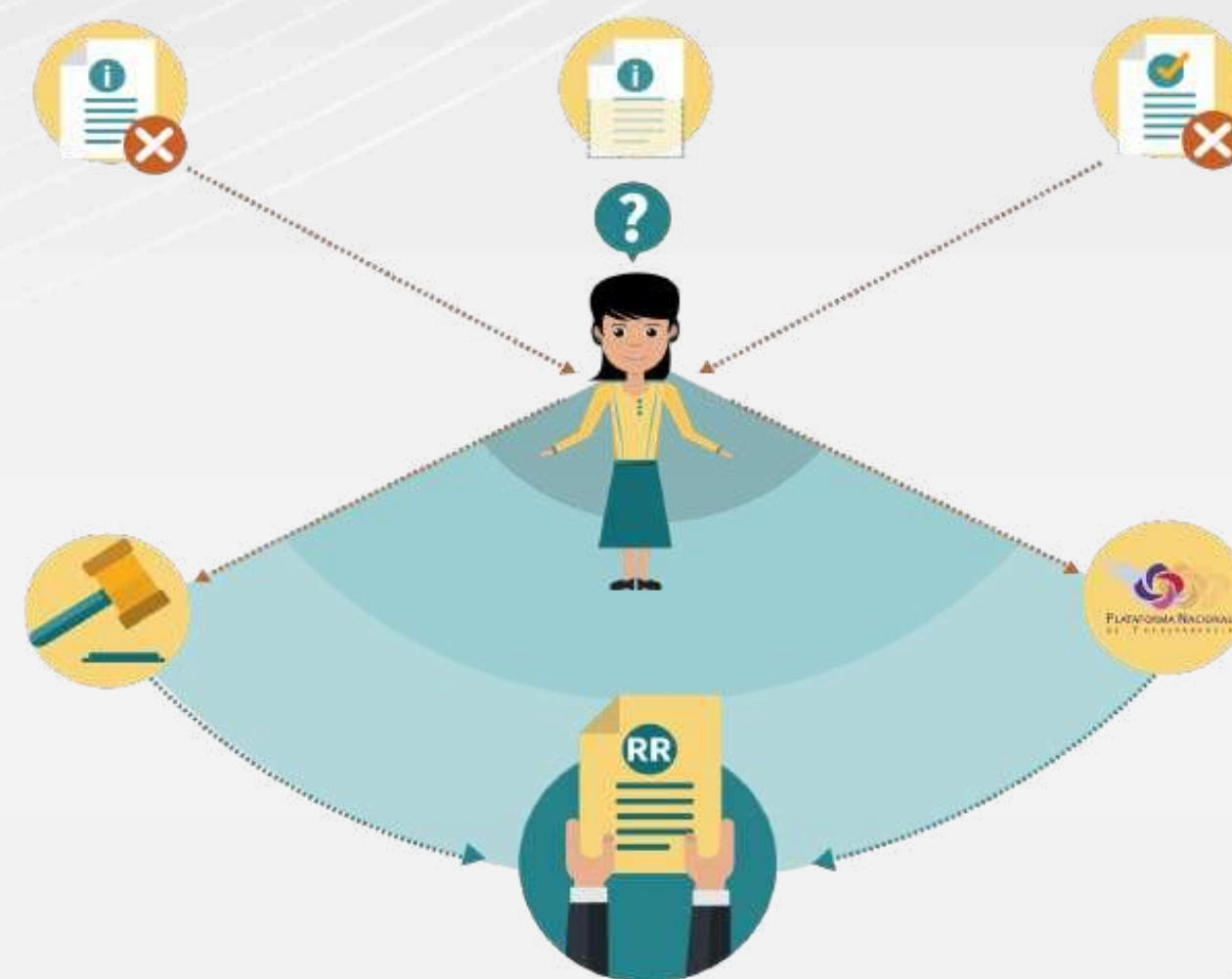
OFICIO Cuando el Instituto cuente con indicios que hagan presumir fundada y motivada la existencia de violaciones a las leyes correspondientes.			DENUNCIA Cuando considere que ha sido afectado por actos del responsable.
--	--	--	--

Medios de Impugnación en materia de protección de datos personales en posesión de sujetos obligados

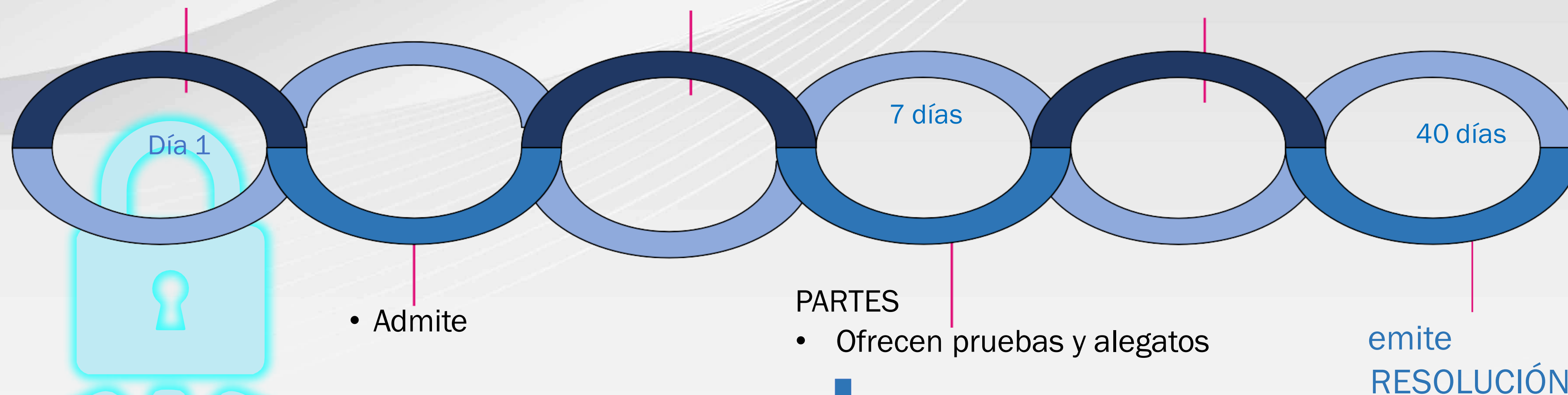


El INAI cuenta con una facultad de atracción, mediante la cual puede conocer y resolver los recursos promovidos ante el INAI, en casos de interés o trascendencia.

Esta facultad puede ejercerse de oficio o a petición de los organismos garantes.



Presentación del Recurso de revisión (RR)



El plazo de 40 días puede ampliarse por 20 días más.

CONCILIACIÓN

Podrá celebrarse:

- Presencialmente
- Medios electrónicos
- Cualquiera que este autorizado por el Instituto

RESOLUCIÓN DEL INSTITUTO

CONFIRMAR

- confirma la respuesta del Sujeto obligado

DESECHAR

- Sea extemporáneo, no se acredite debidamente la identidad, no haya atendido la prevención

SOBRESEE

- El recurrente desista, fallezca. Actualización de alguna causal de improcedencia o quede sin materia

MODIFICA O REVOCA

- Podrá ser modificada o revocada

ORDENA

- El responsable atienda la solicitud ARCO, en caso de omisión.

RECURSO DE INCONFORMIDAD Y AMPARO

Los particulares podrán impugnar las determinaciones o resoluciones del ante el INAI, a través de un recurso de Inconformidad; o ante el Poder Judicial, mediante un amparo. Pero nunca se agotaran ambas vías al mismo tiempo. Estos recursos proceden contra las resoluciones que:

1. Clasifiquen datos personales sin que se cumplan las características señaladas en las leyes locales.
2. Determinen inexistencia de datos personales; o
3. Declaren la negativa de datos personales incompletos

La resolución del INAI será definitiva e inatacable para el organismo garante (INFO) y el sujeto obligado. Sin embargo, el particular podrá impugnar, de nueva cuenta, las resoluciones del INAI ante el Poder Judicial de la Federación, mediante un AMPARO.



CUMPLIMIENTO DE LAS RESOLUCIONES

Los Sujeto Obligados a través de su Unidad de Transparencia darán cumplimiento a las resoluciones del INFO.

El sujeto obligado deberá informar el cumplimiento de la resolución

El INFO verificará de oficio la información , a más tardar al día siguiente de recibir el oficio de cumplimiento, y dará vista al recurrente.

Si el INAIP considera que el Sujeto obligado da cumplimiento , se emitirá un Acuerdo de cumplimiento. En caso contrario el INAIP :

1. Emitirá un acuerdo de incumplimiento
2. Notificará al superior jerárquico del responsable de dar cumplimiento.
3. Determinará las medidas de apremio o sanciones.

A dark blue arrow pointing from the right towards the list of actions.

Posibles vistas
al OIC

MEDIDAS DE APREMIO Y SANCIONES

Medidas de apremio y sanciones

- El Instituto, podrá imponer al encargado de cumplir con la resolución, las siguientes medidas de apremio para asegurar el cumplimiento de sus determinaciones:
- Amonestación pública, o
- Multa

Posibles vistas
al OIC

Causales

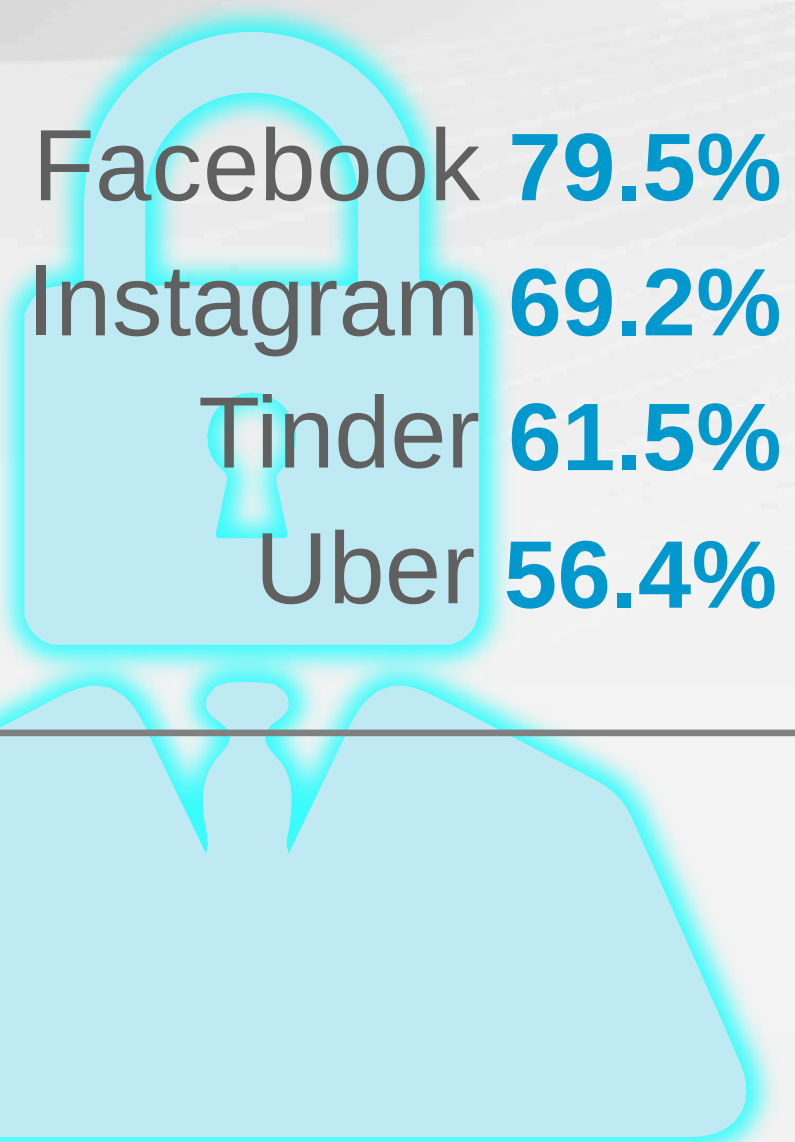
- Actuar con negligencia, dolo o mala fe durante la sustanciación de las solicitudes para el ejercicio de los derechos ARCO;
- Incumplir los plazos de atención previstos en la presente Ley para responder las solicitudes para el ejercicio de los derechos ARCO o para hacer efectivo el derecho de que se trate;
- Usar, sustraer, divulgar, ocultar, alterar, mutilar, destruir o inutilizar, total o parcialmente y de manera indebida datos personales, que se encuentren bajo su custodia o a los cuales tengan acceso o conocimiento con motivo de su empleo, cargo o comisión;
- Dar tratamiento, de manera intencional, a los datos personales en contravención a los principios y deberes establecidos en la presente Ley;
- No recabar el consentimiento del titular, lo que constituye que el tratamiento sea ilícito, o no contar con el aviso de privacidad, o bien tratar de manera dolosa o con engaños datos personales y las demás disposiciones que resulten aplicables en la materia;

El incumplimiento de los sujetos obligados será difundido en los portales de obligaciones de transparencia del Instituto y considerados en las evaluaciones.

El entorno digital como reto para la actualización de la Ley Federal de Protección de Datos Personales en Posesión de Particulares



Almacenamiento de datos personales

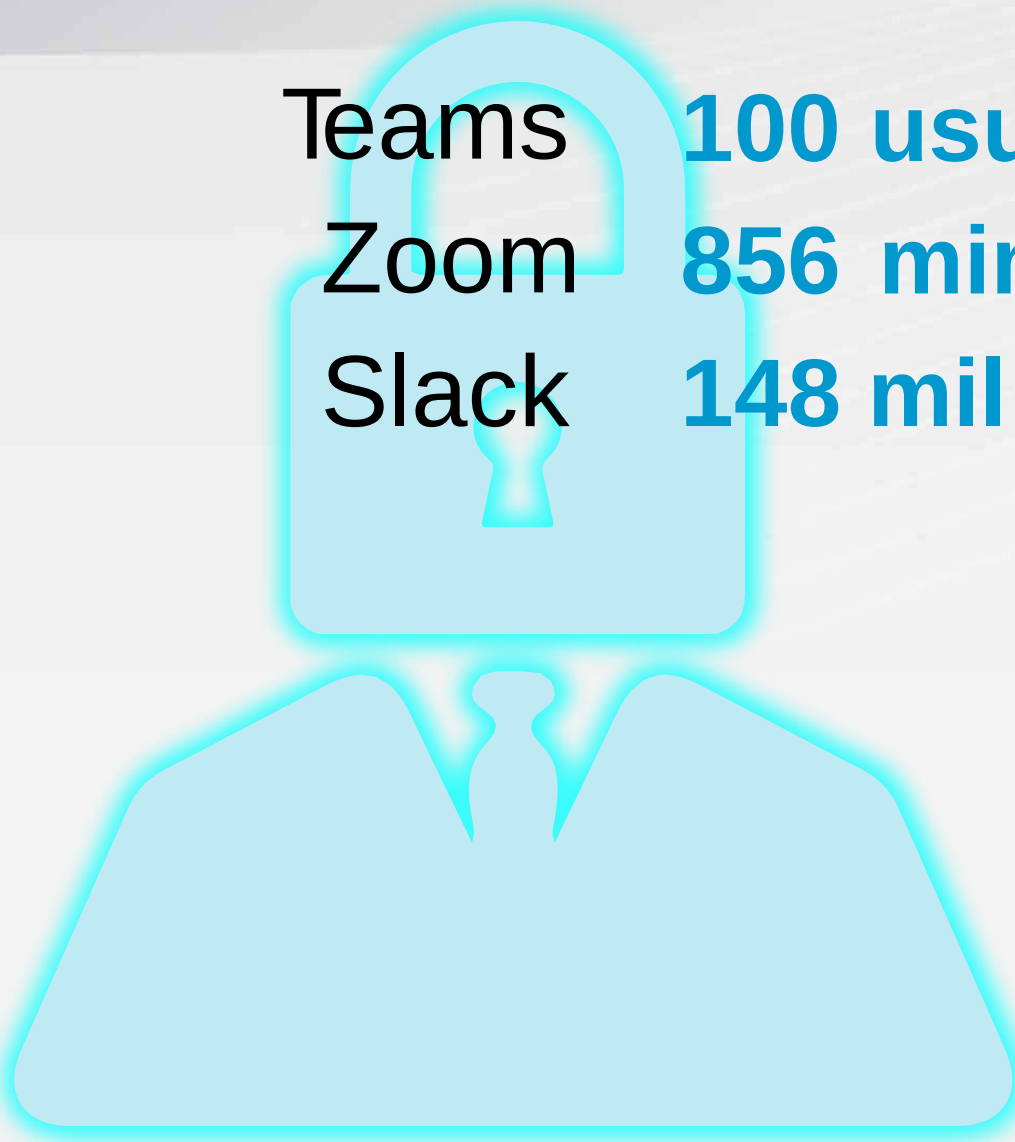


Facebook **79.5%**
Instagram **69.2%**
Tinder **61.5%**
Uber **56.4%**

Estudio “Tus datos nunca duermen”

Instagram	65 mil fotografías
Facebook	240 mil fotos en Facebook
Youtube	240 mil fotos en Facebook
Netflix	694 mil horas de vídeo
TikTok	167 millones de usuarios ven vídeos
Twitter	575 mil usuarios publican un tuit

Teletrabajo

A stylized, light blue icon of a person wearing a suit and tie, with a glowing cyan outline. The person's head is replaced by a square containing a keyhole shape.

Teams 100 usuarios se conectan
Zoom 856 minutos de webinars
Slack 148 mil mensajes

Riesgos y problemáticas en el entorno digital

Violencia digital
Robo de identidad

DERECHO COMPARADO





Protección de Datos Personales en América Latina

Convención Interamericana de Derechos Humanos

Artículo 11. Protección de la Honra y de la Dignidad

1. Toda persona tiene derecho al respeto de su honra y al reconocimiento de su dignidad.
2. Nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación.
3. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques.



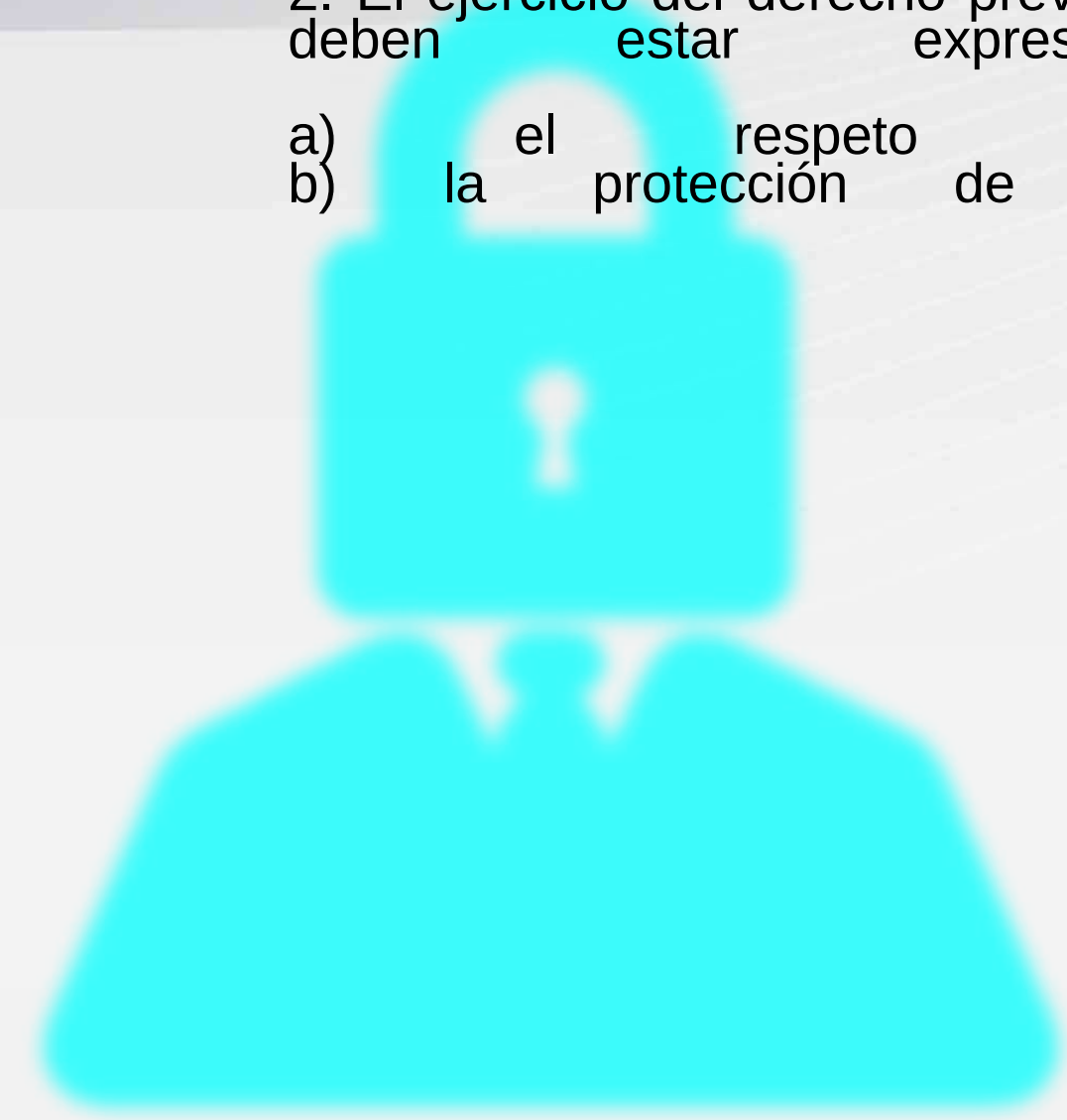
Convención Interamericana de Derechos Humanos

Artículo 13. Libertad de Pensamiento y de Expresión

1. Toda persona tiene derecho a la libertad de pensamiento y de expresión. Este derecho comprende la libertad de buscar, recibir y difundir informaciones e ideas de toda índole, sin consideración de fronteras, ya sea oralmente, por escrito o en forma impresa o artística, o por cualquier otro procedimiento de su elección.

2. El ejercicio del derecho previsto en el inciso precedente no puede estar sujeto a previa censura sino a responsabilidades ulteriores, las que deben estar expresamente fijadas por la ley y ser necesarias para asegurar:

- a) el respeto a los derechos o a la reputación de los demás,
- b) la protección de la seguridad nacional, el orden público o la salud o la moral públicas.



ESTÁNDARES DE PROTECCIÓN DE DATOS PERSONALES PARA LOS ESTADOS IBEROAMERICANOS

Red Iberoamericana de Protección de Datos surgió con motivo del acuerdo alcanzado en el Encuentro Iberoamericano de Protección de Datos, celebrado en La Antigua, Guatemala, del 1 al 6 de junio de 2003, con la asistencia de representantes de 14 países iberoamericanos.

La Red, aprobó los Estándares en el XV Encuentro Iberoamericano de Protección de Datos, celebrado en Santiago de Chile.



A decorative graphic consisting of several overlapping rectangles in shades of purple, blue, and green, located on the left side of the page.

ESTÁNDARES DE PROTECCIÓN DE DATOS PERSONALES PARA LOS ESTADOS IBEROAMERICANOS

Capítulo I: Disposiciones generales

Capítulo II: Principios de protección de datos personales

Capítulo III: Derechos del titular

Capítulo IV: Encargado

Capítulo V: Transferencias internacionales de datos personales

Capítulo VI: Medidas proactivas en el tratamiento de datos personales

Capítulo VII: Autoridades de control

Capítulo VIII: Reclamaciones y Sanciones

Capítulo IX: Derecho de indemnización

Capítulo X: Cooperación internacional

Brasil



Artículo 5, fracción LXXII de la Constitución Política de la República Federativa del Brasil, 1988

Esta Ley establece el procesamiento de datos personales, incluso en medios digitales, por una persona física o jurídica de derecho público o privado, con el objetivo de proteger los derechos fundamentales de libertad y privacidad y el libre desarrollo de la personalidad, de la persona natural.

Ley No. 13.709, de 14 de agosto de 2018; Ley General de Protección de Datos Personales (LGPD). Conformada por 65 artículos en diez capítulos.

Ley No. 13.853, del 8 de julio de 2019; Modifica la Ley N ° 13.709 de 14 de agosto de 2018, para proporcionar la protección de datos personales y crear la Autoridad Nacional de Protección de Datos; entre otras consideraciones. (Entrará en vigor en agosto del 2020)



Brasil



PRINCIPIOS GENERALES

- Limitación del **plazo de conservación** de los datos personales, es decir, bloquear y/o destruir los datos en plazo de tiempo determinado.
- **Transparencia** en cuanto a la información proporcionada a los interesados sobre el tratamiento de sus datos personales.
- **Responsabilidad proactiva** en el uso de medidas de seguridad y políticas antes brechas de seguridad en los sistemas utilizados por las empresas en el tratamiento de los datos personales.
- Obtención de **consentimiento como base de legitimación para el tratamiento** de datos personales, cuando proceda. Este consentimiento deberá ser expreso.
- **Exactitud y veracidad de los datos personales** cuando los mismos no sean proporcionados por los interesados.



Brasil



AUTORIDAD NACIONAL DE PROTECCIÓN DE DATOS (ANPD) Y EL CONSEJO NACIONAL DE PROTECCIÓN Y PRIVACIDAD DE DATOS PERSONALES

ANPD será responsable de inspeccionar las empresas y organismos públicos que llevarán a cabo el procesamiento de los datos de cualquier persona, ya sea con fines comerciales o legales.

La ANPD cuenta con las siguientes atribuciones:

- Reglamentación: emisión de normas y procedimientos, así como deliberación, en el ámbito administrativo, sobre la interpretación de la LGPD.
- Fiscalización y aplicación de sanciones: requerimiento de información, implementación de mecanismos de sanciones administrativas.
- Educación: difusión de las normas y políticas de tratamiento de datos personales y estimulación de la adopción de padrones para servicios y productos que proporcionen el control de los datos personales.



Brasil



Instituto Estatal de Transparencia, Acceso a la Información Pública
y Protección de Datos Personales
Organismo Público Autónomo

AUTORIDAD NACIONAL DE PROTECCIÓN DE DATOS (ANPD) Y EL CONSEJO NACIONAL DE PROTECCIÓN Y PRIVACIDAD DE DATOS PERSONALES

Las sanciones:

El incumplimiento de la LGPD por los agentes de tratamiento de datos puede resultar en diversas penalidades, entre ellas:

- Recepción de advertencia
- Publicidad de la infracción
- Bloqueo o eliminación de los datos personales a que se refiere la infracción
- Multas diarias, o multas simples de hasta el 2% (dos por ciento) de la facturación del grupo empresarial en Brasil, limitadas a R\$50.000.000,00 (cincuenta millones de reales) por infracción.
(Equivalente a \$243,537,930 pesos mxn)



Brasil

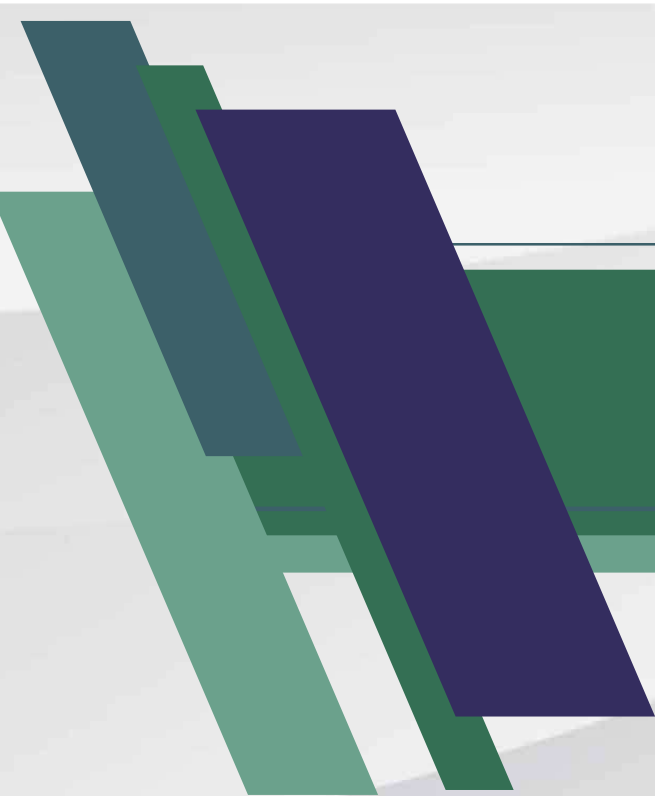


Instituto Estatal de Transparencia, Acceso a la Información Pública
y Protección de Datos Personales
Organismo Público Autónomo

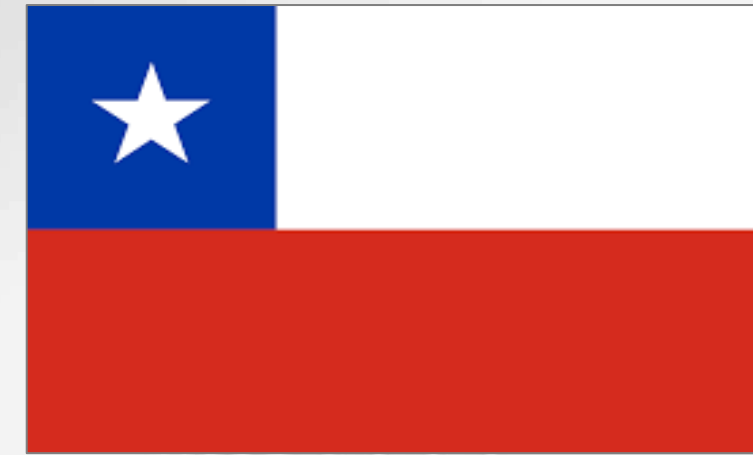
Caso relevante:

Proceso de la presentadora de televisión María das Graças Meneghel, conocida como “Xuxa” en contra del servidor de búsqueda Google.

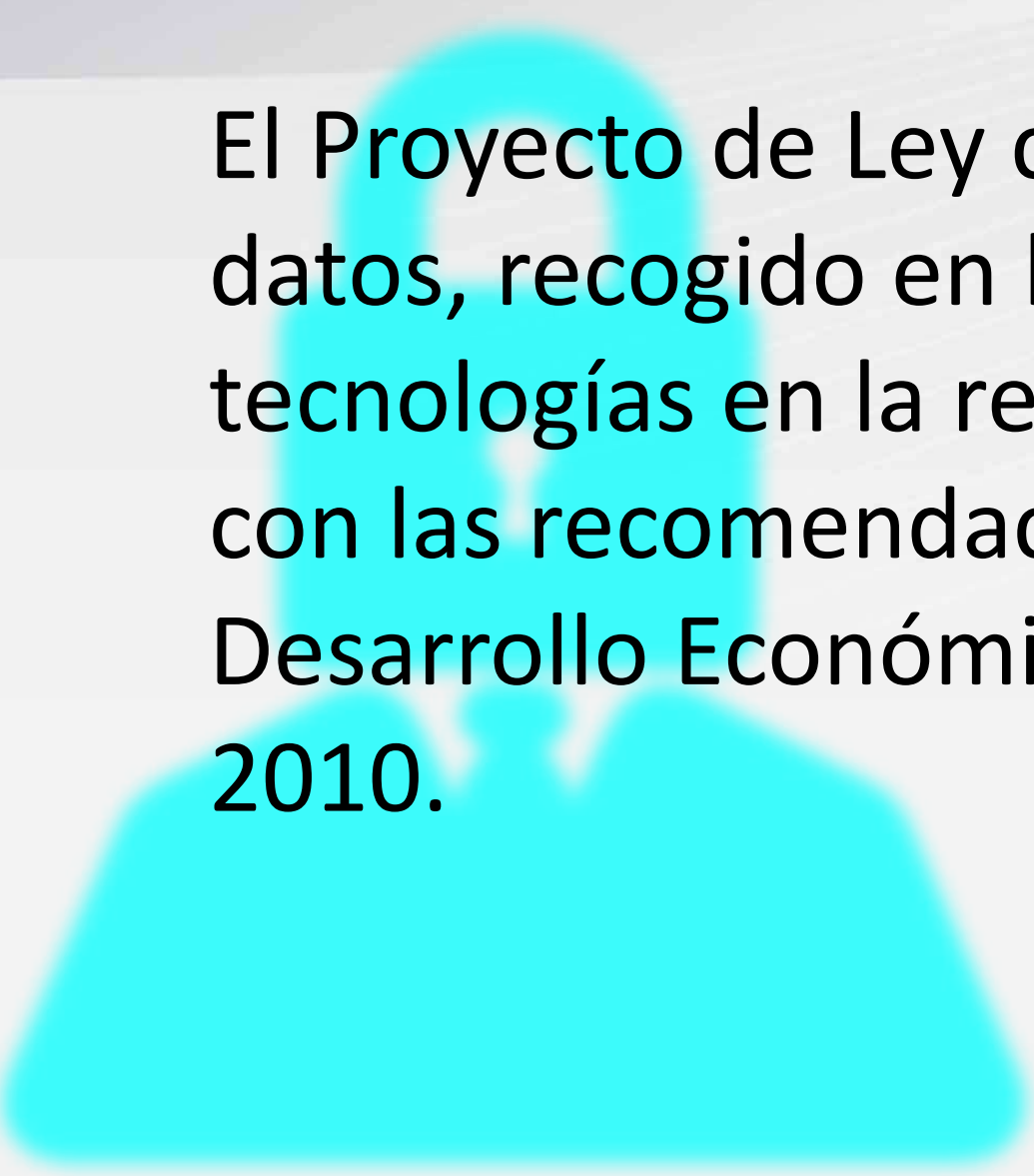
Xuxa solicitó censurar las imágenes de una película que filmó en los años 1980, "Amor Estranho Amor". Llegando a la conclusión que la demanda en contra de Google no tuvo frutos para la comunicadora social, apelando que no existe una tecnología para aplicar una censura tan específica como la solicitada por Xuxa.



Chile



Instituto Estatal de Transparencia, Acceso a la Información Pública
y Protección de Datos Personales
Organismo Público Autónomo



El Proyecto de Ley chileno se propone modernizar el régimen legal de protección de datos, recogido en la actual ley 19.628, regulando aspectos como las nuevas tecnologías en la recogida y difusión de datos personales. Se plantea también cumplir con las recomendaciones en esta materia de la Organización para la Cooperación y el Desarrollo Económico (OCDE), organización de la que Chile es miembro desde el año 2010.



Chile



Instituto Estatal de Transparencia, Acceso a la Información Pública
y Protección de Datos Personales
Organismo Público Autónomo

La propuesta destaca los siguientes puntos:

- Se establecen unos **principios rectores** que inspiran la regulación del tratamiento de datos personales, en concreto, se refiere a los principios de licitud del tratamiento, finalidad, proporcionalidad, calidad, seguridad, responsabilidad e información.
- Se reconocen los denominados derechos “ARCO”, **derecho de acceso, de rectificación, cancelación y oposición** al tratamiento de los datos personales, todos ellos derechos irrenunciables, gratuitos y que no pueden limitarse.
- El **consentimiento** del titular de los datos es la principal fuente de legitimidad para el tratamiento. El consentimiento, que se puede revocar en cualquier momento, debe ser libre, informado, inequívoco, previo al tratamiento y específico en cuanto a la finalidad. El proyecto de Ley también establece casos en los que no es necesario el consentimiento.

Chile



Instituto Estatal de Transparencia, Acceso a la Información Pública
y Protección de Datos Personales
Organismo Público Autónomo

- Se establece un **régimen de responsabilidad** de los responsables de datos incluyendo deberes como el de información, confidencialidad, de adoptar medidas de seguridad y reportar vulneraciones.
- Se adoptan nuevos estándares para el tratamiento de datos personales calificados como **sensibles**, de forma que solo pueden realizarse cuando el titular consienta libre, informado y de forma expresa. Considera que son datos sensibles los vinculados con la salud, biométricos, de perfil biológico, de geolocalización así como los datos de niños y adolescentes.
- Se regula la **transmisión internacional de datos**, permitiendo el flujo a países considerados adecuados por su legislación y estableciendo condiciones, como el aviso previo a la autoridad de control, en el caso de transmisión de datos a países considerados no adecuados.
- Se crea la **Agencia de Protección de Datos Personales**, que es la autoridad de control encargada de regular, supervisar, fiscalizar y sancionar los incumplimientos de la Ley. Dependiendo del tipo de infracción la sanción puede ir desde la amonestación por escrito a multas entre 1 y 5.000 UTM, o en casos excepcionales hasta el cierre de operaciones de tratamiento de datos.

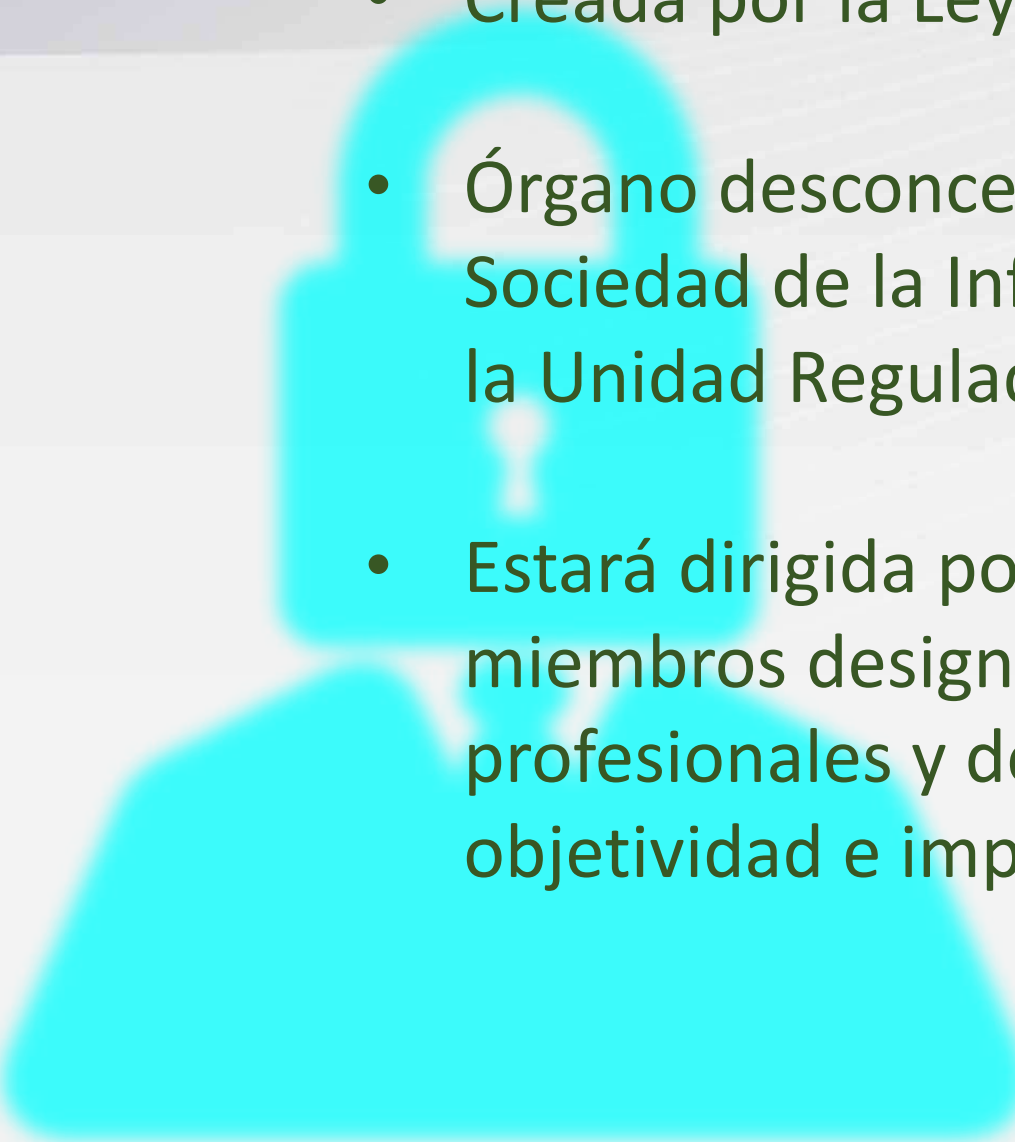


Uruguay



Instituto Estatal de Transparencia, Acceso a la Información Pública
y Protección de Datos Personales
Organismo Público Autónomo

Unidad Reguladora y de Control de Datos Personales

- 
- Creada por la Ley N° 18.331 de Protección de Datos Personales y Acción de Habeas Data (LPDP).
 - Órgano desconcentrado de la Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento (AGESIC), dotado de la más amplia autonomía técnica, la Unidad Reguladora y de Control de Datos Personales.
 - Estará dirigida por un Consejo integrado por tres miembros: el Director Ejecutivo de AGESIC y dos miembros designados por el Poder Ejecutivo entre personas que por sus antecedentes personales, profesionales y de conocimiento en la materia aseguren independencia de criterio, eficiencia, objetividad e imparcialidad en el desempeño de sus cargos.



Uruguay



Funciones y atribuciones:

- A) Asistir y asesorar a las personas que lo requieran acerca de los alcances de la presente ley y de los medios legales de que disponen para la defensa de los derechos que ésta garantiza.
- B) Dictar las normas y reglamentaciones que se deben observar en el desarrollo de las actividades comprendidas por esta ley.
- C) Realizar un censo de las bases de datos alcanzados por la ley y mantener el registro permanente de los mismos.
- D) Controlar la observancia del régimen legal, en particular las normas sobre legalidad, integridad, veracidad, proporcionalidad y seguridad de datos, por parte de los sujetos alcanzados, pudiendo a tales efectos realizar las actuaciones de fiscalización e inspección pertinentes.

Uruguay



Potestades:

- 1) Exigir a los responsables y encargados de tratamientos la exhibición de los libros, documentos y archivos, informáticos o convencionales, propios y ajenos, y requerir su comparecencia ante la Unidad para proporcionar informaciones.
- 2) Intervenir los documentos y archivos inspeccionados, así como tomar medidas de seguridad para su conservación, pudiendo copiarlos.
- 3) Incautarse de dichos elementos cuando la gravedad del caso lo requiera hasta por un lapso de seis días hábiles; la medida será debidamente documentada y sólo podrá prorrogarse por los órganos jurisdiccionales competentes, cuando sea imprescindible.

Uruguay



Instituto Estatal de Transparencia, Acceso a la Información Pública
y Protección de Datos Personales
Organismo Público Autónomo

(Potestades sancionatorias).- El órgano de control podrá aplicar las siguientes sanciones a los responsables de las bases de datos, encargados de tratamiento de datos personales y demás sujetos alcanzados por el régimen legal, en caso que se violen las normas de la presente ley, las que se graduarán en atención a la gravedad, reiteración o reincidencia de la infracción cometida:

- 1) Observación.
- 2) Apercibimiento.
- 3) Multa de hasta 500.000 UI (quinientas mil unidades indexadas).
- 4) Suspensión de la base de datos respectiva por el plazo de cinco días.
- 5) Clausura de la base de datos respectiva. A tal efecto se podrá promover ante los órganos jurisdiccionales competentes la clausura de las bases de datos que se comprobare infringieren o transgredieren la ley

Uruguay



Acción de protección de datos personales o habeas data

- A) Cuando quiera conocer sus datos personales que se encuentran registrados en una base de datos o similar y dicha información le haya sido denegada, o no le hubiese sido proporcionada por el responsable de la base de datos, en las oportunidades y plazos previstos por la ley.
- B) Cuando haya solicitado al responsable de la base de datos o tratamiento su rectificación, actualización, eliminación, inclusión o supresión y éste no hubiese procedido a ello o dado razones suficientes por las que no corresponde lo solicitado, en el plazo previsto al efecto en la ley.

Competencia para conocer de la acción:

- 1) En la Capital, los Juzgados Letrados de Primera Instancia en lo Contencioso Administrativo, cuando la acción se dirija contra una persona pública estatal, y los Juzgados Letrados de Primera Instancia en lo Civil en los restantes casos.
- 2) Los Juzgados Letrados de Primera Instancia del Interior a quienes se haya asignado competencia en dichas materias.

Colombia



Instituto Estatal de Transparencia, Acceso a la Información Pública
y Protección de Datos Personales
Organismo Público Autónomo

La Ley 1581 de 2012 distingue cuatro tipos de reclamos:

- 1. RECLAMO DE CORRECCIÓN:** Es el derecho del Titular a que se actualicen, rectifiquen o modifiquen aquellos datos parciales, inexactos, incompletos o aquellos cuyo tratamiento esté expresamente prohibido o no haya sido autorizado.
- 2. RECLAMO DE SUPRESIÓN:** Es el derecho del Titular a que se supriman los datos que resulten inadecuados, excesivos o que no respeten los principios de legalidad.
- 3. RECLAMO DE REVOCACIÓN:** Es el derecho del Titular a dejar sin efecto la autorización previamente prestada para el tratamiento de sus datos personales.
- 4. RECLAMO DE INFRACCIÓN:** Es el derecho del Titular a solicitar que se subsane el incumplimiento de la normativa en materia de Protección de Datos.



Observaciones.

La Superintendencia de Industria y Comercio SIC, mediante la Delegatura para la Protección de Datos Personales es la encargada de garantizar que en la recolección, el uso, la circulación y el Tratamiento de datos personales se respeten los principios, derechos, garantías y procedimientos previstos en la Constitución y en la Ley de Protección de Datos Personales,

Cuenta con un sistema de sanciones proporcional en función de la categoría y gravedad de las infracciones que se lleven a cabo.



Colombia



SIDAD
ET

Puede imponer sanciones por el incumplimiento de la normativa sobre protección de datos personales al responsable del tratamiento como son:

1. Multas de carácter personal e institucional hasta por el equivalente a dos mil (2.000) salarios mínimos mensuales legales vigentes al momento de la imposición de la sanción.
2. Suspensión de las actividades relacionadas con el tratamiento hasta por un término de seis meses.
3. Cierre temporal o definitivo de las operaciones relacionadas con el tratamiento una vez transcurrido el término de suspensión sin que se hubieren adoptado los correctivos ordenados por la Superintendencia de Industria y Comercio.

Caso Relevante

Mediante resolución 39298 del pasado 21 de Junio de 2016, la Dirección de investigaciones de protección de datos personales de la Superintendencia de Industria y Comercio impuso a la empresa COLMEDICA MEDICINA PREPAGADA S.A., la multa más alta impuesta a una empresa en Colombia por la cantidad de \$1.034 millones.

Los motivos: la entidad dejó en evidencia información de 30 usuarios que habían realizado consultas por la página web de la empresa y la entidad no había tomado las medidas de seguridad adecuadas.



Argentina



Instituto Estatal de Transparencia, Acceso a la Información Pública
y Protección de Datos Personales
Organismo Público Autónomo

Constitución

Artículo 43. Toda persona podrá interponer esta acción para tomar conocimiento de los datos a ella referidos y de su finalidad, que consten en registros o bancos de datos públicos, o privados destinados a proveer informes, y en caso de falsedad o discriminación, para exigir la supresión, rectificación, confidencialidad o actualización de aquellos. No podrá afectarse el secreto de las fuentes de información periodística.

Ley 1845



Título I. Disposiciones Generales: artículos 1 al 3

Título II. Del Régimen de los Archivos, Registros, Bases o Bancos de Datos: artículos 4 a 5

Título III. Principios Generales de la Protección de Datos Personales: artículos: 6 al 12

Título IV. Derechos de los Titulares de Datos Personales: artículos: 13 al 15

Título V. Obligaciones Relacionadas con los Datos Personales Asentados en Archivos, Registros, Bases o Bancos de Datos: artículos 16 al 21

Título VI. Control: artículos 22 al 24

Título VII. Infracciones: artículo 25

Título VIII. Sanciones: artículos: 26 a 27

Título IX. Acción de protección de datos: artículos 28 a 37

Título X. Disposiciones particulares: artículos 28 a 39

Título XI. Disposiciones transitorias: 2 artículos



Observaciones.

- El cuerpo normativo vigente en la Ley 25.326, sigue a rajatabla la estructura y contenidos de las legislaciones de los países europeos, razón por la cual, Argentina ha sido declarado por la Comisión Europea como un país que garantiza un nivel adecuado de protección de datos.
- Argentina cuenta con la particularidad de tener una Ley en materia de Protección de Datos para la provincia de Buenos Aires, la Ley 1845 que sigue los lineamientos de la vigente ley 25326, esto es, prohibiciones de transferencias interprovinciales a provincias o municipios del país que no ofrezcan niveles adecuados de protección, siguiendo los esquemas habituales de transferencias internacionales.



Perú



Instituto Estatal de Transparencia, Acceso a la Información Pública
y Protección de Datos Personales
Organismo Público Autónomo

Constitución

Artículo 2. – Toda persona tiene derecho a:

5. A solicitar sin expresión de causa la información que requiera y a recibirla de cualquier entidad pública, en el plazo legal (.....). Se exceptúan las informaciones que afectan la intimidad personal y las que expresamente se excluyan por ley o por razones de seguridad nacional.

6. A que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar.

Artículos 161 y 162. – Defensa de los derechos fundamentales de la persona y de la comunidad.

Artículo 200: Garantías constitucionales.

3.- La Acción de Hábeas Data, que la Procede contra el hecho u omisión, Parte de cualquier autoridad funcionario o persona, que vulnera o amenaza los derechos a que se refiere el Artículo 2, inciso 5) y 6) de la Constitución

Perú



Instituto Estatal de Transparencia, Acceso a la Información Pública
y Protección de Datos Personales
Organismo Público Autónomo

Ley N° 29733,

Ley de Protección de Datos Personales (LPDP), publicada en el Diario Oficial El Peruano con fecha 03 de julio de 2011, la cual establece los términos en que se garantiza el derecho fundamental a la protección de los datos personales a través de un adecuado tratamiento, en un marco de respeto de los demás derechos fundamentales.

Artículo 1. La presente Ley tiene el objeto de garantizar el derecho fundamental a la protección de los datos personales, previsto en el artículo 2 numeral 6 de la Constitución Política del Perú, a través de su adecuado tratamiento, en un marco de respeto de los demás derechos fundamentales que en ella se reconocen.

Perú



Instituto Estatal de Transparencia, Acceso a la Información Pública
y Protección de Datos Personales
Organismo Público Autónomo

Autoridad Reguladora

Decreto Legislativo N° 1353, Decreto Legislativo que crea la Autoridad Nacional de Transparencia y Acceso a la Información Pública,

- La autoridad nacional de protección de datos personales debe cumplir y hacer cumplir la normatividad vigente en materia de protección de datos personales. Tiene funciones administrativas, orientadoras, normativas, resolutivas, fiscalizadoras y sancionadoras.
- Los derechos con los que cuenta el titular de los datos -Acceso, actualización, inclusión, rectificación y supresión, impedir el suministro, oposición, tratamiento objetivo y tutela-, están sujetos a una contraprestación por parte del titular, regulada en la Ley del Procedimiento Administrativo General.

Observaciones.

INFRACCIONES

Ley N° 29733, Ley de Protección de Datos Personales

Artículo 132.- Infracciones

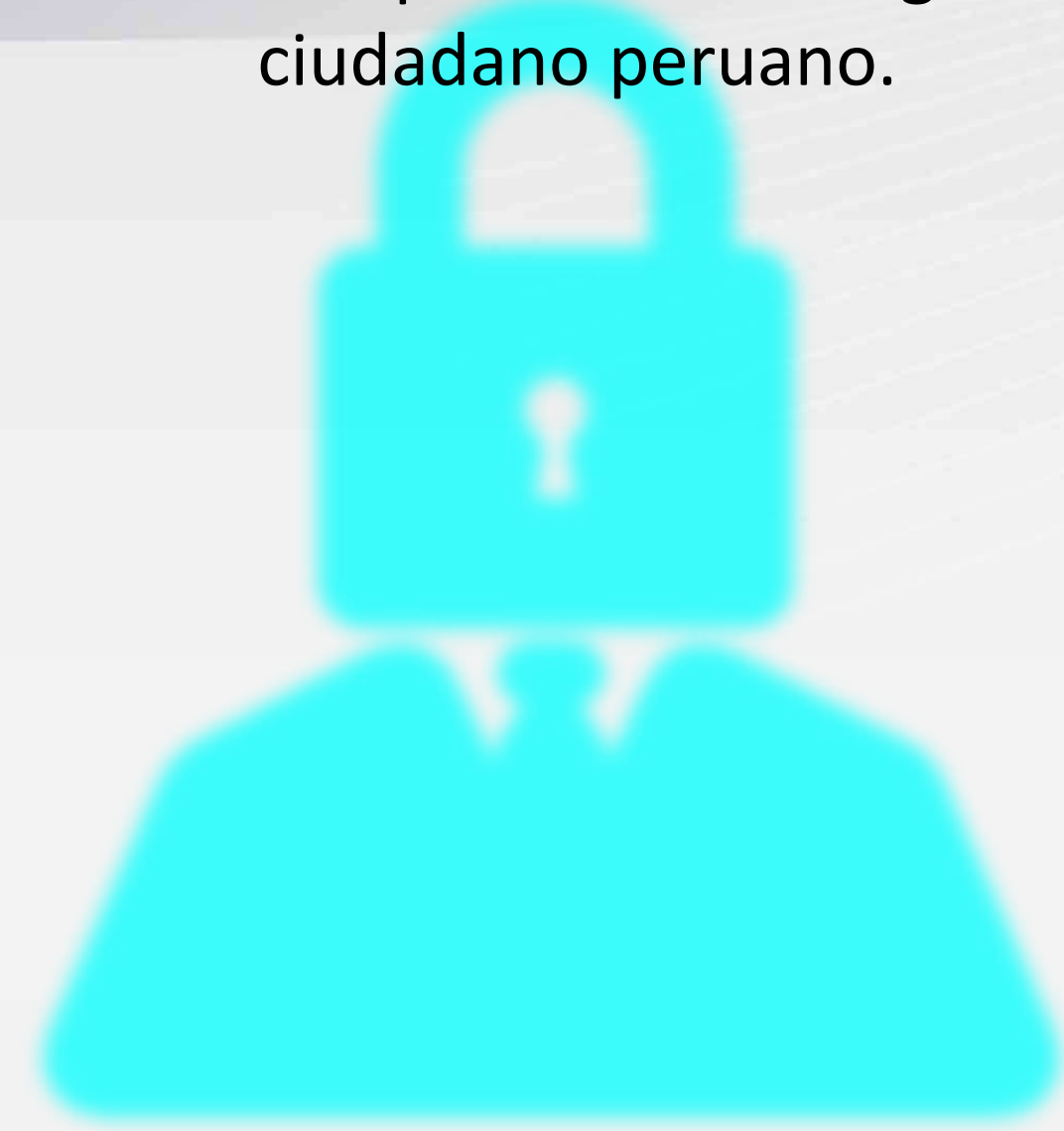
- Las infracciones y sanciones siguen el sistema de clasificación entre Las infracciones a la Ley N° 29733, Ley de Protección de Datos Personales, o su Reglamento se califican como leves, graves y muy graves y se sancionan con multa de acuerdo al artículo 39 de la citada Ley.
- Van desde 0.5 Unidades Impositiva Tributarias (50 soles hasta 100 Unidades Impositivas Tributarias 10,000 soles)



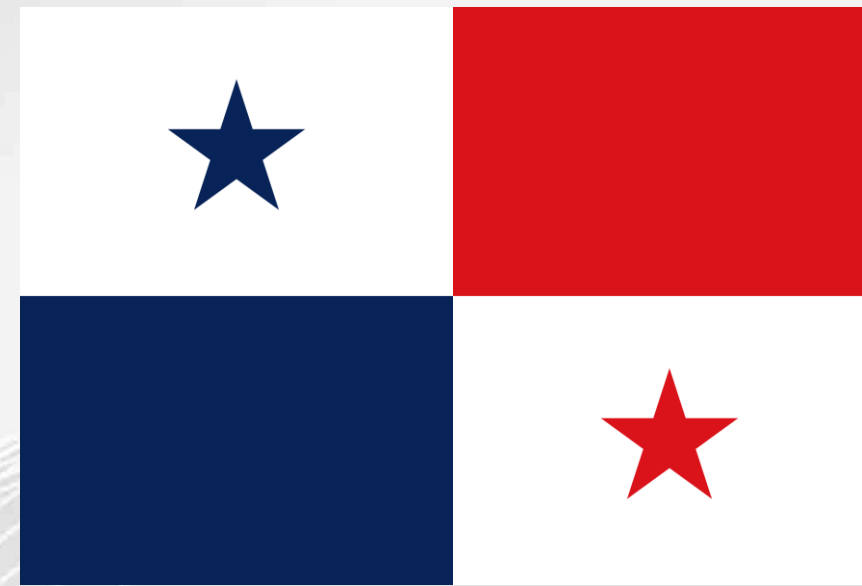
Caso Relevante

Google es sancionado por desconocer el Derecho a la Verdad

La Dirección General de Protección de Datos Personales resolvió donde aplicó por vez primera el derecho al olvido. El Ministerio de Justicia ordenó a google ocultar ciertos resultados de búsqueda cuando alguien buscara el nombre del algún ciudadano peruano.



Panamá



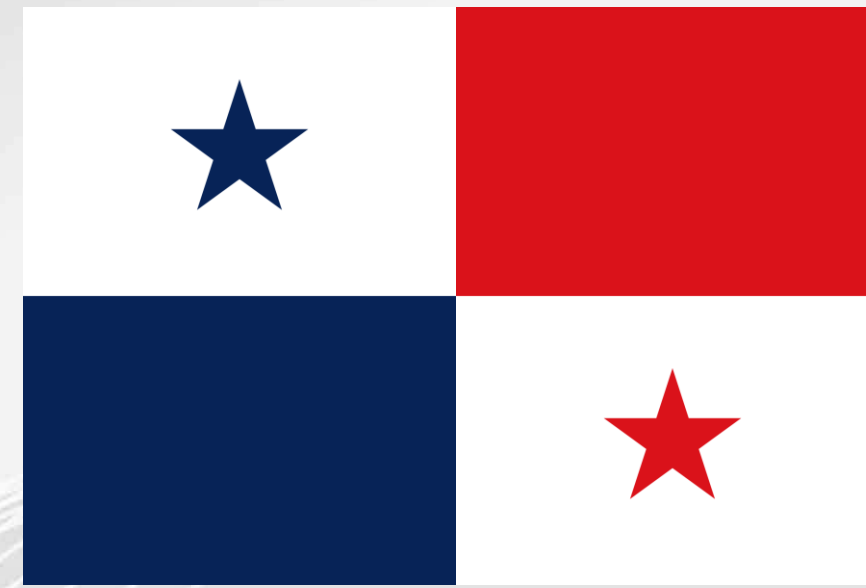
Instituto Estatal de Transparencia, Acceso a la Información Pública
y Protección de Datos Personales
Organismo Público Autónomo

Constitución de la República de Panama.

Artículo 17: Las autoridades de la República están instituidas para proteger en su vida, honra y bienes a los nacionales dondequiera se encuentren y a los extranjeros que estén bajo su jurisdicción; asegurar la efectividad de los derechos y deberes individuales y sociales, y cumplir y hacer cumplir la Constitución y la Ley

Artículo 29: La correspondencia y demás documentos privados son inviolables y no pueden ser examinados ni retenidos, sino por mandato de autoridad competente y para fines específicos, de acuerdo con las formalidades legales. En todo caso, se guardará absoluta reserva sobre los asuntos ajenos al objeto del examen o de la retención.

Panamá



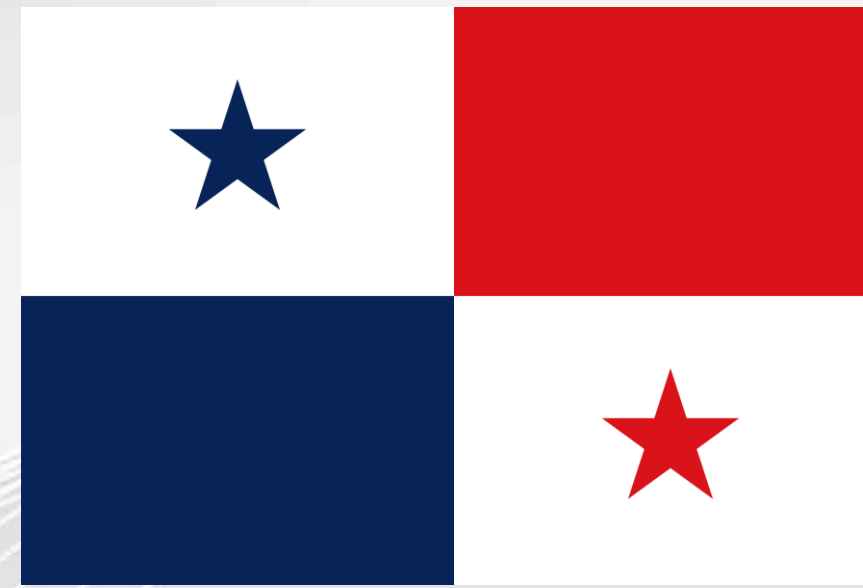
Ley No. 81, Protección de Datos Personales

Tiene por objeto establecer los principios, derechos, obligaciones y procedimientos que regulan la protección de datos personales, por parte de las personas naturales o jurídicas, de derecho público o privado, que procesen datos personales en los términos previstos en la norma.

La Autoridad tendrá como competencia el ejercicio pleno de todas la personas a su Derecho de Protección de Datos Personales en cualquiera de sus modalidades:

- Acceso: obtenerlos y conocer la finalidad y origen para los cuales fueron recabados,
- Rectificación: Acceder y solicitar corrección, modificación o actualización,
- Cancelación: Solicitar eliminación de datos,
- Oposición: Negarse a proporcionar o revocar su consentimiento,
- Portabilidad: Obtener una copia de los datos personales de manera estructurada en ciertas circunstancias

Panamá



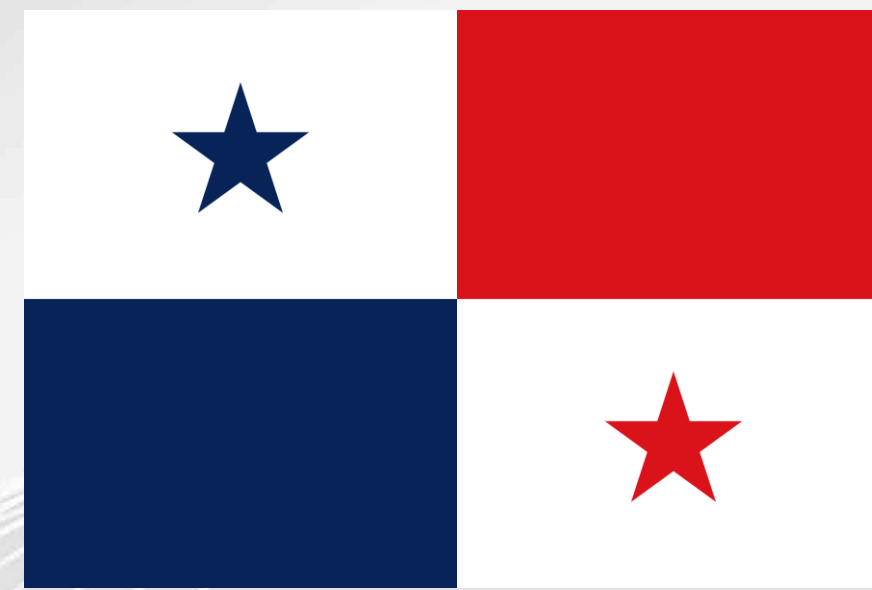
Observaciones

El organismo competente para el cumplimiento de las obligaciones es la Autoridad Nacional de Transparencia y Acceso a la Información (ANTAI), quien dará cumplimiento a la recién aprobada Ley No. 81 en materia de protección de Datos Personales.

Sanciones e indemnizaciones.

Este organismo está facultado para imponer sanciones, las cuales podrán oscilar entre los 1,000 Balboa/ Dólar y los 10,000 Balboa/Dólar dependiendo de la gravedad y recurrencia. Así mismo, podrá imponerse igualmente advertencia escrita, citación ante la ANTAI, clausura del registro de la base de datos o suspensión e inhabilitación de la actividad de almacenamiento y/o tratamiento de datos personales.

Panamá



Casos relevantes

Panama Papers.

En 2015 se gestó uno de los escándalos de la nueva era digital, se filtraron 11, 5 millones de documentos confidenciales que detallan las actividades bancarias de 214,000 de empresas que operan en el extranjero, a través de la firma panameña “Mossack Fonseca”

Se compartieron los documentos con el Consorcio Internacional de Periodistas de Investigación (ICIJ), que luego los distribuyó a cerca de 400 periodistas en 107 organizaciones de medios de comunicación en todo el mundo. los datos se guardaron por más de un año antes de que se publicaran los informes iniciales y el ICIJ prometió publicar una lista completa de las empresas involucradas en Mossack Fonseca en mayo de 2016.

Se generaron acusaciones de evasión de impuestos contra una serie de figuras públicas de alto rango.

Paraguay



Constitución

Artículo 33 – Del Derecho a la Intimidad.

La intimidad personal y familiar, así como el respeto a la vida privada, son inviolables. La conducta de las personas, en tanto no afecte al orden público establecido en la ley o a los derechos de terceros, está exenta de la autoridad pública. Se garantizan el derecho a la protección de la intimidad, de la dignidad y de la imagen privada de las personas.

Artículo 135 – Del Hábeas Data.

Toda persona puede acceder a la información y a los datos que sobre sí misma, o sobre sus bienes, obren en registros oficiales o privados de carácter público, así como conocer el uso que se haga de los mismos y de su finalidad. Podrá solicitar ante el magistrado competente la actualización, la rectificación o la destrucción de aquellos, si fuesen erróneos o afectaran ilegítimamente sus derechos.

Paraguay



Instituto Estatal de Transparencia, Acceso a la Información Pública
y Protección de Datos Personales
Organismo Público Autónomo

Normativa sobre protección de datos:

Ley N° 3440, de 16 de julio de 2008, que modifica varias disposiciones de la Ley N° 1160/97, Código Penal.

Ley N° 4439, de 3 de octubre de 2011, que modifica y amplía varios artículos de la Ley N° 1160/97, Código Penal.
Artículos 146 b; 146 c; 146 d; 174; 174 b; 175; 175 b y 188.

Ley N° 1682, de 16 de enero de 2001, que reglamenta la información de carácter privado.

Ley N° 1969, de 3 de septiembre de 2002, que modifica, amplía y deroga varios artículos de la Ley N° 1682.

Paraguay



Instituto Estatal de Transparencia, Acceso a la Información Pública
y Protección de Datos Personales
Organismo Público Autónomo

Ley N° 1969, de 3 de septiembre de 2002, que modifica, amplía y deroga varios artículos de la Ley N° 1682.

Ley N° 4017, de 23 de diciembre de 2010, de validez jurídica de la firma electrónica, la firma digital, los mensajes de datos y el expediente electrónico.

Decreto N° 7369, de 23 de septiembre de 2011, por el que se aprueba el Reglamento de la Ley N° 4017/10

Ley N° 4868, de 26 de febrero de 2013, de Comercio electrónico.

Decreto N° 1165, de 27 de enero de 2014, por el que se aprueba el Reglamento de la Ley N° 4868, de Comercio electrónico.

Ley N° 4989, de 9 de agosto de 2013, que crea el marco de aplicación de las tecnologías de la información y comunicación en el sector público y crea la Secretaría Nacional de Tecnologías de la Información y Comunicación (SENATICs).

Derechos digitales en España

Carta de Derechos Digitales

Marco de referencia para garantizar
derechos de la ciudadanía

Aumentar confianza ante los
cambios y y interrupciones de las
nuevas tecnologías.

Derechos de libertad

Derechos de igualdad

Derechos del entorno
específico

NEURODERECHOS

- Establecidos en la Carta de Derechos Digitales de España. Artículo 26
- Constitución de Chile
- Declaración del Comité Jurídico Interamericano sobre Neurociencia, Neurotecnologías y Derechos Humanos
- Artículo 3 de la Carta de los derechos fundamentales de la Unión Europea. Derecho a la integridad mental
- Propuesta de reglamento del Parlamento Europeo para establecer normas armonizadas en materia de inteligencia artificial

Finalidades de los neuroderechos

- Privacidad mental;
- Evitar la manipulación de ideas y pensamientos;
- Posibilidad de mejorar las capacidades mentales



Neuroderechos propuestos en el desarrollo del derecho internacional

- Formulación nueva y más reciente de los derechos humanos
- Derecho a la preservación de la identidad personal
- Derecho a la no interferencia en la libertad de decisión
- Derechos a la privacidad de la información cerebral
- Derecho a la equidad en el mejoramiento de la capacidad cerebral
- Derecho a la protección frente a los sesgos de algoritmos
- Necesaria para que la Inteligencia Artificial sea una herramienta en manos del individuo

California Consumer Privacy Act de 2020 (CCPA)

Multas a empresas de 7.500 dls por infracción
y 750 dls por usuario afectado.



- Información personal
- Identificadores directos
- Identificadores únicos
- Datos biométricos
- Datos de geo localización
- Actividad internauta
- Información sensible

Canadá:

- PIPEDA

Principios de la protección de datos

- Responsabilidad.
- Identificación de fines.
- Consentimiento.
- Recolección limitada.

Recomendaciones para proteger los datos personales en el entorno digital

- Higiene digital
- Elaboración de contraseñas para el acceso a los diversos servicios de internet
- Borrar nuestro historial de navegación en internet
- Revisión de los permisos que se otorgan a las aplicaciones que descargamos en nuestros dispositivos
- Verificación previa de los enlaces a páginas de internet