certiprof®

DATA PROTECTION GENERAL LAW FOUNDATION

LGPDF™ Versión 102021

DATA PROTECTION GENERAL LAW FOUNDATION LGPDF™

LGPDF™ Versión 102021

¿Quién es Certiprof®?

Certiprof® es una entidad certificadora fundada en los Estados Unidos en 2015, ubicada actualmente en Sunrise, Florida.

Nuestra filosofía se basa en la creación de conocimiento en comunidad y para ello su red colaborativa está conformada por:

- **Nuestros Lifelong Learners (LLL)** se identifican como Aprendices Continuos, lo que demuestra su compromiso inquebrantable con el aprendizaje permanente, que es de vital importancia en el mundo digital en constante cambio y expansión de hoy. Independientemente de si ganan o no el examen.
- Las universidades, centros de formación, y facilitadores en todo el mundo forman parte de nuestra red de aliados **ATPs (Authorized TrIAning Partners.)**
- **Los autores (co-creadores)** son expertos de la industria o practicantes que, con su conocimiento, desarrollan contenidos para la creación de nuevas certificaciones que respondan a las necesidades de la industria.
- **Personal Interno:** Nuestro equipo distribuido con operaciones en India, Brasil, Colombia y Estados Unidos está a cargo de superar obstáculos, encontrar soluciones y entregar resultados excepcionales.

Nuestras Afiliaciones

Memberships

itcc
IT CERTIFICATION COUNCIL

Agile Alliance®

ANSI MEMBER

Digital badges issued by

Credly
by Pearson

IT Certification Council - ITCC

Certiprof® es un miembro activo de ITCC.

Una de las ventajas de hacer parte del ITCC es como líderes del sector colaboran entre sí en un formato abierto para explorar maneras nuevas o diferentes formas de hacer negocios que inspiran y fomentan la innovación, estableciendo y compartiendo buenas prácticas que nos permiten extender ese conocimiento a nuestra comunidad.

Certiprof ha contribuido a la elaboración de documentos blancos en el Career Path Ways Taskforce, un grupo de trabajo que se implementó internamente para ofrecer a los estudiantes la oportunidad de saber qué camino tomar después de una certificación.

Algunos de los miembros del ITCC

- **IBM**
- **CISCO**
- **ADOBE**
- **AWS**
- **SAP**
- **GOOGLE**
- **ISACA**

Agile Alliance

Certiprof® es un miembro corporativo de Agile Alliance.

Al unirnos al programa corporativo Agile Alliance, continuamos empoderando a las personas ayudándolas a alcanzar su potencial a través de la educación. Cada día, brindamos más herramientas y recursos que permiten a nuestros socios formar profesionales que buscan mejorar su desarrollo profesional y sus habilidades.

https://www.agilealliance.org/organizations/certiprof/

Credly

Esta alianza permite que las personas y empresas certificadas con Certiprof® cuenten con una distinción a nivel mundial a través de un distintivo digital.

Credly es el emisor de insignias más importante del mundo y empresas líderes en tecnología como IBM, Microsoft, PMI,Nokia, la Universidad de Stanford, entre otras, emiten sus insignias con Credly.

Empresas que emiten insignias de validación de conocimiento con Credly:

- **IBM**
- **Microsoft**
- **PMI**
- **Universidad de Stanford**
- **Certiprof**

Insignias Digitales

Insignias Digitales:
¿Qué Son?

- Según el estudio del IT Certification Council (ITCC), años atrás, la gente sabía muy poco sobre las insignias digitales. Hoy, grandes empresas e instituciones educativas de todo el mundo expiden insignias.

- Las insignias digitales contienen metadatos detallados sobre quién las ha obtenido, las competencias requeridas y la organización que las ha expedido. Algunas insignias incluso están vinculadas a las actividades necesarias para obtenerlas.

- Para las empresas e instituciones educativas, las insignias y la información que proporcionan son tan importantes que muchas decisiones, como las de contratación o admisión, se basan en los datos que aportan.

¿Por qué son importantes?

- **Facilidad de Compartir y Verificar Logros:**

  - Las insignias digitales permiten a los profesionales mostrar y verificar sus logros de manera instantánea y global. Según un informe de Credly, **los perfiles de LinkedIn con insignias digitales reciben un 40% más de atención por parte de reclutadores y empleadores.**

- **Visibilidad en Plataformas Digitales:**

  En una encuesta realizada por Pearson y Credly, el **85%** de los usuarios que obtuvieron insignias digitales **las compartieron en LinkedIn,** y el **75%** reportó que esto mejoró su **credibilidad profesional en sus redes.** Además, el **76%** de los empleadores encuestados afirmó que las insignias digitales les ayudan a identificar rápidamente habilidades específicas.

¿Por qué son importantes?

- **Impacto en la Contratación:**

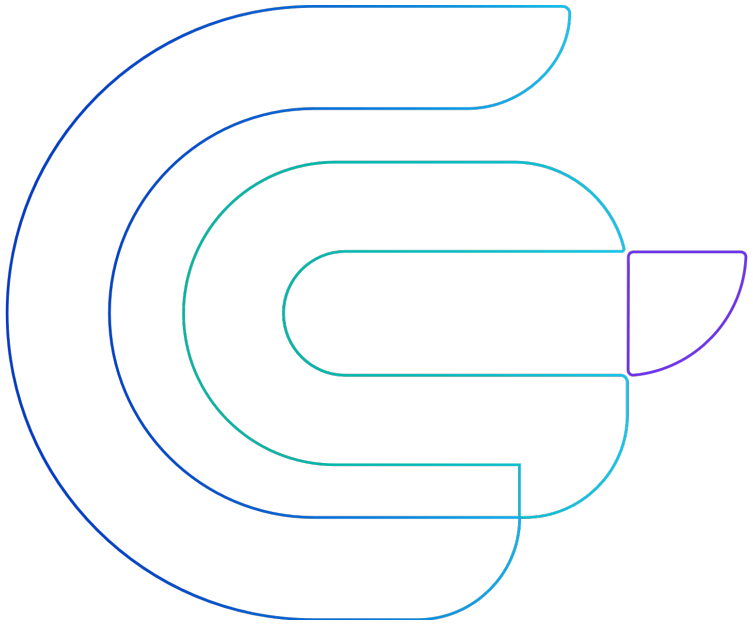
  Un estudio de la **Asociación Internacional de Gestión de Proyectos (PMI)** encontró que los candidatos que muestran insignias digitales de gestión de proyectos tienen **un 60%** más de probabilidades de ser contratados en comparación con aquellos que solo mencionan sus habilidades sin verificación digital.

¿Por qué son importantes?

- **Empoderamiento de la Marca Personal:**

La visibilidad y verificación instantánea proporcionada por las insignias digitales permiten a los profesionales no solo demostrar sus habilidades, sino también construir una marca personal fuerte. Según un estudio de LinkedIn, los profesionales que utilizan insignias digitales tienen un 24% más de probabilidades de avanzar en sus carreras.

La certificación y las insignias digitales no son solo una validación del conocimiento, sino también una herramienta poderosa para la mejora continua y la empleabilidad. En un mundo donde el aprendizaje permanente se ha convertido en la norma, estas credenciales son clave para el desarrollo profesional y la competitividad en el mercado laboral global.



- No todas las insignias son iguales, y en **Certiprof,** estamos comprometidos con ofrecerte más que un simple reconocimiento digital. Al obtener una insignia emitida por certiprof, estarás recibiendo una validación de tu conocimiento respaldada por una de las entidades líderes en certificación profesional a nivel mundial.

- **Da el siguiente paso y obtén la insignia que te abrirá puertas y te posicionará como un experto en tu campo.**

¿Por qué es importante obtener su certificado?

- **Prueba de experiencia:** Su certificado es un reconocimiento formal de las habilidades y conocimientos que ha adquirido. Sirve como prueba verificable de sus cualificaciones y demuestra su compromiso con la excelencia en su campo.

- **Credibilidad y reconocimiento:** En el competitivo mercado laboral actual, las empresas y los compañeros valoran las credenciales que le distinguen de los demás. Un certificado de una institución reconocida, como Certiprof, proporciona credibilidad instantánea e impulsa su reputación profesional.

- **Avance profesional:** Tener tu certificado puede abrirte las puertas a nuevas oportunidades. Ya se trate de un ascenso, un aumento de sueldo o un nuevo puesto de trabajo, las certificaciones son un factor diferenciador clave que los empleadores tienen en cuenta a la hora de evaluar a los candidatos.

¿Por qué es importante obtener su certificado?

- **Oportunidades de establecer contactos:** Poseer un certificado le conecta con una red de profesionales certificados. Muchas organizaciones cuentan con grupos de antiguos alumnos o de trabajo en red en los que puede compartir experiencias, intercambiar ideas y ampliar su círculo profesional.

- **Logro personal:** Obtener una certificación es un logro importante, y su certificado es un recordatorio tangible del trabajo duro, la dedicación y el progreso que ha realizado. Es algo de lo que puede sentirse orgulloso y mostrar a los demás.

Insignia

Earn this Badge

Data Protection General Law Foundation - LGPDF™

Issued by Certiprof

The holder of this badge has validated his skills and knowledge in Data Protection General Law Foundation. They show a broad familiarization with the law that provides the processing of personal data, even in digital media, by a natural or legal person under public or private law. They have shown that they have in-depth knowledge of the law and its impact on institutions, users, and society.

Learn more

Certification | $ Paid

Skills

Foundation | General Data Protection Law | Governance | Information Technology

https://www.credly.com/org/certiprof/badge/data-protection-general-law-foundation-lgpdf

Aprendizaje Permanente

- Certiprof ha creado una insignia especial para reconocer a los aprendices constantes.
- Para el 2024, se han emitido más de 1,000,000 de estas insignias en más de 11 idiomas.

Propósito y Filosofía

- Esta insignia está destinada a personas que creen firmemente en que la educación puede cambiar vidas y transformar el mundo.
- La filosofía detrás de la insignia es promover el compromiso con el aprendizaje continuo a lo largo de la vida.

Acceso y Obtención de la Insignia

- La insignia de Lifelong Learning se entrega sin costo a aquellos que se identifican con este enfoque de aprendizaje.
- Cualquier persona que se considere un aprendiz constante puede reclamar su insignia visitando:

https://certiprof.com/pages/certiprof-lifelong-learning

Agradecimientos Especiales

DATA GOVERNANCE LATAM

Daniel Monastersky | Adaptación y revisión LGPDF en español

Abogado. Se especializa en delitos informáticos, robo de identidad, reputación online y datos personales. DPO Certificado en España. Cuenta con un Certificate en Gestión y estrategias de la Ciberseguridad de la Universidad Internacional de Florida (FIU), Estados Unidos. Fue uno de los miembros del Advisory Board del Global Forum on Cyber Expertise, iniciativa liderada por el Consejo de Europa y la OEA.

Socio Fundador Data Governance LATAM, consultora especializada en privacy.

Director del CECIB, el Centro de Estudios en Ciberseguridad y Protección de Datos Personales de la Universidad del CEMA. Recientemente fue elegido como uno de los 20 influencers, de habla hispana, que considera más destacados en ciberseguridad. Entre los elegidos hay expertos informáticos dedicados a consultoría o auditoría, así como abogados y periodistas, entre otras especialidades.

Agradecimientos Especiales

Facundo Malaureille | Adaptación y revisión LGPDF en español

Abogado UCA.

MBA IAE Business School, Leadership Professional in Ethics & Compliance (LPEC) Certification Candidate, ECI and IAE Compliance, IAE Business School.

Data Protection Officer (DPO) Francisco de Vittoria-Wolters Kluvers.

Socio Fundador Data Governance LATAM, consultora especializada en Privacy, Data Governance. Data Governance VP en illow.

Director de la Diplomatura en “Data Governance” de UCEMA.

COMPARTE Y VERIFICA TUS LOGROS DE APRENDIZAJE FÁCILMENTE

#LGPDF #certiprof

certiprof®

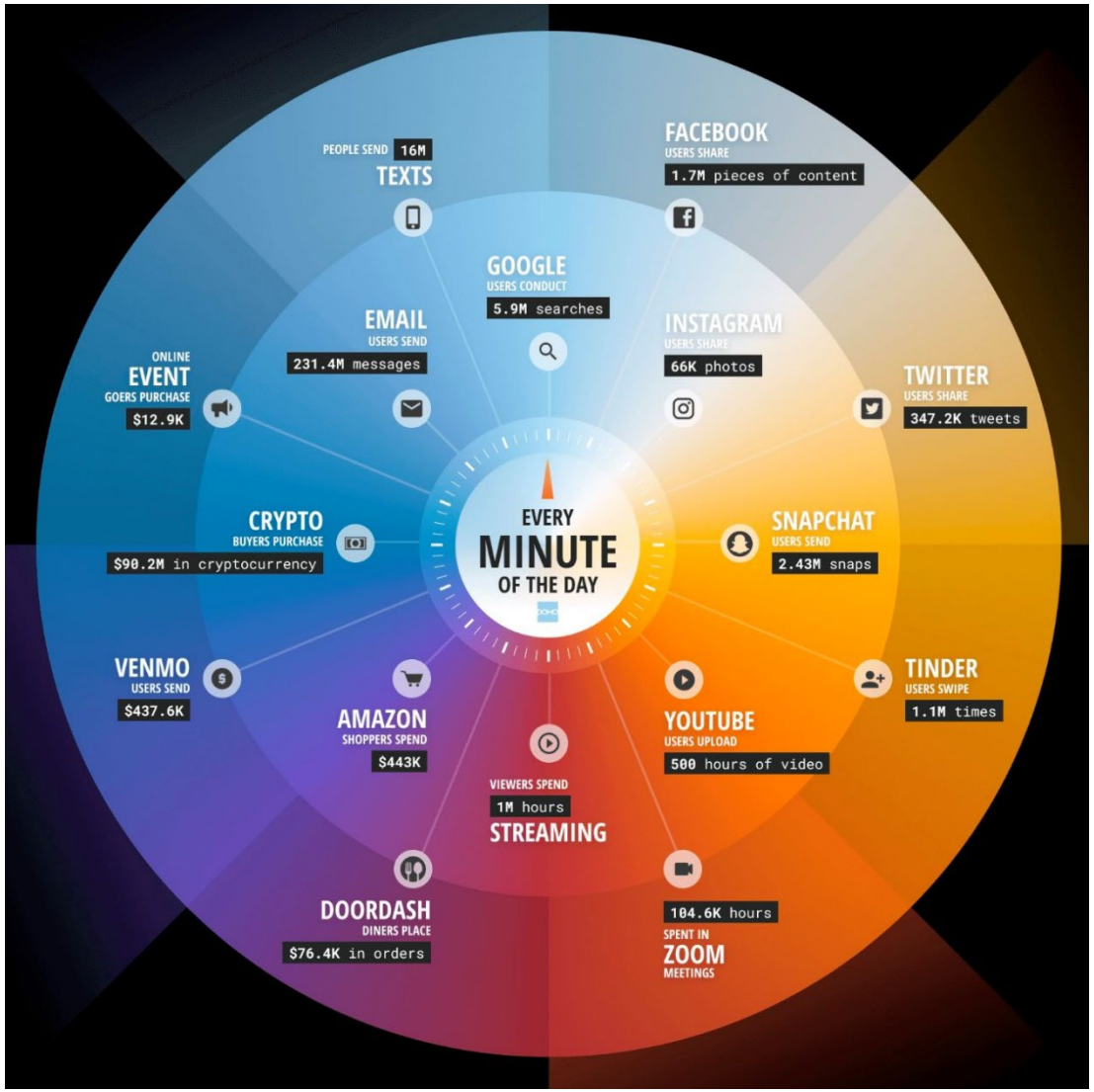
Módulo 1: Contextualización

LGPDF™ Versión 102021

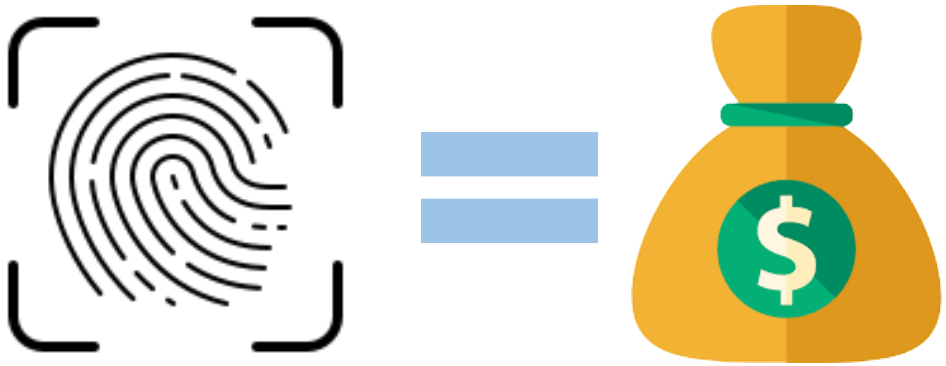
¿Qué es la privacidad de los datos?

- Es la capacidad de una persona para controlar la exposición y la disponibilidad de información sobre sí misma (Diccionario Informal)
- Condición de lo que es privado, personal, íntimo (Diccionario Priberam)
- Es el derecho al respeto de la vida privada de una persona, en su familia y correspondencia
- Dependerá de cómo se recopilen, almacenen y compartan los datos con terceros, además del cumplimiento de las leyes de privacidad aplicables

¿Qué pasa en 1 minuto de internet?



Los Datos Personales son una Moneda de Cambio



La aplicación FaceApp se convirtió en una gran sensación cuando se lanzó, lo que llevó a millones de personas en todo el mundo a usar la tecnología de reconocimiento facial para mostrar a sus amigos cómo se verían si fueran mayores o más jóvenes. Sin embargo, ha habido muchas sospechas de robo de datos a través de esta aplicación.

"Cuando no pagas por algo en el mundo digital, eres la mercancía".

¿Por qué la privacidad es importante para todos?

1. Límite de poder: Cuanto más sabe alguien sobre nosotros, más poder puede tener sobre nosotros. Es apropiado limitar el poder que las empresas pueden tener sobre nosotros
2. Respeto por las personas: La privacidad es respetar a las personas. Si una persona tiene el deseo de mantener algo confidencial, es irrespetuoso ignorar sus deseos sin una razón convincente
3. Gestión de la reputación: La privacidad nos permite gestionar nuestra reputación. La forma en que somos juzgados por los demás afecta nuestras oportunidades, amistades y bienestar general
4. Mantenimiento de las limitaciones sociales: Las personas establecen límites a los demás en la sociedad. Estos límites son físicos e informativos. Por ejemplo, nadie necesita saber dónde estamos en todo momento
5. Confianza: En las relaciones, ya sean personales, profesionales, gubernamentales o empresariales, dependemos de confiar en la otra parte. Las violaciones de confidencialidad son violaciones de esta confianza. ¿Confiaría en una empresa que promete usar sus datos para un propósito y usarlos para otro?

¿Por qué la privacidad es importante para todos?

6. Control sobre nuestras vidas: Sin saber qué datos se están utilizando, cómo se están utilizando, la capacidad de corregirlos y cambiarlos, estamos prácticamente fuera de lugar en el mundo de hoy
7. Libertad de pensamiento y de expresión: La privacidad es la clave de la libertad de pensamiento. Una mirada cercana a todo lo que leemos o vemos puede impedirnos explorar otros pensamientos
8. Libertad de actividades políticas y sociales: La privacidad ayuda a proteger nuestra capacidad de asociarnos con otros y participar en actividades políticas
9. No tener que explicarte ni justificarte: Puede ser demasiado pesado si tenemos que pensar en cómo todo lo que hacemos será percibido por los demás y que tendremos que estar preparados para explicar situaciones embarazosas
10. Capacidad para cambiar y tener segundas oportunidades: Las personas están en constante evolución; cambiamos y crecemos a lo largo de nuestras vidas. Hay un gran valor en la capacidad de tener una segunda oportunidad, de poder aprender del error, de poder reinventarse. ¿Es justo que una persona sea juzgada eternamente por algún comentario publicado en una red social?

La Exposición a Datos Sensibles es uno de los Principales Riesgos

OWASP es una organización sin fines de lucro y fue fundada en los EE. UU. en 2004

La organización realizó una encuesta colaborativa global de los 10 riesgos de seguridad web más críticos conocidos como OWASP TOP 10 2022.

1 - Pérdida del control de acceso (*Broken Access Control*)
2 - Fallos criptográficos (*Cryptographic Failures*)
3 - Inyección (*Injection*)
4 - Diseño inseguro (*Insecure Design*)
5 - Configuración de seguridad defectuosa (*Security Misconfiguration*)
6 - Componentes vulnerables y obsoletos (*Vulnerable and Outdated Components*)
7 - Fallos de identificación y autenticación (*Identification and Authentication Failures*)
8 - Fallos en el software y en la integridad de los datos (*Software and Data Integrity Failures*)
9 - Fallos en el registro y la supervisión de la seguridad (*Security Logging and Monitoring Failures*)
10 - Falsificación de Solicitud del Lado del Servidor (*Server-side Request Forguery o SSRF*)

La Privacidad de los Datos no es lo Mismo que la Seguridad de los Datos

Seguridad de los datos ≠ **Privacidad de datos**

La seguridad de los datos se refiere a los medios de protección que una organización está adoptando para evitar que terceros no autorizados accedan a sus datos.
Se centra en proteger los datos de ataques maliciosos y evita la explotación de datos (violación de datos o ciberataque).
Incluye controles de acceso, cifrado, seguridad de red, etc.

La privacidad de los datos se centra en los derechos de las personas, el propósito de la recopilación y el procesamiento de datos, las preferencias de privacidad y cómo las organizaciones controlan los datos personales de los interesados.
Se centra en cómo recopilar, procesar, compartir, archivar y eliminar datos de acuerdo con la ley.

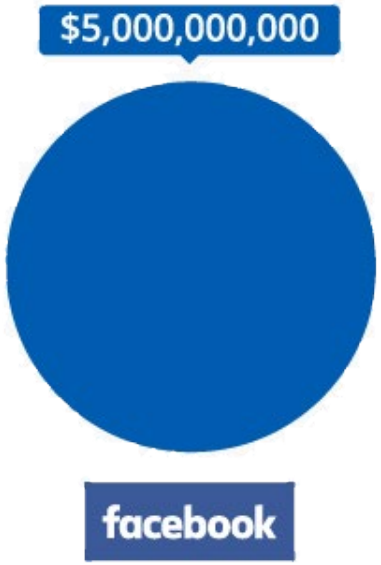
¿Qué necesitan aprender las empresas?

- En la era del ahorro de datos, el verdadero valor de la empresa radica en los datos recopilados del cliente
- Esto significa que los datos son un activo digno de protección y mantenimiento
- Los datos personales de las personas procesadas por las empresas solo se toman prestados, no son propiedad de las empresas
- Para que las empresas mantengan los datos y sigan la confianza, tendrán que demostrar transparencia, comunicando abiertamente qué datos recopilan, para qué fines, quién es su procesador de datos, etc

Consecuencias del Incumplimiento

- Es demasiado arriesgado para las empresas no cumplir con las leyes de privacidad
- Las empresas corren el riesgo de multas y demandas, sin mencionar la pérdida de reputación y lealtad del cliente

Algunas de las multas más grandes jamás impuestas hasta la fecha



Multa establecida por el Departamento de Protección al Consumidor de los Estados Unidos por no haber respondido a una solicitud de protección de la privacidad del cliente en 2012.

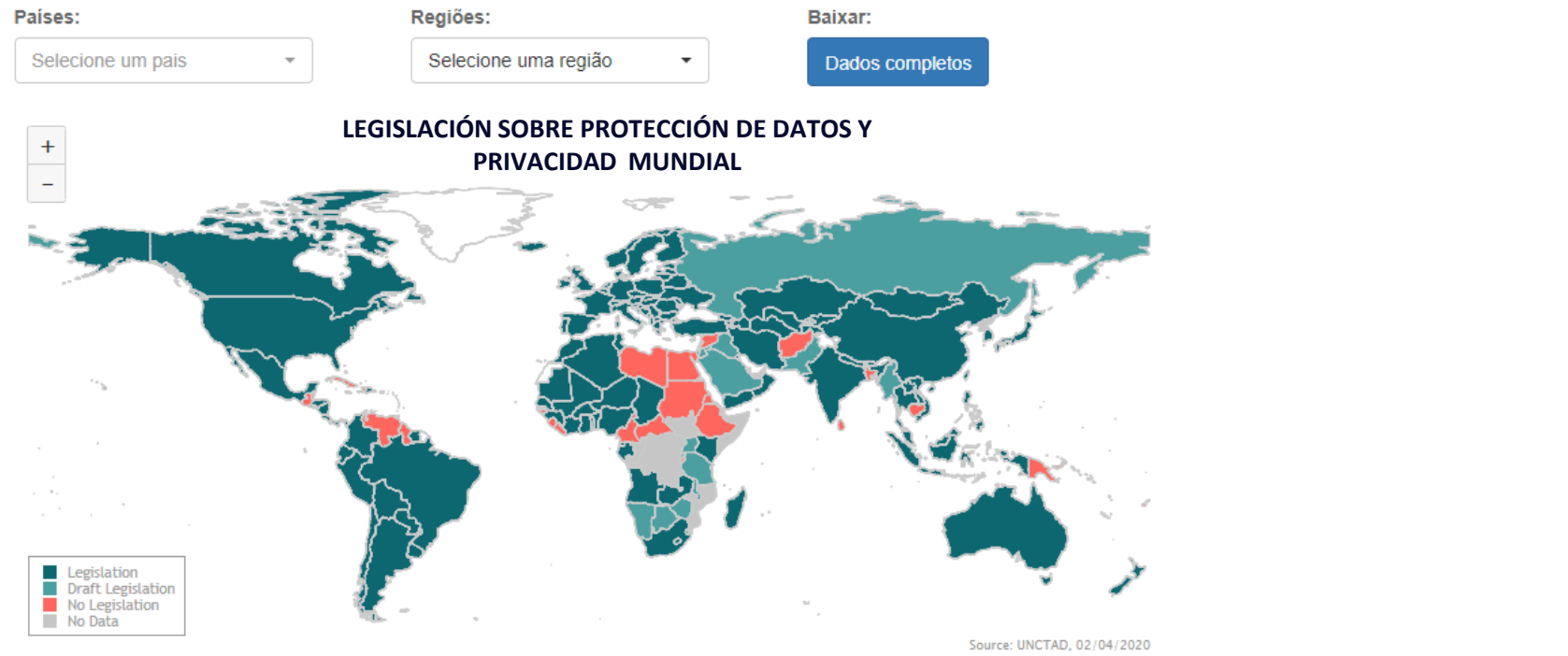
Violación de datos que afectó a 147 millones de clientes en 2017.

Violación de datos que afectó a 500,000 clientes en 2018.

Violación de datos que afectó a 57 millones de clientes en 2016.

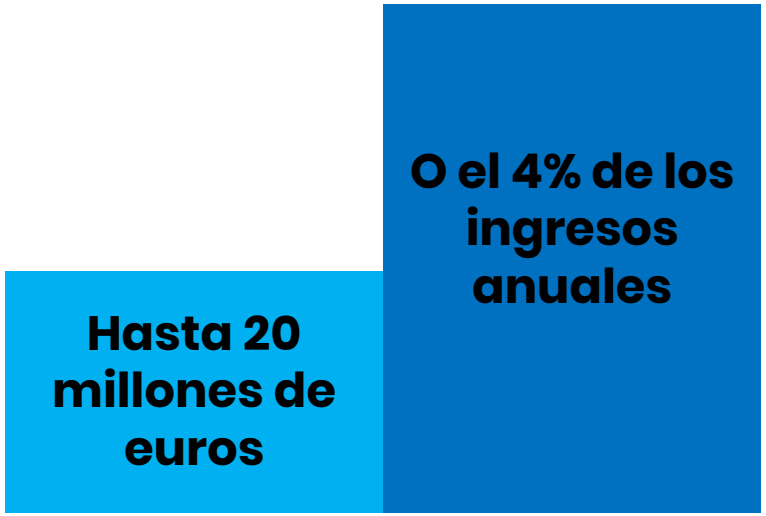
Cada Vez Hay Más Regulaciones de Privacidad en Todo el Mundo

66%	10%	19%	5%
PAÍSES CON LEGISLACIÓN	PAÍSES CON PROYECTO DE LEY	PAÍSES SIN LEGISLACIÓN	PAÍSES SIN DATOS



Fuente: https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Data-Protection-Laws.aspx

Multas – GDPR y LGPD



GDPR

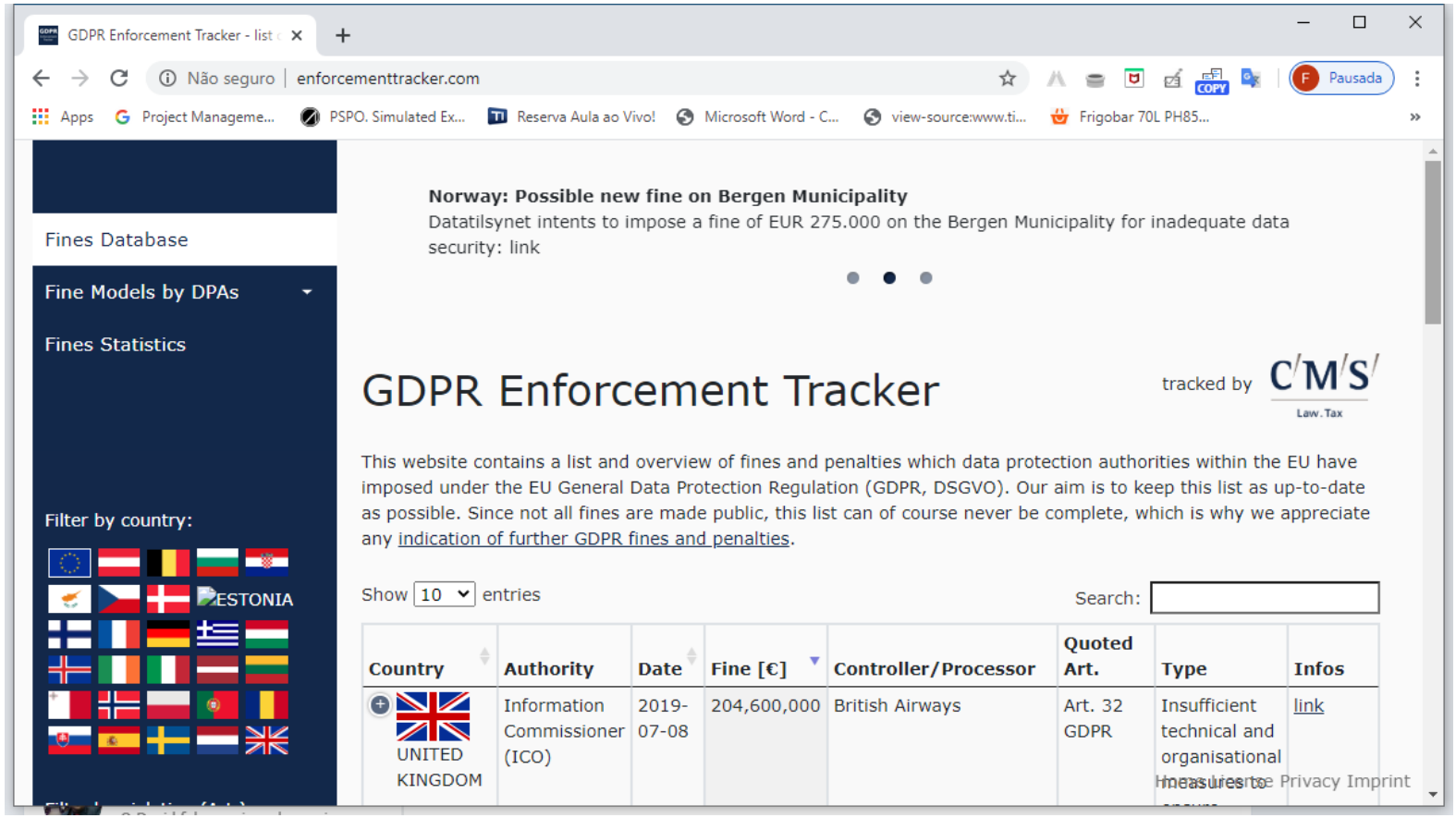
LGPD

Multas Aplicadas con Base en GDPR (2020)

Multas Aplicadas con Base en GDPR (2020)

#	Empresa	Importe	País	Artículo	Infracción
1	Amazon	746 millones de euros	Luxemburgo	Datos no disponibles	Incumplimiento del procesamiento de datos personales de conformidad con el GDPR.
2	Whatsapp	225 millones de euros	Irlanda	5,12,13,14	Incumplimiento de los requisitos de transparencia del GDPR hacia los usuarios y amonestación y orden de adecuación de su tratamiento.
3	Notebooksbilliger.de	10,4 millones de euros	Alemania	5,6	Base jurídica insuficiente para el tratamiento de datos. El video de la empresa monitoreó a sus empleados durante al menos dos años sin tener una base legal para hacerlo.
4	Austrian Post	9,5 millones de euros	Austria	Datos no disponibles	No permitir que las personas realicen consultas sobre los datos personales almacenados por correo electrónico.
5	Vodafone España	8,15 millones	España	21, 24, 28, 44, 48	Infracciones en materia de marketing y prospección a través de comunicaciones telefónicas y electrónicas; medidas sin autorización previa por escrito, procesamiento de datos a pesar de las objeciones del interesado.

¿Dónde consultar las multas aplicadas en función del RGPD?



Fuente: https://www.enforcementtracker.com/

¿Dónde consultar las multas aplicadas en base a la LGPD?

Fuente: https://anppd.org/violacoes

La Ley General de Protección de Datos Personales (LGPD) Ley Federal Nº 13.709/2018

Regulación
el uso, la protección y la transferencia de datos personales de personas naturales (personas físicas).

Violaciones
desde la suspensión de las actividades de recolección de datos personales hasta multas de hasta R USD 9,5M

Aprobado en 2018

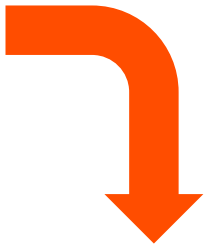
Inspirado en GDPR.

Obliga a todas las empresas a invertir en ciberseguridad e implementar sistemas de cumplimiento efectivos para prevenir, identificar y mitigar las violaciones de datos personales de los clientes.

Requiere el nombramiento de un responsable.

¿Dónde acceder a la LGPD?

Disponible en línea

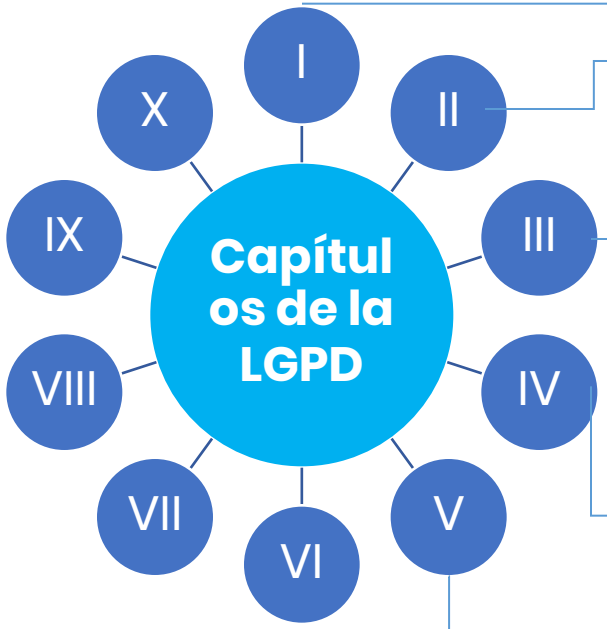


http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm

Módulo 2: Introducción a la LGPD y Fundamentos

LGPDF™ Versión 102021

Estructura de la LGPD



CAPÍTULO I – DISPOSICIONES PRELIMINARES

Artículos 1 al 6 (definiciones, aplicabilidad)

CAPÍTULO II – DEL TRATAMENTO DE DATOS PERSONALES

Artículos 7 al 16
Sección– De los Requisitos para el Tratamiento de Datos Personales – Artículos 7 al 10
Sección II - Del Tratamiento de Datos Personales Sensibles – Artículos 11 a 13
Sección III - Del Tratamiento de Datos Personales de Niños y Adolescentes – Artículo 14
Sección IV - De la Terminación de Tratamiento de Datos – Artículos 15 y 16

CAPÍTULO III – DE LOS DERECHOS DE LOS TITULARES

Articulos 17 al 22

CAPÍTULO IV – DEL TRATAMIENTO DE DATOS PERSONALES POR EL PODER PÚBLICO

Artículos 23 al 32
Sección I - Las Normas – Artículos 23 al 30
Sección II - De Responsabilidades – Artículos 31 al 32

CAPÍTULO V – DE LA TRANSFERENCIA INTERNACIONAL DE DATOS

Artículos 33 al 36

Estructura de la LGPD

CAPÍTULO X – DISPOSICIONES FINALES Y TRANSITORIAS

Artículos 60 al 65

CAPÍTULO IX – DE LA AUTORIDAD NACIONAL DE PROTECCION DE DATOS (ANPD) Y DEL CONSEJO NACIONAL DE PROTECCIÓN DE DATOS PERSONALES Y DE PRIVACIDAD

Artículos 55-A al 58-B
Sección I - De la Autoridad Nacional de Protección de Datos (ANPD) – Artículos 55-A al 55-L
Sección II - De Consejo Nacional de Protección de Datos Personales y de Privacidad – Artículos 58-A al 58-B

CAPÍTULO VIII – Del Control

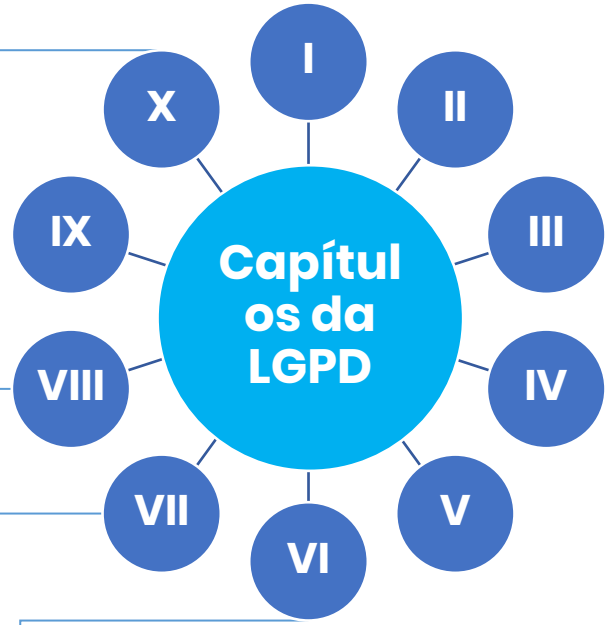
Sección - Sanciones Administrativas – Artículos 52 al 54

CAPÍTULO VII – DE SEGURIDAD Y BUENAS PRÁCTICAS

Artículos 46 al 51
Sección I - De Seguridad y Cuidado de datos – Artículos 46 al 49
Sección II - De Buenas prácticas y de Gobierno de datos – Artículos 50 al 5

CAPÍTULO VI – LOS AGENTES DE TRATAMIENTO DE DATOS PERSONALES

Artículos 37 al 45 Sección I - De Controlador y del Operador – Artículos 37 al 40
Sección II - Del Delegado del Protección de Datos Personales – Artículo 41 Sección III - De la Responsabilidad y el Resarcimiento de Daños – Artículos 42 al 45



Objeto de la LGPD

Artículo 1. Esta Ley prevé el tratamiento de datos personales, incluso en medios digitales, por una persona física o por una entidad 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.

Párrafo único. Las normas generales contenidas en esta Ley son de interés nacional y deben ser observadas por la Unión, los Estados, el Distrito Federal y los Municipios.

Palabras-clave en la LGPD

Fundamentos

Artículo 2. La disciplina de la protección de datos personales se basa en:

1. Respeto a la privacidad
2. Autodeterminación informativa
3. Libertad de expresión, información, comunicación y opinión
4. La inviolabilidad de la intimidad, el honor y la imagen
5. Desarrollo e innovación económica y tecnológica
6. Libre empresa, libre competencia y protección del consumidor
7. Los derechos humanos, el libre desarrollo de la personalidad, la dignidad y el ejercicio de la ciudadanía por las personas físicas

Ámbito Territorial

Artículo 3. La presente Ley se aplica a cualquier operación de tratamiento realizada por una persona natural o por una persona jurídica de derecho público o privado, independientemente del medio, el país de su sede social o el país donde se encuentren los datos, siempre que:

I - la operación de transformación se realiza en el territorio nacional

II - la finalidad de la actividad de tratamiento es ofrecer o suministrar bienes o servicios o tratar datos de personas físicas ubicadas en el territorio nacional

III - los datos personales tratados han sido recabados en el territorio nacional.

Ámbito Territorial

Artículo. 3º, III § 1º Los datos personales cuyo titular se encuentre presente en el momento de la recogida se consideran recogidos en el territorio nacional.

¿Cuándo no se aplica la LGPD?

Artículo 4. Esta Ley no se aplica al tratamiento de datos personales:

1. Realizado por una persona natural con fines exclusivamente privados y no económicos.
El artículo 3, apartado 2, segundo guión, de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, debe interpretarse en el sentido de que el funcionamiento de un sistema de cámaras que da lugar a una grabación de vídeo de personas, almacenado en un dispositivo de registro continuo, como un disco duro, un sistema instalado por una persona natural en su hogar familiar, para proteger la propiedad, la salud y la vida de los propietarios de esa casa, y que también monitorea el espacio público, no constituye un procesamiento de datos realizado en el ejercicio de actividades exclusivamente personales o domésticas, en el sentido de esta disposición.

(Fuente: Tribunal de Justicia (Sala Cuarta), de 11 de diciembre de 2014, asunto C-212/13, https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A62013CJ0212)

¿Cuándo no se aplica la LGPD?

2. Realizado para fines exclusivamente:

a) Periodístico y artístico.
b) Académicos, aplicando a esta hipótesis las artículos 7° y 11° de esta Ley.

3. Realizado con los fines exclusivos de:

a) Seguridad pública.
b) Defensa nacional.
c) Seguridad del Estado.
d) Actividades de investigación y enjuiciamiento de delitos penales.

4. Provenientes de fuera del territorio nacional y no objeto de comunicación, uso compartido de datos con agentes brasileños o sujetos de transferencia internacional de datos con un país distinto de la procedencia, siempre que el país de procedencia proporcione un grado de protección de datos personales adecuado a las disposiciones de esta Ley.

Palabras-clave en LGPD

Artículo 5. A los efectos de la presente Ley:

I. Datos personales: Información relacionada con una persona natural identificada o identificable.
II. Datos personales sensibles: Datos personales sobre origen racial o étnico, convicciones religiosas, opiniones políticas, afiliación a un sindicato u organización de carácter religioso, filosófico o político, datos relativos a la salud o la vida sexual, datos genéticos o biométricos, cuando estén vinculados a una persona física.
III. Base de datos: Conjunto estructurado de datos personales, establecido en una o más ubicaciones, en soporte electrónico o físico.

Palabras-clave en LGPD

Información personal:
Para efectos del Decreto Nº 10.046/2019 (Registro de Base Ciudadana y Comité Central de Gobernanza de Datos) se considera:

1. Atributos biográficos: Datos de personas natural relacionados con los hechos de su vida, como nombre civil o social, fecha de nacimiento, afiliación, naturalidad, nacionalidad, sexo, estado civil, grupo familiar, dirección y relaciones laborales.
2. Atributos biométricos: Características biológicas y de comportamiento medibles de la persona natural que se pueden recopilar para el reconocimiento automatizado, como huellas dactilares de la palma de la mano, los dedos, la retina o el iris de los ojos, la forma de la cara, la voz y la forma de caminar.

Palabras-clave en LGPD

3. Datos de registro- información de identificación ante los registros de organismos públicos, tales como:

a) El número de inscripción en el Registro de Personas - CPF
b) El número de inscripción en el Registro Nacional de Personas Jurídicas - CNPJ
c) Otros datos públicos relativos a la entidad jurídica o a la empresa individual

4. Atributos genéticos - características hereditarias de la persona natural, obtenidas por análisis de ácidos nucleicos u otros análisis científicos (...)

Artículo 5. A los efectos de la presente Ley, se considera.

IV. Datos anonimizados: Datos relativos a un titular que no puede ser identificado, teniendo en cuenta el uso de medios técnicos razonables disponibles en el momento de su tratamiento.
V. Anonimización: Uso de medios técnicos razonables disponibles en el momento del tratamiento, a través de los cuales un dato pierde la posibilidad de asociación, directa o indirectamente, con un individuo (+ art. 12)

Palabras-clave en LGPD

VI. Titular: Persona natural a la que se refieren los datos personales que se tratan.

VII. Controlador: Persona natural o jurídica, de Derecho público o privado, a la que se refieren las decisiones relativas al tratamiento de datos personales.

VIII. Operador: Persona natural o jurídica, de derecho público o privado, que lleva a cabo el tratamiento de datos personales en nombre del responsable del tratamiento.

IX. Agentes de tratamiento: Controlador y operador

Persona designada por el controlador y el operador para actuar como un canal de comunicación entre el controlador, los interesados y la Autoridad Nacional de Protección de Datos (ANPD).

Nota: Art. 41, párr. 4: se eliminó la necesidad de conocimientos jurídicos y técnicos del responsable de la protección de datos personales, pero en la práctica se identifica la obligación.

Palabras-clave en LGPD

Información (nombre)	Anonimizado
Peter	*****
Annabelle	******
Mark	*****
Elizabeth	******
Mark	******
Annabelle	******

Se trata de datos personales convertidos en datos no identificables, cuyo proceso de anonimización no puede ser reversible.

Palabras-clave en LGPD

XII. Consentimiento: Manifestación libre, informada e inequívoca mediante la cual el titular acepta el tratamiento de sus datos personales para una finalidad específica.
XIII. Bloqueo: Suspensión temporal de cualquier operación de procesamiento, sujeta a la custodia de los datos personales o la base de datos.
XIV. Eliminación: Eliminación de datos o conjuntos de datos almacenados en la base de datos, independientemente del procedimiento empleado.
XV. Transferencia internacional de datos: Transferencia de datos personales a un país extranjero u organismo internacional del que el país sea miembro.
XVI. Uso compartido de datos: Comunicación, difusión, transferencia internacional, interconexión de datos personales o tratamiento compartido de bases de datos personales por parte de organismos y entidades públicas en cumplimiento de sus competencias legales, o entre éstos y entidades privadas, recíprocamente, con autorización específica, para una o más modalidades de tratamiento permitidas por estas entidades públicas, o entre entidades privadas.
XVII. Informe de impacto de la protección de datos personales: Documentación del responsable del tratamiento que contiene una descripción de los procesos de tratamiento de datos personales que pueden crear riesgos para las libertades civiles y los derechos fundamentales, así como medidas, salvaguardias y mecanismos de mitigación de riesgos.

Palabras-clave en LGPD

XVIII. **Organismo de investigación:** Organismo o entidad de la administración pública directa o indirecta o entidad privada de derecho privado sin fines de lucro legalmente constituida bajo las leyes brasileñas, con domicilio social y foro en el país, que incluye en su misión institucional o en su objetivo social o estatutario la investigación básica o aplicada de carácter histórico, científico, tecnológico o estadístico.

XIX. **Autoridad nacional:** Organismo de la administración pública encargado de velar, implementar y supervisar el cumplimiento de la presente Ley en todo el territorio nacional.

Principios

Artículo 6. Las actividades de procesamiento de datos personales deben cumplir con la buena fe y los siguientes principios:

I FINALIDAD	II ADECUACIÓN	III NECESIDAD	IV LIBRE ACCESO	V CALIDAD DE DATOS
VI TRANSPARENCIA	VII SEGURIDAD	VIII PREVENCIÓN	IX NO DISCRIMINACIÓN	X RESPONSABILIDAD

Principios

Para Miguel Reale, el legislador, al redactar la ley, reconoce que el "sistema de leyes no es capaz de abarcar todo el campo de la experiencia humana, quedando siempre un gran número de situaciones imprevistas, algo que era imposible de imaginar".

Para estas deficiencias del derecho, "existe la posibilidad de recurrir a los principios generales del derecho, pero hay que advertir que no sólo son responsables de llenar o llenar los vacíos en la legislación" (1998, p. 306).
(REALE, Miguel. Lecciones preliminares de derecho. 24. ed. São Paulo: Saraiva, 1998.

CUNHA, Guilherme Bohrer Lopes. La situación actual de la teoría de principios en Brasil. Jus Navigandi Magazine, ISSN 1518-4862, Teresina, año 15, n. 2410, 5 de febrero. 2010. Disponible en: https://jus.com.br/artigos/14289. Acceso: Jun 12. 2020).

Principios

“Violar un principio es mucho más grave que romper cualquier regla. La falta de atención al principio implica ofender no solo a un mandamiento obligatorio específico, sino a todo el sistema de comando. Es la forma más grave de ilegalidad o inconstitucionalidad, según el rango del principio alcanzado, porque representa la insurgencia contra todo el sistema, la subversión de sus valores fundamentales, la contumelia irremisible a su marco lógico y la corrosión de su estructura maestra. Esto se debe a que, con la ofensa de él, se bajan las vigas que las sostienen y se alude a toda la estructura".

(MELLO, Celso Antônio Bandeira de, Curso de Derecho Administrativo. 12ª ed. – São Paulo : Malheiros, 2000, p. 747/748.)

Principios y la Declaración de Adecuación de la LGPD

Artículo 49. Los sistemas utilizados para el tratamiento de datos personales se estructurarán de manera que respondan:

- Requisitos de seguridad
- A las normas de buenas prácticas y gobernanza
- Los principios generales establecidos en esta Ley y en las demás normas reglamentarias

Principios

1. **Finalidad:** Tratamiento con fines legítimos, específicos, explícitos e informados para el titular, sin posibilidad de tratamiento posterior de forma incompatible con estas finalidades
2. **Adecuación:** Compatibilidad del tratamiento con las finalidades informadas al titular, según el contexto del tratamiento
3. **Necesidad:** Limitación del tratamiento al mínimo necesario para la consecución de sus finalidades, con el alcance de los datos pertinentes, proporcionales y no excesivos en relación con las finalidades del tratamiento de datos
4. **Libre acceso:** Garantía, a los titulares, de una consulta fácil y gratuita sobre la forma y duración del tratamiento, así como sobre la exhaustividad de sus datos personales
5. **Calidad de los datos:** Garantía, a los titulares, de exactitud, claridad, pertinencia y actualización de los datos, según la necesidad y para el cumplimiento de la finalidad de su tratamiento

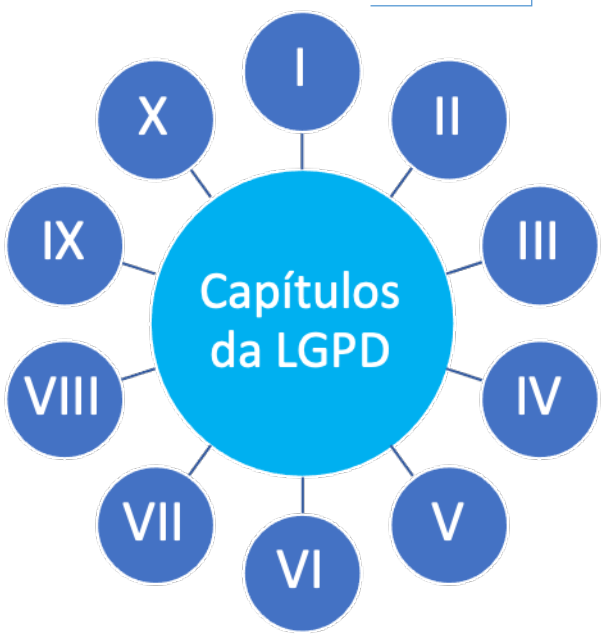
Principios

6. **Transparencia:** Garantía, a los titulares, de informaciones claras, precisas y fácilmente accesibles sobre la ejecución del tratamiento y los respectivos agentes del tratamiento, observando los secretos comerciales e industriales
7. **Seguridad:** Uso de medidas técnicas y administrativas para proteger los datos personales de accesos no autorizados y situaciones accidentales o ilícitas de destrucción, pérdida, alteración, comunicación o difusión
8. **Prevención:** Adopción de medidas para evitar la ocurrencia de daños debidos al procesamiento de datos personales
9. **No discriminación:** Imposibilidad de tratamiento con fines discriminatorios ilícitos o abusivos
10. **Responsabilidad y rendición de cuentas:** Demostración, por parte del agente, de la adopción de medidas efectivas capaces de acreditar la observancia y el cumplimiento de las normas de protección de datos personales e, incluso, la eficacia de estas medidas

Módulo 3: Bases legales para el Tratamiento de Datos Personales

LGPDF™ Versión 102021

¿En qué parte de la ley estamos?



CAPÍTULO II – DEL TRATAMIENTO DE DATOS PERSONALES

Artículos 7 a 16
Sección I - Requisitos para el tratamiento de datos personales - Artículos 7 a 10
Sección II - Tratamiento de datos personales sensibles - Artículos 11 a 13
Sección III - Tratamiento de Datos Personales de Niños, Niñas y Adolescentes - Artículo 14
Sección IV - Fin del tratamiento de datos - Artículos 15 y 16

Los requisitos para el procesamiento de datos personales

Base Jurídica en la LGPD

Requisitos para el Tratamiento de Datos Personales

Artículo 7. El tratamiento de los datos personales solo puede llevarse a cabo en los siguientes casos:

1. Proporcionando el consentimiento del titular

2. Para el cumplimiento de la obligación legal o reglamentaria por parte del responsable del tratamiento

3. Por la administración pública, para el tratamiento y uso compartido de los datos necesarios para la ejecución de las políticas públicas previstas en las leyes y reglamentos o respaldadas por contratos, acuerdos o instrumentos similares, en cumplimiento de lo dispuesto en el Capítulo IV de esta Ley

4. Para los estudios realizados por un organismo de investigación, se garantiza, siempre que sea posible, la anonimización de los datos personales

5. Cuando sea necesario para la ejecución de un contrato o procedimientos preliminares relativos al contrato en el que el titular sea parte, a petición del interesado

Requisitos para el Tratamiento de Datos Personales

6. Para el ejercicio regular de los derechos en los procedimientos judiciales, administrativos o arbitrales, estos últimos de conformidad con la Ley Nº 9.307 de 23 de septiembre de 1996 (Ley de Arbitraje)

7. Para la protección de la vida o la seguridad física del titular o de un tercero

8. Para la protección de la salud, exclusivamente, en un procedimiento realizado por profesionales de la salud, servicios de salud o autoridad sanitaria

9. Cuando sea necesario para tener en cuenta los intereses legítimos del responsable del tratamiento o de un tercero, excepto cuando prevalezcan los derechos y libertades fundamentales del interesado

10. Para la protección del crédito, incluidas las disposiciones de la legislación pertinente

Requisitos para el Tratamiento de Datos Personales

Artículo. 7:

1. (Revocado)
2. (Revocado)
3. El tratamiento de datos personales cuyo acceso sea público deberá tener en cuenta la finalidad, la buena fe y el interés público que justifique su disponibilidad
4. Se renuncia a la exigencia del consentimiento previsto en el capítulo de este artículo para los datos hechos manifiestamente públicos por el titular, protegidos por los derechos del titular y los principios previstos en esta Ley
5. El responsable del tratamiento que haya obtenido el consentimiento a que se refiere el punto I del capítulo de este artículo que necesite comunicar o compartir datos personales con otros responsables del tratamiento deberá obtener el consentimiento específico del titular a tal efecto, con sujeción a las posibilidades de renuncia al consentimiento previstas en la presente Ley

Requisitos para el Tratamiento de Datos Personales

6. Cualquier renuncia al requisito de consentimiento no exime a los agentes del tratamiento de otras obligaciones en virtud de esta Ley, especialmente el cumplimiento de los principios generales y la garantía de los derechos del titular
7. El tratamiento posterior de los datos personales a que se refieren los apartados 3 y 4 de este artículo podrá llevarse a cabo con nuevas finalidades, siempre que se observen las finalidades legítimas y específicas para el nuevo tratamiento y conservación de los derechos del titular, así como las causales y principios previstos en esta Ley

Consentimiento

Artículo 8. El consentimiento previsto en el inciso I del art. 7 de esta Ley se prestará por escrito o por cualquier otro medio que demuestre la expresión de voluntad del titular.

1. Si el consentimiento se proporciona por escrito, se incluirá en una cláusula destacada de las otras cláusulas contractuales.
2. El controlador tiene la carga de la prueba de que se obtuvo el consentimiento de conformidad con las disposiciones de esta ley.
3. Queda prohibido el tratamiento de datos personales por falta de consentimiento.
4. El consentimiento debe referirse a fines específicos, y las autorizaciones genéricas para el procesamiento de datos personales serán nulas.
5. El consentimiento podrá ser revocado en cualquier momento previa manifestación expresa del titular, por procedimiento libre y facilitado, ratificado de los tratamientos realizados bajo el consentimiento previo prestado siempre y cuando no exista solicitud de eliminación, de conformidad con el numeral VI del capítulo del art. 18 de esta Ley.
6. En caso de cambio de información a que se refieren los párrafos I, II, III o V del art. 9 de esta Ley, el responsable del tratamiento informará al titular, con especial énfasis en el contenido de los cambios, y el titular podrá, en los casos en que se requiera su consentimiento, revocarlo si no está de acuerdo con el cambio.

Interés Legítimo

Artículo 10. El interés legítimo del controlador solo puede justificar el procesamiento de datos personales para fines legítimos, considerados a partir de situaciones específicas, que incluyen, entre otras:

Apoyo y promoción de las actividades de los controladores.
Protección, en relación con el titular, del ejercicio regular de sus derechos o prestación de servicios que le beneficien, respetando su confianza legítima y derechos y libertades fundamentales, conforme a esta Ley.

1. Cuando el procesamiento se basa en el interés legítimo del controlador, solo se pueden procesar los datos personales estrictamente necesarios para el propósito previsto.
2. El controlador del tratamiento debe adoptar medidas para garantizar la transparencia en el tratamiento de datos sobre la base de su interés legítimo.
3. La autoridad nacional podrá solicitar al responsable del tratamiento que informe sobre la protección de los datos personales, cuando el tratamiento se base en su interés legítimo, en interés de los secretos comerciales e industriales.

Procesamiento de datos personales sensibles

Hipótesis para el Tratamiento de Datos Personales Sensibles

Art. 11. El tratamiento de datos personales sensibles sólo puede darse en los siguientes casos:

1. Cuando el titular o su tutor legal lo consienta, de manera expresa y destacada, para fines específicos
2. Sin prestar el consentimiento del titular, en los casos en que sea imprescindible para:
   a) Cumplimiento de una obligación legal o reglamentaria por parte del responsable del tratamiento
   b) Tratamiento compartido de datos necesarios para la ejecución, por parte de la administración pública, de políticas públicas previstas en leyes o reglamentos
   c) Realización de estudios por parte de un organismo de investigación, asegurando, siempre que sea posible, la anonimización de los datos personales sensibles.
   d) Ejercicio regular de los derechos, incluso en el contrato y en los procedimientos judiciales, administrativos y arbitrales, estos últimos de conformidad con la Ley N° 9.307, de 23 de septiembre de 1996 (Ley de Arbitraje)
   e) Protección de la vida o integridad física del titular o de un tercero
   f) Tutela de salud, exclusivamente, en un procedimiento realizado por profesionales de la salud, servicios de salud o autoridad sanitaria
   g) Garantía de prevención del fraude y seguridad del titular, en los procesos de identificación y autenticación de registro en sistemas electrónicos, resguardando los derechos mencionados en el art. 9 de esta Ley y salvo en el caso de que prevalezcan los derechos y libertades fundamentales del interesado que requieran la protección de datos personales.

Datos Anonimizados

Artículo 12. Los datos anonimizados no tendrán la consideración de datos personales a los efectos de esta Ley, salvo que se revierta el proceso de anonimización al que han sido sometidos, utilizando exclusivamente medios propios, o cuando, con esfuerzos razonables, pueda ser revertido.

1. La determinación de lo que es razonable debe tener en cuenta factores objetivos, como el costo y el tiempo necesarios para revertir el proceso de anonimización, de acuerdo con las tecnologías disponibles, y el uso exclusivo de medios propios.

2. Para los efectos de esta Ley, también podrán ser considerados como datos personales aquellos utilizados para formar el perfil de comportamiento de determinada persona natural, en caso de ser identificada.

3. La autoridad nacional podrá establecer normas y técnicas utilizadas en los procesos de anonimización y llevar a cabo controles de su seguridad, previa audiencia del Consejo Nacional de Protección de Datos Personales.

Acceso de los Organismos de Investigación

Artículo 13. En la realización de estudios en salud pública, los organismos de investigación podrán tener acceso a bases de datos personales, que serán tratadas exclusivamente dentro de la agencia y estrictamente con el fin de realizar estudios e investigaciones y mantenidas en un entorno controlado y seguro, de acuerdo con las prácticas de seguridad previstas en un reglamento específico y que incluyen, siempre que sea posible, anonimización o seudonimización de los datos, así como considerar los estándares éticos adecuados relacionados con los estudios y la investigación.

El tratamiento de datos personales de niños, niñas y adolescentes

Tratamiento de Datos Personales de Niños, Niñas y Adolescentes

Artículo 14. El tratamiento de datos personales de niños, niñas y adolescentes deberá realizarse en el interés superior de éstos, en los términos de este artículo y de la legislación correspondiente.

§ 1. El procesamiento de los datos personales de los niños debe llevarse a cabo con el consentimiento específico y destacado otorgado por al menos uno de los padres o tutores legales.
§ 2. En el tratamiento de los datos a que se refiere el apartado 1 de este artículo, los responsables del tratamiento mantendrán pública la información sobre los tipos de datos recogidos, la forma de su uso y los procedimientos para el ejercicio de los derechos a que se refiere el art. 18 de esta Ley.
§ 3. Los datos personales podrán ser recogidos de menores sin el consentimiento a que se refiere el § 1 de este artículo cuando la recogida sea necesaria para contactar con los padres o tutores legales, utilizados una sola vez y sin almacenamiento, o para su protección, y en ningún caso podrán ser cedidos a un tercero sin el consentimiento del apartado 1 de este artículo.

Tratamiento de Datos Personales de Niños, Niñas y Adolescentes

§ 4. Los responsables del tratamiento no condicionarán la participación de los titulares del apartado 1 de este artículo en juegos, aplicaciones de internet u otras actividades al suministro de información personal más allá de las estrictamente necesarias para la actividad.
§ 5. El responsable del tratamiento hará todos los esfuerzos razonables para verificar que el consentimiento a que se refiere el párrafo 1 del presente artículo haya sido prestado por la persona responsable del menor, teniendo en cuenta las tecnologías disponibles.
§ 6. La información sobre el tratamiento de los datos a que se refiere este artículo deberá facilitarse de forma sencilla, clara y accesible, teniendo en cuenta las características físico-motoras, perceptivas, sensoriales, intelectuales y mentales del usuario, utilizando recursos audiovisuales cuando proceda, con el fin de facilitar la información necesaria a los padres o al tutor legal y adecuada a la comprensión del menor.

Fin del procesamiento de datos

¿Cuándo finaliza el tratamiento?

Art. 15 La terminación del tratamiento de datos personales se producirá en los siguientes casos:

1. Cuando ya no son necesarios o pertinentes para la consecución del fin específico perseguido.
2. Cuando se cumpla con el fin del período del tratamiento.
3. Notificación al titular, incluyendo el ejercicio de su derecho a revocar el consentimiento según lo previsto en el § 5, art. 8 de esta Ley, salvaguardando el interés público.
4. Cuando lo determine la autoridad nacional, en caso de incumplimiento de las disposiciones de esta Ley.

Eliminación de Datos Personales

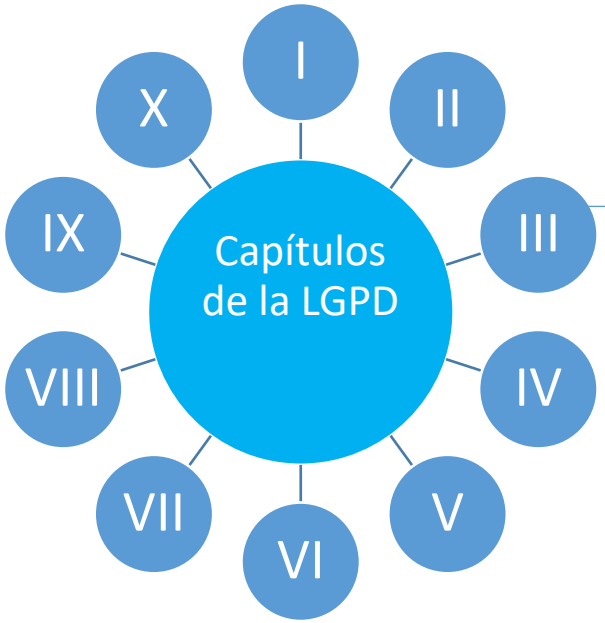
Art. 16. Los datos personales se eliminarán una vez finalizado su tratamiento, dentro del ámbito y los límites técnicos de las actividades, estando autorizada la conservación para los siguientes fines:

1. Cumplimiento de obligaciones legales o reglamentarias por parte del responsable del tratamiento.
2. Estudio por organismo de investigación científica, garantizando, siempre que sea posible, la anonimización de los datos personales.
3. Transferencia a un tercero, siempre que se cumplan los requisitos de tratamiento de datos establecidos en esta Ley.
4. Uso exclusivo por parte del responsable del tratamiento, sin acceso por parte de terceros, y siempre que los datos estén anonimizados.

Módulo 4: Derechos del Titular – Teoría y Práctica

LGPDF™ Versión 102021

¿En qué parte de la ley estamos?



CAPÍTULO III – LOS DERECHOS DEL TITULAR

Artículos 17 a 22

Derechos del Titular

Artículo. 17. Se garantiza a toda persona natural la titularidad de sus datos personales y los derechos fundamentales de libertad, intimidad y privacidad, en los términos de esta Ley.

Artículo. 18. El titular de datos personales tiene derecho a obtener del responsable del tratamiento, en relación con los datos del titular tratados por él, en cualquier momento y previa solicitud:

1. Confirmación de la existencia del tratamiento;
2. Acceso a los datos;
3. Corrección de datos incompletos, inexactos o desactualizados;
4. Anonimización, bloqueo o eliminación de datos innecesarios, excesivos o tratados en violación de las disposiciones de esta Ley;

Derechos del Titular

5. Portabilidad de datos para otro proveedor de servicios o productos, previa solicitud expresa y observando secretos comerciales e industriales, de acuerdo con la regulación del órgano de control;
6. Eliminación de datos personales tratados con el consentimiento del titular, excepto en los casos previstos en el art. 16 de esta Ley;
7. Información sobre las entidades públicas y privadas con las cuales el controlador hizo uso compartido de los datos;
8. Información sobre la posibilidad de no prestar el consentimiento y sobre las consecuencias de la negación;
9. Revocación del consentimiento, en los términos del § 5 del art. 8 de esta Ley.

Derechos del Titular

- 1º El interesado tiene derecho a presentar una solicitud en relación con sus datos contra el responsable del tratamiento ante la autoridad nacional
- 2º El interesado podrá oponerse al tratamiento basándose en alguno de los supuestos de renuncia al consentimiento, en caso de incumplimiento de lo dispuesto en esta Ley
- 3º Los derechos previstos en este artículo se ejercerán a petición expresa del interesado o de un representante legalmente constituido, ante un encargado del tratamiento
- 4º Si no es posible adoptar inmediatamente la medida prevista en el apartado 3 del presente artículo, el responsable del tratamiento enviará al titular una respuesta en la que podrá:
  1. Notificar que no es el encargado del tratamiento de datos e indicar, cuando sea posible, el encargado
  2. Indique las razones de hecho o de derecho que impiden la adopción inmediata de la medida.
- 5º La solicitud a la que se refiere el inciso 3 de este artículo se llevará a cabo sin coste alguno para el titular, en los plazos y términos establecidos en la normativa
- 6º El responsable deberá informar inmediatamente a los encargados del tratamiento con los que haya compartido datos de la rectificación, supresión, anonimización o bloqueo de los mismos, para que puedan repetir el mismo procedimiento, salvo en los casos en que esta comunicación sea manifiestamente imposible o suponga un esfuerzo desproporcionado
- 7º La portabilidad de los datos personales a la que se refiere el inciso V del título de este artículo no incluye los datos que ya han sido anonimizados por el responsable del tratamiento
- 8º El derecho mencionado en el § 1 de este artículo también puede ejercerse ante los organismos de protección de los consumidores

Derechos del Titular

Art. 19. La confirmación de la existencia o el acceso a los datos personales se proporcionará a petición del interesado:

1. Sin ninguna formalidad, inmediatamente
2. Mediante una declaración clara y completa, en la que se indique el origen de los datos, la inexistencia de un registro, los criterios utilizados y la finalidad del tratamiento, observando el secreto comercial e industrial, facilitada en el plazo de 15 (quince) días desde la fecha de la solicitud del titular

- 1º Los datos personales se almacenarán en un formato que facilite el ejercicio del derecho de acceso.
- 2º La información y los datos pueden facilitarse a discreción del titular:
  - I. Por medios electrónicos, seguros y adecuados para este fin
  - II. En formato impreso

Art. 20. El interesado tendrá derecho a solicitar una revisión de las decisiones adoptadas únicamente sobre la base del tratamiento automatizado de datos personales que afecten a sus intereses, incluidas las decisiones destinadas a definir su perfil personal, profesional, de consumo y de crédito o aspectos de su personalidad.

- 1º El responsable del tratamiento proporcionará, siempre que se le solicite, información clara y adecuada sobre los criterios y procedimientos utilizados para la decisión automatizada, teniendo en cuenta los secretos comerciales e industriales
- 2º En caso de que no se proporcione la información a la que se refiere el inciso 1 de este artículo, basándose en el cumplimiento de la confidencialidad comercial e industrial, la autoridad nacional podrá realizar una auditoría para verificar los aspectos discriminatorios en el tratamiento automatizado de datos personales

Derechos del Titular

Art. 21. Los datos personales relativos al ejercicio legítimo de los derechos del interesado no podrán utilizarse en detrimento de éste.

Art. 22. La defensa de los intereses y derechos de los titulares de los datos podrá ejercerse ante los tribunales, individual o colectivamente, de conformidad con lo dispuesto en la legislación pertinente sobre los instrumentos de protección individual y colectiva.

Resumen de los Derechos del Titular

Derechos del Titular

PARTE PRÁCTICA: DPO y los Derechos de los Titulares

Cumplimiento de la LGPD en los Portales WEB:

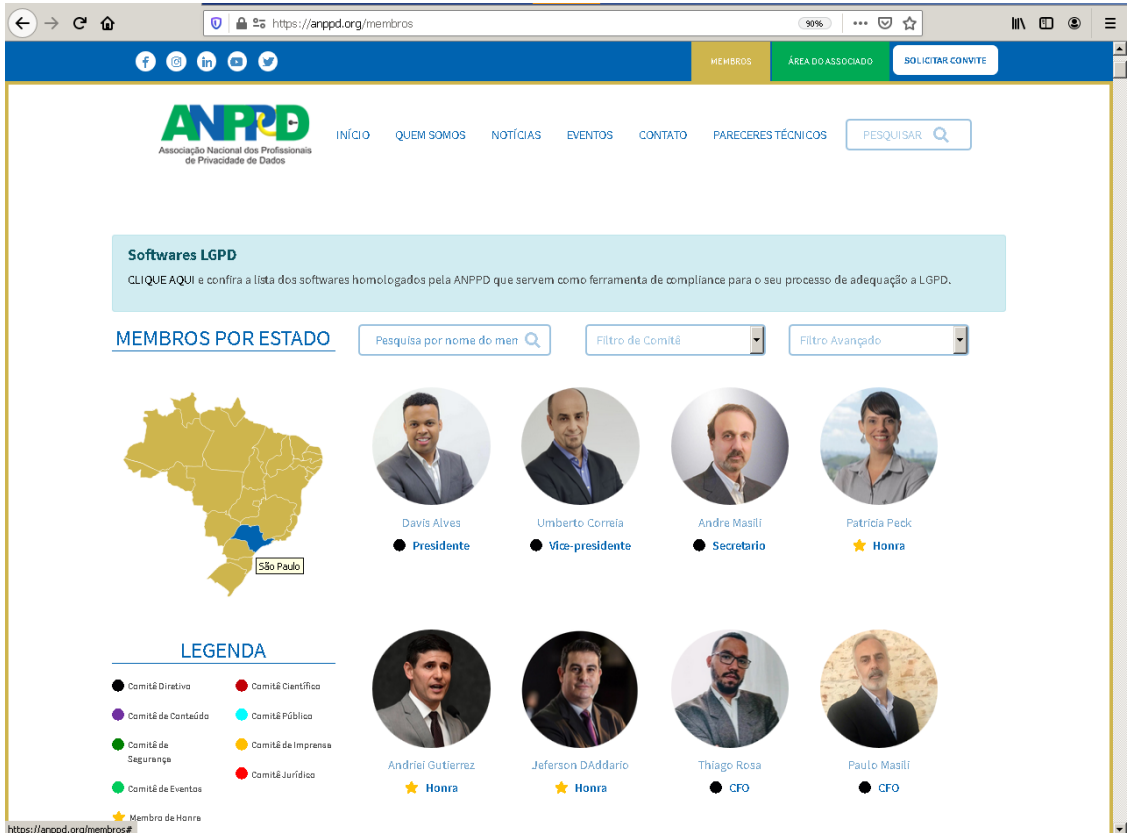
- Información sobre el DPO (Art. 41)
- Principio de Minimización (Art. 6, III - LGPD)
- Derecho de Acceso y modificación (Art. 18, II, III - LGPD)
- Derecho de Eliminación de Datos (Art. 18, V LGPD)
- Registro de Operaciones de Tratamiento (Art. 37 - LGPD)
- Derecho de Portabilidad (Art. 18, V - LGPD)

Estudio de caso público: ANPPD.org

Derechos del Titular

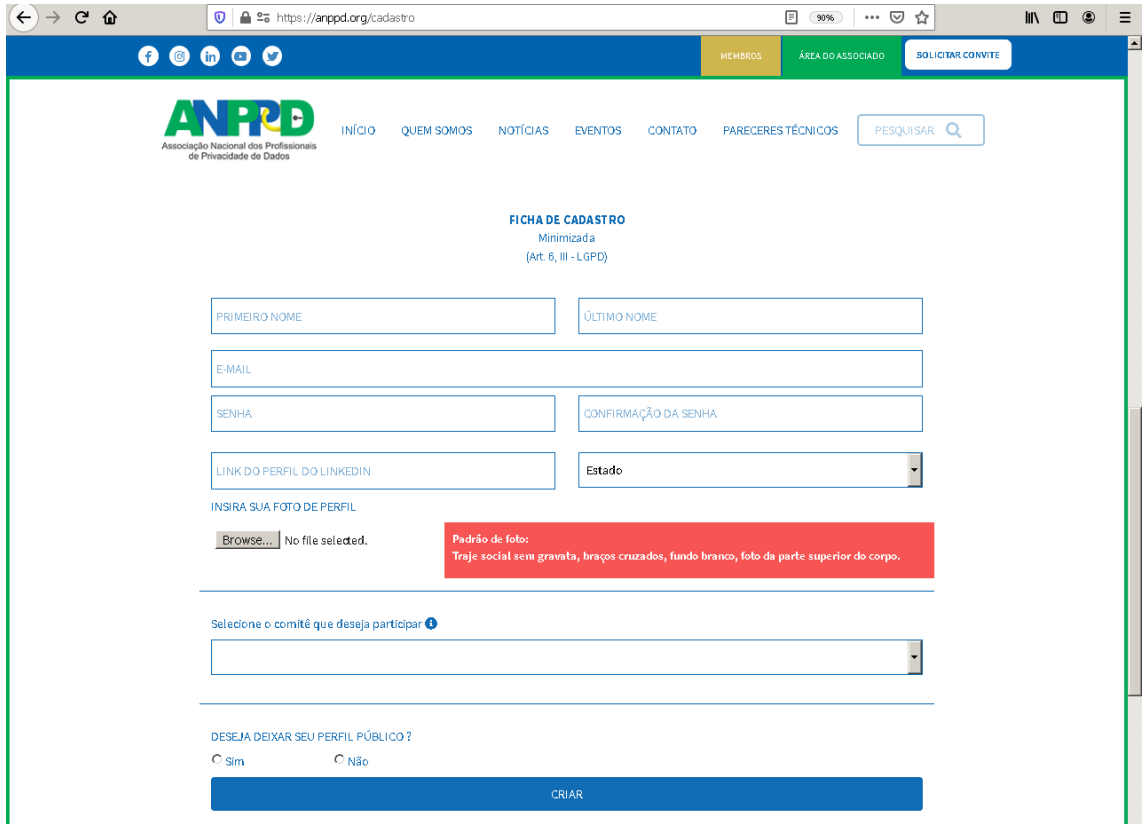
Estudio de Caso Público: ANPPD.org

El Sitio de la ANPPD fue uno de los primeros sitios web de Brasil en ofrecer los Derechos de los Titulares. En la imagen de al lado vemos el objetivo principal de la exposición de los profesionales en el mapa de miembros.



Derechos del Titular

Para ello, el profesional deberá completar un Registro de Inscripción, minimizada y referenciada con el Art. 6, III. Esta es la puerta de entrada para que el Responsable del Tratamiento introduzca los datos personales. Es importante señalar que también hay un enlace en la página a la Política de Privacidad de la institución.

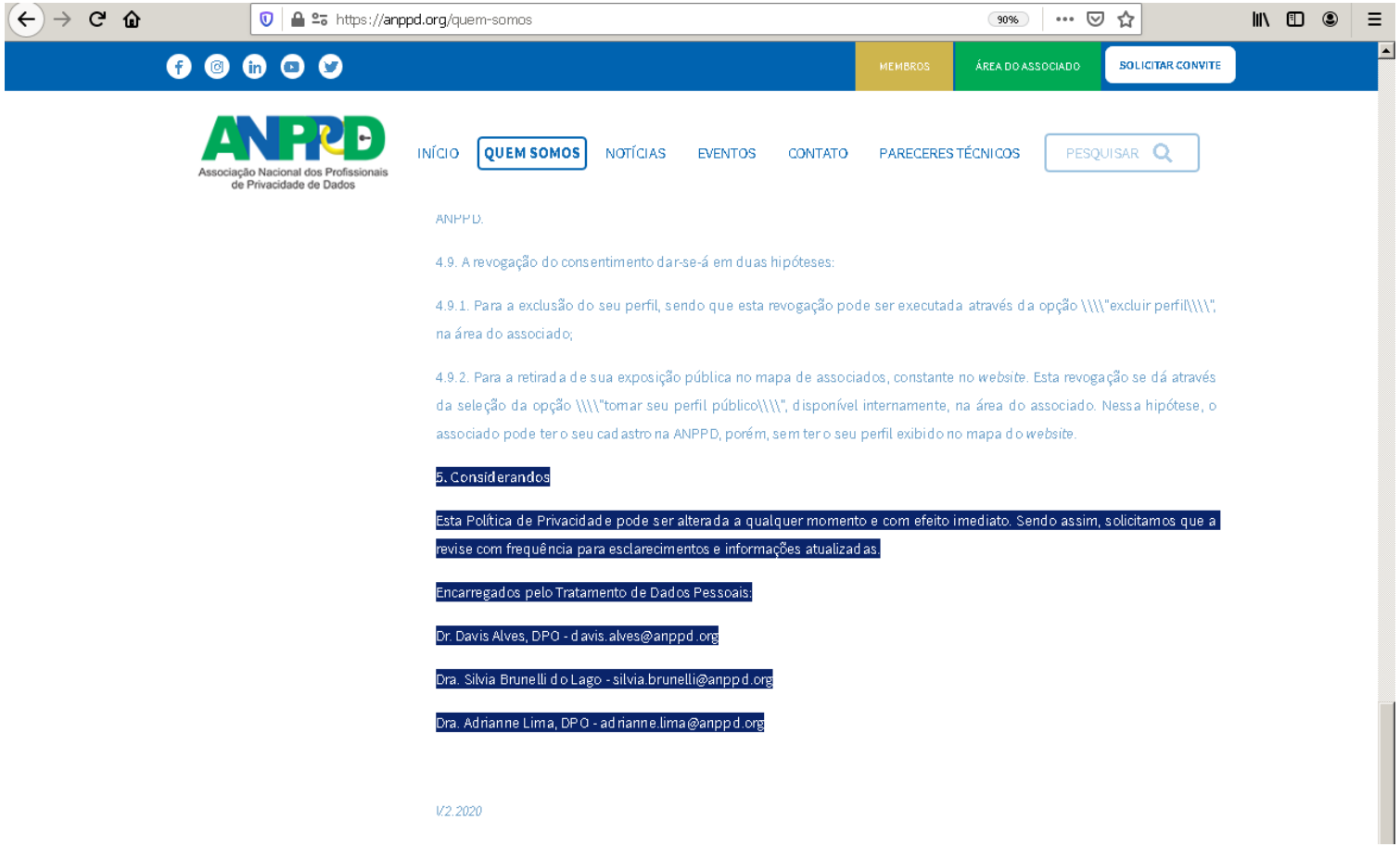


Derechos del Titular

La Política de Privacidad puede consultarse en el "Área LGPD" contenida en "Quiénes somos". Por ejemplo, es importante que los responsables del tratamiento faciliten el acceso en caso de que los interesados deseen obtener más información sobre el tratamiento de los datos personales.

Derechos del Titular

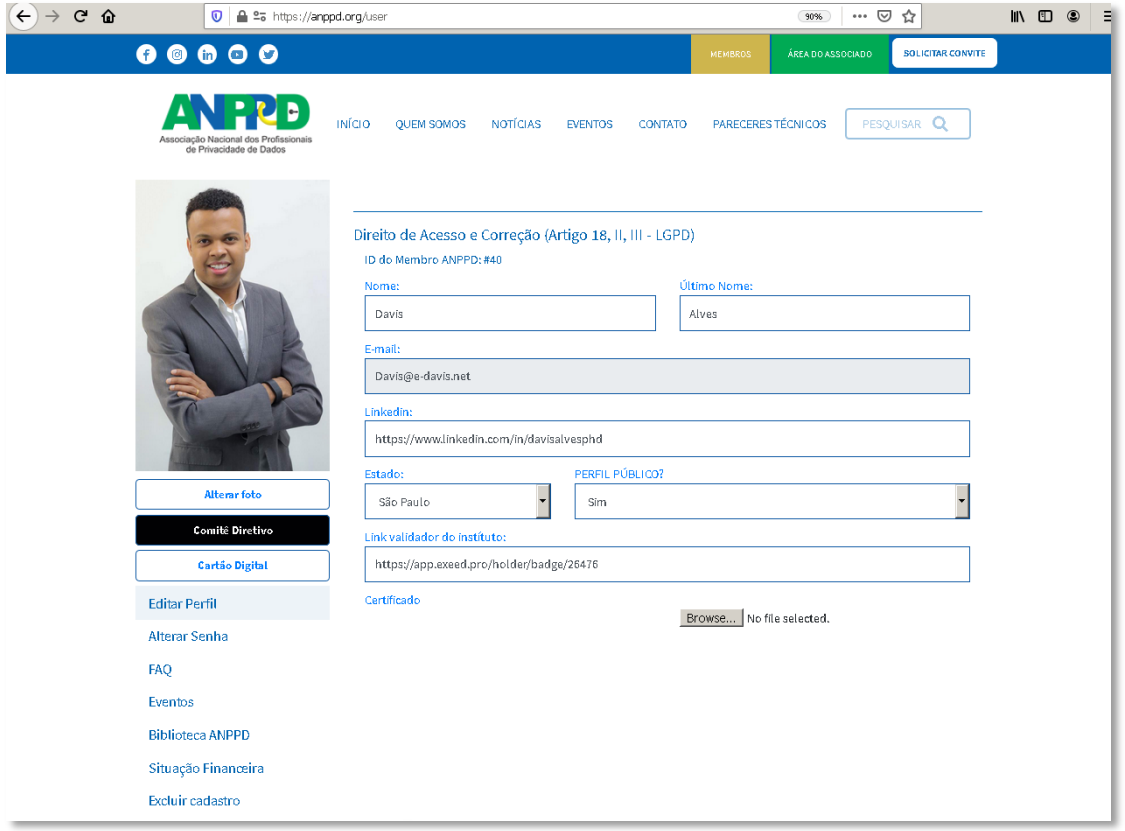
Junto con la Política de Privacidad es recomendable publicar la información sobre el DPO (art. 41), junto con su equipo de trabajo.



Derechos del Titular

Una vez comunicada la Política de Privacidad, los titulares pueden ver su cumplimiento siguiendo las instrucciones informadas.

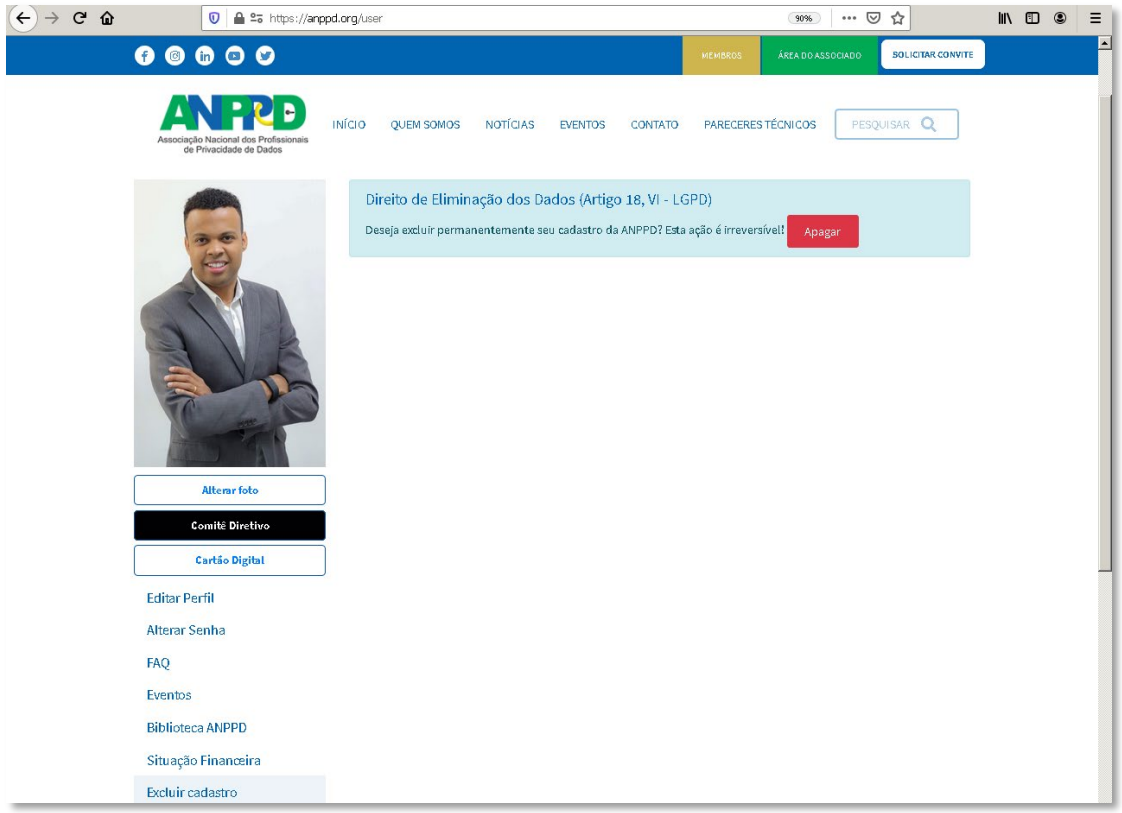
A modo de ejemplo, en la imagen de al lado se puede ver como se ejerce el Derecho de Acceso y Rectificación de los datos introducidos al momento de la inscripción, de acuerdo con el Art. 18, II e III – LGPD).



Derechos del Titular

Una vez comunicada la Política de Privacidad, los titulares pueden ver su cumplimiento siguiendo las instrucciones informadas.

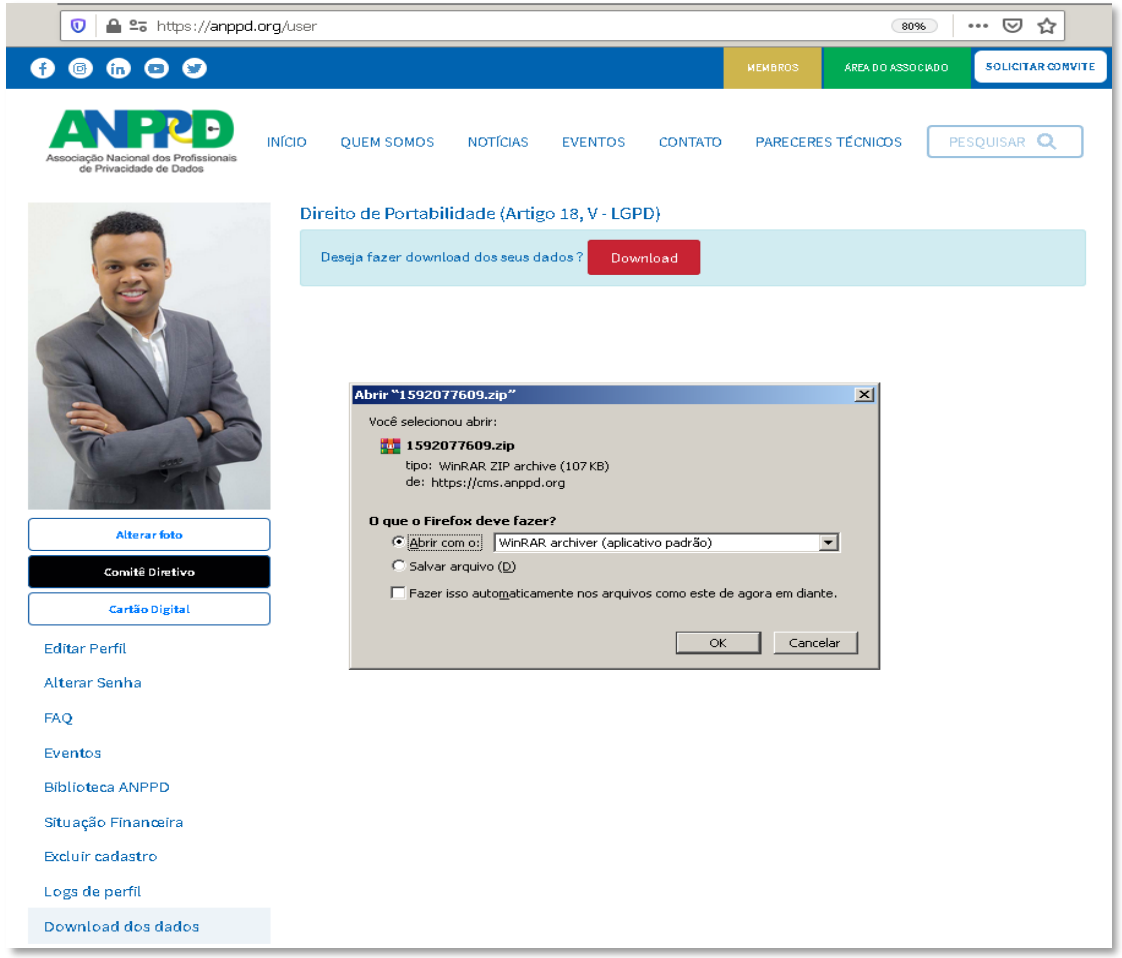
A modo de ejemplo, en la imagen de al lado se muestra como se ejerce el Derecho de Supresión de los datos introducidos al momento del registro, de acuerdo con el artículo 18, VI - LGPD).



Derechos del Titular

Una vez comunicada la Política de Privacidad, los titulares pueden ver su cumplimiento siguiendo las instrucciones informadas.

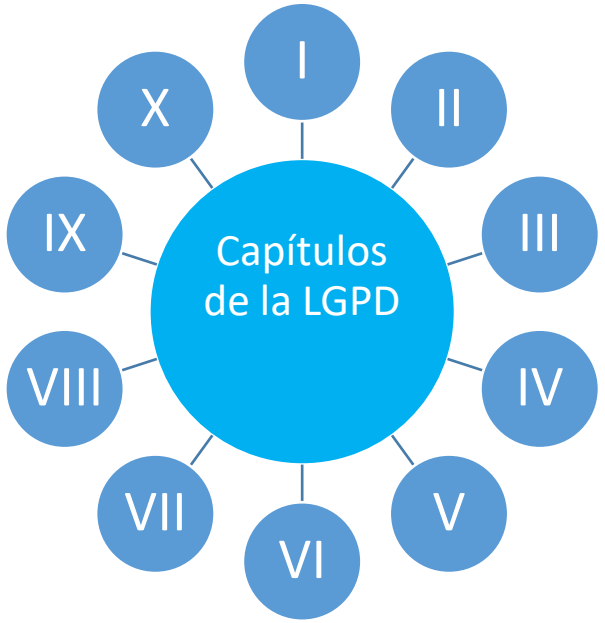
A modo de ejemplo, en la imagen de al lado se puede ver como se ejerce el Derecho de Portabilidad introducido al momento del registro, de acuerdo con el Art. 18, V – LGPD).



Módulo 5: Tratamiento de Datos Personales por Parte de las Autoridades Públicas

LGPDF™ Versión 102021

¿En qué parte de la ley estamos?



CAPÍTULO IV – TRATAMIENTO DE DATOS PERSONAL DE LAS AUTORIDADES PÚBLICAS

Artículos 23 a 32
Sección I - Reglamento - Artículos 23 a 30
Sección II - Responsabilidad - Artículos 31 y 32

Premisas

- Constitución de la República Federativa de Brasil de 1988. Acceso en: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm
- Administración Pública = un conjunto de órganos, servicios y agentes del Estado que busca satisfacer las necesidades de la sociedad, tales como: educación, cultura, seguridad, salud.
- La Administración Pública es la gestión de los intereses públicos a través de la prestación de servicios públicos

(Fuente: Gregorius, Marcio Rosni. 2015. https://marciorosni.jusbrasil.com.br/artigos/195654350/a-administracao-publica-e-suas-funcoes)

Premisas

Constitución Federal

Art. 3º. Los siguientes son objetivos fundamentales de la República Federativa de Brasil:

1. Construir una sociedad libre, justa y solidaria
2. Garantizar el desarrollo nacional
3. Erradicar la pobreza y la marginación y reducir las desigualdades sociales y regionales
4. Promover el bien de todos, sin prejuicios de origen, raza, sexo, color, edad y cualquier otra forma de discriminación

Art. 37. **La administración pública** directa e indirecta de cualquiera de los Poderes de la Unión, de los Estados, del Distrito Federal y de los Municipios se deberá atender a los principios de legalidad, impersonalidad, moralidad, publicidad y eficacia, así como a los siguientes:

- 3º La ley regulará las formas de participación de los usuarios en la administración pública directa e indirectamente, haciendo hincapié especialmente:
  - **II** - acceso de los usuarios a los registros administrativos y a la información sobre los actos de la Administración, en cumplimiento de lo dispuesto en art. 5º, X e XXXIII; (Incluído por la Enmienda Constitucional nº 19, de 1998)

Premisas

Art. 5:

- **X** - la intimidad, la vida privada, el honor y la imagen pública son inviolables, y se garantiza el derecho a la reparación de los daños materiales o morales derivados de su violación
- **XXXIII** - toda persona tiene derecho a recibir de los organismos públicos información de su interés privado o de interés colectivo o general, que le será facilitada en el plazo que establezca la ley, bajo pena de incurrir en responsabilidad, con excepción de la información cuyo secreto sea esencial para la seguridad de la sociedad y del Estado; (Reglamento) (Ver Ley nº 12.527, de 2011)

Las Reglas

¿Cuándo está permitido el tratamiento de datos personales?

Art. 23. El tratamiento de datos personales por parte de las personas jurídicas de derecho público a que se refiere el párrafo único del art. 1 de la Ley de Acceso a la Información, se realizará para el cumplimiento de su finalidad pública, en la búsqueda del interés público, con el fin de ejecutar las competencias legales o cumplir las atribuciones legales del servicio público, siempre que:

Personas jurídicas de derecho público:
http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm

1. Los organismos públicos que forman parte de la administración directa del Ejecutivo, del Legislativo, incluidos los Tribunales de Cuentas, el Poder Judicial y el Ministerio Fiscal.
2. Las entidades autárquicas, fundaciones públicas, empresas públicas, sociedades de economía mixta y otras entidades controladas directa o indirectamente por la Unión, los Estados, el Distrito Federal y los Municipios

Información sobre el tratamiento en el sitio web

1. Ser informados de los casos en los que, en el ejercicio de sus competencias, tratan datos personales, proporcionando información clara y actualizada sobre las disposiciones legales, la finalidad, los procedimientos y las prácticas utilizadas para llevar a cabo estas actividades, en vehículos fácilmente accesibles, preferiblemente en sus sitios web
2. II e IV – VETADOS (prohibición de compartir datos, así como con personas jurídicas de derecho privado) – ago/2018

¿Cuándo está permitido el tratamiento de datos personales?

“Tras ser oído, el Ministerio de Hacienda expresó su veto a la siguiente disposición: Inciso II del art. 23

´II - los datos personales de los solicitantes de acceso a la información son protegidos y preservados, en los términos de la Ley nº 12.527 de 18 de noviembre de 2011 (Ley de Acceso a la Información), y se prohíbe compartirlos dentro del Poder Público y con personas jurídicas privadas.´

Motivos del veto: ´La disposición prohíbe compartir datos personales dentro del Poder Público y con entidades jurídicas privadas. El intercambio de información relacionada con personas físicas identificadas o identificables es una medida recurrente y esencial para el ejercicio regular de diversas actividades y políticas públicas. Es el caso, por ejemplo, de la base de datos de la Seguridad Social y del Registro Nacional de Información Social, cuya información se utiliza para el reconocimiento del derecho de sus beneficiarios y se alimenta de la puesta en común de varias bases de datos gestionadas por otros organismos públicos. Además, se podrían hacer inviables algunas actividades relacionadas con el poder de policía administrativa, como las investigaciones en el ámbito del Sistema Financiero Nacional, entre otras.´”

¿Cuándo está permitido el tratamiento de datos personales?

Art. 23. El tratamiento de datos personales por parte de las personas jurídicas de derecho público al que se refiere el párrafo único del art. 1 de la Ley de Acceso a la Información, se realizará para el cumplimiento de su finalidad pública, en la búsqueda del interés público, con el fin de ejecutar las competencias legales o cumplir las atribuciones legales del servicio público, siempre que:

Cuando estas personas jurídicas sean Encargados del Tratamiento de Datos, deberán designar a un DPO.

- III - Se nombre a una persona a cargo (DPO) al llevar a cabo operaciones de procesamiento de datos personales, de acuerdo con el art. 39 de esta Ley

En el Caso de las Empresas Públicas y las Sociedades de Economía Mixta

Si explotan una actividad económica, pueden tener el mismo tratamiento que las personas jurídicas de derecho privado

Art. 24. Las empresas públicas y las sociedades de capital mixto que operen bajo el régimen de licitación, con sujeción a lo dispuesto en el artículo 173 de la Constitución Federal, tendrán el mismo tratamiento que las personas jurídicas privadas, de conformidad con esta Ley.

- Párrafo único. Las empresas públicas y las sociedades de economía mixta, cuando operen políticas públicas y en el ámbito de su ejecución, tendrán el mismo tratamiento que los órganos y entidades del Poder Público, en los términos de este Capítulo.

Formato de Uso Compartido Interoperable

Art. 25. Los datos deben mantenerse en un formato interoperable y estructurado para su uso compartido, con vistas a la ejecución de políticas públicas, la prestación de servicios públicos, la descentralización de la actividad pública y la difusión y el acceso a la información por parte del público en general.

Uso Compartido de Datos Personales

Art. 26. El uso compartido de los datos personales por parte de las Administraciones Públicas debe responder a los fines específicos de ejecución de políticas públicas y de atribución legal por parte de los organismos y entidades públicas, respetando los principios de protección de datos personales enumerados en el artículo 6 de esta Ley.

- 1º El Poder Público tiene prohibido ceder a entidades privadas los datos personales contenidos en las bases de datos a las que tiene acceso, salvo:
  1. En los casos de ejecución descentralizada de actividades públicas que requieran la transferencia exclusivamente para este fin específico y determinado, en cumplimiento de lo dispuesto en la Ley de Acceso a la Información
  2. (VETADO)
  3. En los casos en que los datos sean de acceso público, con sujeción a lo dispuesto en la presente Ley
  4. Cuando exista una disposición legal o la transferencia esté respaldada por contratos, acuerdos o instrumentos similares
  5. En el caso de que la transferencia de datos tenga como objetivo exclusivo la prevención de fraudes e irregularidades o la protección y salvaguarda de la seguridad e integridad del interesado, siempre que se prohíba el tratamiento para otros fines

Uso Compartido de Datos Personales con el Consentimiento del Interesado

Norma: Compartir datos personales entre personas públicas y privadas = conocimiento de la ANPD + consentimiento del interesado

Art. 27. La comunicación o el uso compartido de datos personales de una persona jurídica de derecho público a una persona jurídica de derecho privado se comunicará a la autoridad nacional y dependerá del consentimiento del interesado, salvo:

1. En los casos de renuncia al consentimiento previstos en esta Ley; (por ejemplo, datos hechos manifiestamente públicos por el titular)
2. En los casos de uso compartido de datos, en cuyo caso se dará publicidad en los términos del inciso I del encabezado del artículo 23 de esta Ley; o (información en el sitio)
3. En las excepciones previstas en el § 1 del art. 26 de esta Ley. (cuando hay acuerdos, contratos notificados a la ANPD)

- Párrafo único. La información a la autoridad nacional mencionada en el encabezado de éste artículo será objeto de regulación

Registros de Operaciones de Tratamiento

Art. 29. La autoridad nacional podrá solicitar, en cualquier momento, a los órganos y entidades del poder público que realicen operaciones de tratamiento de datos personales, información específica sobre el alcance y la naturaleza de los datos y otros detalles del tratamiento realizado, y podrá emitir un dictamen técnico complementario para garantizar el cumplimiento de esta Ley.

Art. 30. La autoridad nacional podrá establecer normas complementarias para las actividades de comunicación y el uso compartido de datos personales.

Publicación y Normas del RIPD y Acciones de Buenas Prácticas

Art. 32. La autoridad nacional puede solicitar a los funcionarios de la autoridad pública que publiquen informes de impacto sobre la protección de datos personales y que sugieran la adopción de normas y buenas prácticas para el tratamiento de datos personales por parte de la autoridad pública.

Registros de Operaciones de Tratamiento

Ejemplo: En una demanda promovida por los Defensores Públicos de la Unión y de San Pablo, Instituto Brasileño de Protección al Consumidor, Artigo 19 e Intervozes, el Poder Judicial exigió la presentación del RIPD para la producción de pruebas por parte del Metro de San Pablo sobre la identificación facial de los pasajeros.

Enlace a más información: https://www.linkedin.com/pulse/relat%C3%B3rio-de-impacto-prote%C3%A7%C3%A3o-dados-pessoais-%C3%A9-ao-sp-correia-lima/

Responsabilidad

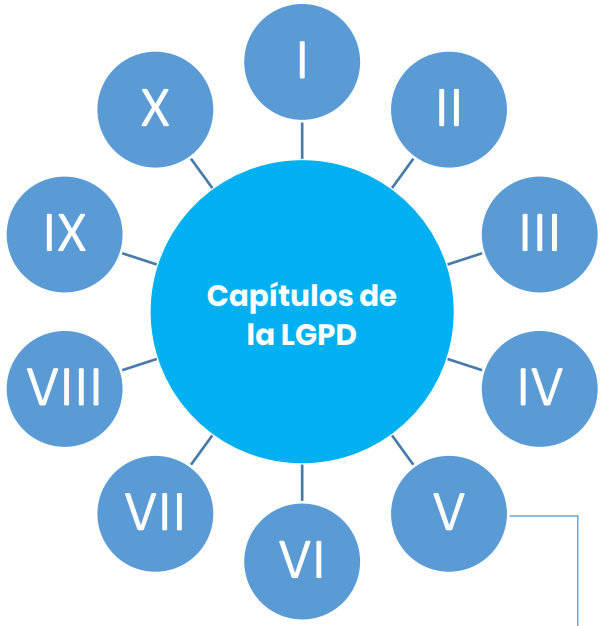
En Caso de Infracción

Art. 31. Cuando se produzca una infracción de esta Ley como consecuencia del tratamiento de datos personales por parte de organismos públicos, la autoridad nacional podrá enviar un informe con las medidas adecuadas para poner fin a la misma.

Módulo 6: Transferencia Internacional de Datos

LGPDF™ Versión 102021

¿En qué parte de la ley estamos?



CAPÍTULO V – TRANSFERENCIA INTERNACIONAL DATOS

Artículos 33 a 36

¿Cuándo se permite una transferencia internacional?

Art. 33. La transferencia internacional de datos personales sólo está permitida en los siguientes casos:

1. Para los países u organismos internacionales que proporcionan un nivel de protección de los datos personales adecuado al previsto en esta Ley
2. Cuando el responsable del tratamiento ofrezca y acredite garantías de cumplimiento de los principios, los derechos del interesado y el régimen de protección de datos previsto en esta Ley, en forma de:
   a) Cláusulas contractuales específicas para una transferencia concreta
   b) Cláusulas contractuales estándar
   c) Normas corporativas globales
   d) Sellos, certificados y códigos de conducta emitidos regularmente

¿Cuándo se permite la transferencia internacional?

3. Cuando la transferencia sea necesaria para la cooperación jurídica internacional entre los organismos públicos de inteligencia, investigación y enjuiciamiento, de conformidad con los instrumentos de derecho internacional
4. Cuando la transferencia sea necesaria para proteger la vida o la seguridad física del titular o de un tercero
5. Cuando la autoridad nacional autoriza la transferencia
6. Cuando la transferencia es el resultado de un compromiso asumido en un acuerdo de cooperación internacional
7. cuando la transferencia sea necesaria para la ejecución de una política pública o atribución legal del servicio público, dándose publicidad en los términos del sub-I del encabezado del artículo 23 de esta Ley
8. cuando el titular de los derechos haya prestado su consentimiento específico y destacado a la transferencia, con información previa sobre el carácter internacional de la operación, distinguiéndola claramente de otros fines
9. Cuando sea necesario para cumplir las hipótesis previstas en los apartados II, V y VI del art. 7º de esta Ley

- **Párrafo único.** A los efectos del punto I de este artículo, las personas jurídicas de derecho público a las que se refiere el párrafo único del art. 1 de la Ley de Acceso a la Información, en el ámbito de sus competencias legales, y los responsables, en el ámbito de sus actividades, podrán solicitar a la autoridad nacional que evalúe el nivel de protección de datos personales conferido por un país u organismo internacional

Nivel de Protección Requerido en el Extranjero

Art. 34. El nivel de protección de datos del país extranjero o de la organización internacional mencionada en el inciso I del encabezado del artículo 33 de esta Ley será evaluado por la autoridad nacional, que tomará en consideración:

1. Las normas generales y sectoriales de la legislación vigente en el país de destino u organización internacional
2. La naturaleza de los datos
3. La observancia de los principios generales de protección de datos personales y de los derechos de los interesados previstos en esta Ley
4. La adopción de medidas de seguridad previstas en la normativa
5. La existencia de garantías judiciales e institucionales para el respeto de los derechos de protección de datos personales
6. Otras circunstancias específicas relacionadas con la transferencia

Garantías Mínimas

Art. 35. La definición del contenido de las cláusulas contractuales tipo, así como la verificación de las cláusulas contractuales específicas para una determinada transferencia, las normas o sellos corporativos globales, los certificados y los códigos de conducta, a los que se refiere el punto II del encabezado del artículo 33 de esta Ley, serán realizados por la autoridad nacional.

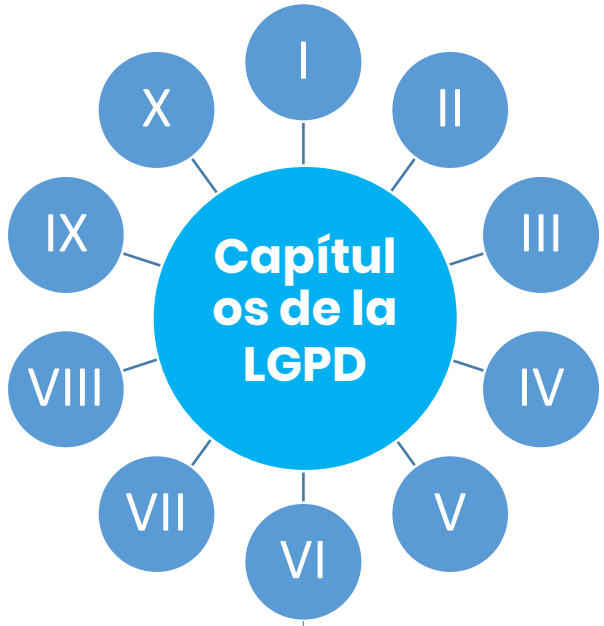
- 1º. A los efectos de verificar lo dispuesto en el encabezamiento de este artículo, se deben considerar los requisitos, condiciones y garantías mínimas para la transferencia que cumplan con los derechos, garantías y principios de esta Ley
- 2º. Al revisar las cláusulas contractuales, los documentos o las normas corporativas globales que se presenten para su aprobación a la autoridad nacional, se podrá solicitar información adicional o verificar las operaciones de tratamiento cuando sea necesario
- 3º. La autoridad nacional podrá designar organismos de certificación para llevar a cabo lo dispuesto en el encabezado de este artículo, que quedarán bajo su supervisión en los términos definidos en el reglamento
- 4º. Los actos realizados por un organismo de certificación podrán ser revisados por la autoridad nacional y, en caso de incumplimiento de esta Ley, sometidos a revisión o anulados
- 5º. Las garantías suficientes de cumplimiento de los principios generales de protección y de los derechos del titular a los que se refiere la frase del encabezado de este artículo se analizarán también en función de las medidas técnicas y organizativas adoptadas por el Responsable, de acuerdo con lo dispuesto en los §§ 1 y 2 del art. 46 de esta Ley

Art. 36. Los cambios en las garantías que se presenten como suficientes para cumplir con los principios generales de protección y los derechos del titular a los que se refiere el sub II del Art. 33 de esta Ley serán comunicados a la autoridad nacional.

Módulo 7: Responsables de los Datos Personales

LGPDF™ Versión 102021

¿En qué parte de la ley nos encontramos?



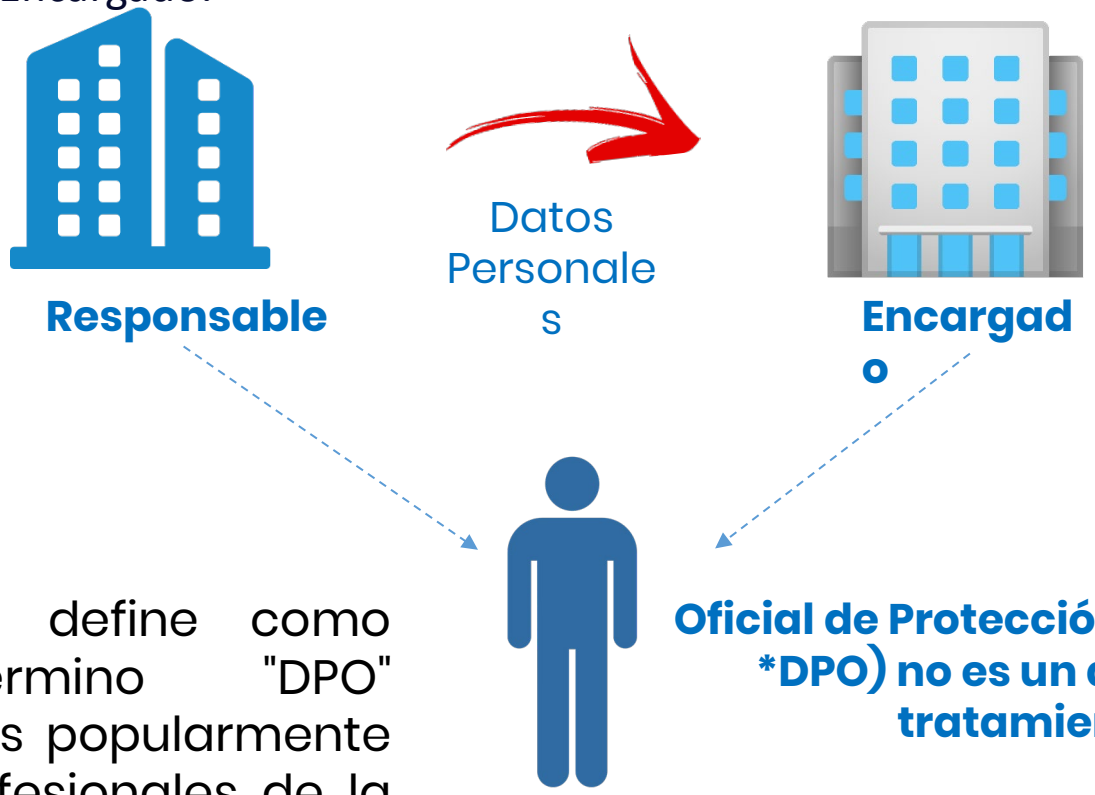
CAPÍTULO VI – LOS RESPONSABLES DE TRATAMIENTO DE DATOS PERSONALES

Artículos 37 a 45 Sección I - Del responsable y del operador - Artículos 37 a 40
Sección II - Del responsable del tratamiento de datos personales - Artículo 41
Sección III - Responsabilidad e indemnización por daños y perjuicios - Artículos 42 a 45

Recordar

Art. 5º. A los efectos de esta Ley, se considera:

- IX - responsables de datos personales: Agentes de tratamiento, Responsable o Encargado.



* Aunque la LGPD lo define como "Encargado", el término "DPO" (proveniente del GDPR) es popularmente referido por muchos profesionales de la privacidad de datos en Brasil.

Sección I

Del Responsable del Tratamiento y del Encargado del Tratamiento

Registro de Tratamiento de Datos

Art. 37. El responsable del tratamiento y el encargado mantendrán un registro de las operaciones de tratamiento de datos personales que lleven a cabo, especialmente cuando se basen en un interés legítimo.

# tratamento	Qual a finalidade	Categorias de Dados tratados																
		dados de identificação		dados de contacto		dados de faturação		vida familiar		vida profissional		informações de ordem financeira e patrimonial		dados de tráfego e de localização		dados de navegação na internet		outras categorias se
		Dados	prazo de conservação	Dados	prazo de conservação	Dados	prazo de conservação	Dados	prazo de conservação	Dados	prazo de conservação	Dados	prazo de conservação	Dados	prazo de conservação	Dados	prazo de conservação	Dados
T000	*ex: gestão de processamento de salários / gestão de sanções disciplinares / controlo de assiduidade / gestão de clientes / marketing / gravação de chamadas na relação contratual / gestão de processos clínicos / gestão de crédito e solvabilidade*	*ex: nome, fotografia, número de identificação civil*	*ex: 10 dias / 2 meses / 3 anos a partir da data da recolha dos dados / 2 anos a partir do fim da relação contratual*	*ex: morada, e-mail, telefone*	*ex: 10 dias / 2 meses / 3 anos a partir da data da recolha dos dados / 2 anos a partir do fim da relação contratual*	*ex: NIF, montante cobrado, data, IBAN*	*ex: 10 dias / 2 meses / 3 anos a partir da data da recolha dos dados / 2 anos a partir do fim da relação contratual*	*ex: situação familiar, dados do agregado familiar, estado civil*	*ex: 10 dias / 2 meses / 3 anos a partir da data da recolha dos dados / 2 anos a partir do fim da relação contratual*	*ex: CV, situação profissional, escolaridade, formação, distinções, diplomas*	*ex: 10 dias / 2 meses / 3 anos a partir da data da recolha dos dados / 2 anos a partir do fim da relação contratual*	*ex: vencimento, situação financeira, dados bancário, rendimentos, património*	*ex: 10 dias / 2 meses / 3 anos a partir da data da recolha dos dados / 2 anos a partir do fim da relação contratual*	*ex: endereços IP, logs, identificadores dos terminais, identificadores de ligação, dados de data e hora, dados de GPS, GSM, pontos wi-fi*	*ex: 10 dias / 2 meses / 3 anos a partir da data da recolha dos dados / 2 anos a partir do fim da relação contratual*	*ex: IP cookies de sessão, cookies de utilizador, cookies de terceiros, dados de navegação, device fingerprinting, medição de acesso a sites e interação através de ferramentas analíticas e de monitorização*	*ex: 10 dias / 2 meses / 3 anos a partir da data da recolha dos dados / 2 anos a partir do fim da relação contratual*	*ex: cor dos sapatos na festa de Natal*
T001																		
T002																		
T003																		
T004																		
T005																		
T006																		
T007																		
T008																		
T009																		
T010																		
T011																		
T012																		
T013																		
T014																		
T015																		
T016																		

Registro de Tratamiento de Datos

Art. 37. El responsable del tratamiento y el encargado mantendrán un registro de las operaciones de tratamiento de datos personales que lleven a cabo, especialmente cuando se basen en un interés legítimo.

	dados de navegação na internet		outras categorias de dados pessoais não sensíveis		perfis		Art.º 9.º, n.º 1			Art.º 10.º			Categorias dos titulares de dados						Fundamento de Licitude
rvação	Dados	prazo de conservação	Dados	prazo de conservação	Dados	prazo de conservação	sim/não	se sim, quais	prazo de conservação	sim/não	se sim, quais	prazo de conservação	Recursos Humanos	Clientes	Potenciais clientes	Fornecedores	Outros		
																	sim/não	se sim, quais	
meses / ir da a dos os a n da atual	*ex: IP cookies de sessão, cookies de utilizador, cookies de terceiros, dados de navegação, device fingerprinting, medição de acesso a sites e interação através de ferramentas analíticas e de monitorização*	*ex: 10 dias / 2 meses / 3 anos a partir da data da recolha dos dados / 2 anos a partir do fim da relação contratual*	*ex: cor dos sapatos na festa de Natal*	*ex: 10 dias / 2 meses / 3 anos a partir da data da recolha dos dados / 2 anos a partir do fim da relação contratual*	*ex: hábitos de vida, bom devedor, saudável*	*ex: 10 dias / 2 meses / 3 anos a partir da data da recolha dos dados / 2 anos a partir do fim da relação contratual*	*ex: sim*	*ex: origem racial ou étnica, opiniões políticas, convicções religiosas e filosóficas, filiação sindical, dados genéticos, dados biométricos (controlo de acesso físico, controlo de acesso lógico), dados sobre a saúde, a vida sexual e a orientação sexual*	*ex: 10 dias / 2 meses / 3 anos a partir da data da recolha dos dados / 2 anos a partir do fim da relação contratual*	*ex: sim*	*dados relativos às condenações e às infrações penais*	*ex: 10 dias / 2 meses / 3 anos a partir da data da recolha dos dados / 2 anos a partir do fim da relação contratual*	*ex: sim*	*ex: sim*	*ex: sim*	*ex: não*	*ex: sim*	*ex.: beneficiários / candidatos*	*ex: Consentimento, contrato, interesse legítimo, obrigação legal, prestação de serviços de saúd, interesse público ou exercício de autoridade pública*

Registro de Tratamiento de Datos

Art. 37. El responsable del tratamiento y el encargado mantendrán un registro de las operaciones de tratamiento de datos personales que lleven a cabo, especialmente cuando se basen en un interés legítimo.

#	dados dos destinatários			categorias de dados	categoria do destinatário	Se transferência internacional nos termos do artigo 49.º, n.º 1, segundo parágrafo, link para o documento que comprove a existência de garantias adequadas	Tratamentos a que se aplica por referência à finalidade
	nome da entidade	NIF	país				
C000a	*ex: Empresa destinatária 1*	*ex: NIF empresa 1*	*ex: Suíça*	*ex: nome, situação familiar, vencimento*	*ex: Subcontratante fora da UE*		*ex: T001*
C000b	*ex: Empresa destinatária 2*	*ex: NIF empresa 2*		*nome, vencimento, dados relativos às condenações*	*ex: Subcontratante dentro da EU/EEE*		*ex: T001*
C001							
C002							
C003							
C004							
C005							
C006							
C007							
C008							
C009							
C010							
C011							
C012							
C013							
C014							
C015							
C016							
C017							
C018							
C019							
C020							
C021							
C022							
C023							
C024							
C025							
C026							
C027							
C028							
C029							

Registro de Tratamiento de Datos

Art. 37. El responsable del tratamiento y el encargado mantendrán un registro de las operaciones de tratamiento de datos personales que lleven a cabo, especialmente cuando se basen en un interés legítimo.

# medida	tipo de medida	Medidas concretas	Tempo de conservação (se aplicável)	Tratamentos a que se aplica
M000a	*ex: Medidas de proteção lógica*	*ex: antivirus, palavras passe com utilização de no mínimo 8 caracteres alfanuméricos, implementação regular de atualizações de segurança, testes*		*ex: T000, T005, T011*
M000b	*ex: Controlo de acessos às instalações*	*ex: apenas utilizadores com cartão nominal da entidade podem aceder*		*ex: todos os tratamentos*
M000c	*ex: Registo de log*	*ex: logs de acesso e alteração ou eliminação de dados com identificador, data e hora da ligação, IP*	*ex: 2 anos*	*ex: T002 a T010*
M000d	*ex: Encriptação dos dados*	*ex: site acessível através de https, utilização de TLS, pseudonimização do campo data de nascimento*		*ex: T004*
M000e	*ex: Salvaguarda dos dados*	*ex: backups diários, redundância, plano de disaster recovery com centro alternativo*	*ex: os backups são conservados por 3 anos*	*ex: T012*
M001				
M002				
M003				
M004				
M005				
M006				
M007				
M008				
M009				
M010				
M011				
M012				
M013				
M014				
M015				
M016				
M017				
M018				
M019				
M020				
M021				
M022				
M023				
M024				
M025				

Informe de Impacto sobre la Protección de Datos Personales (RIPD)

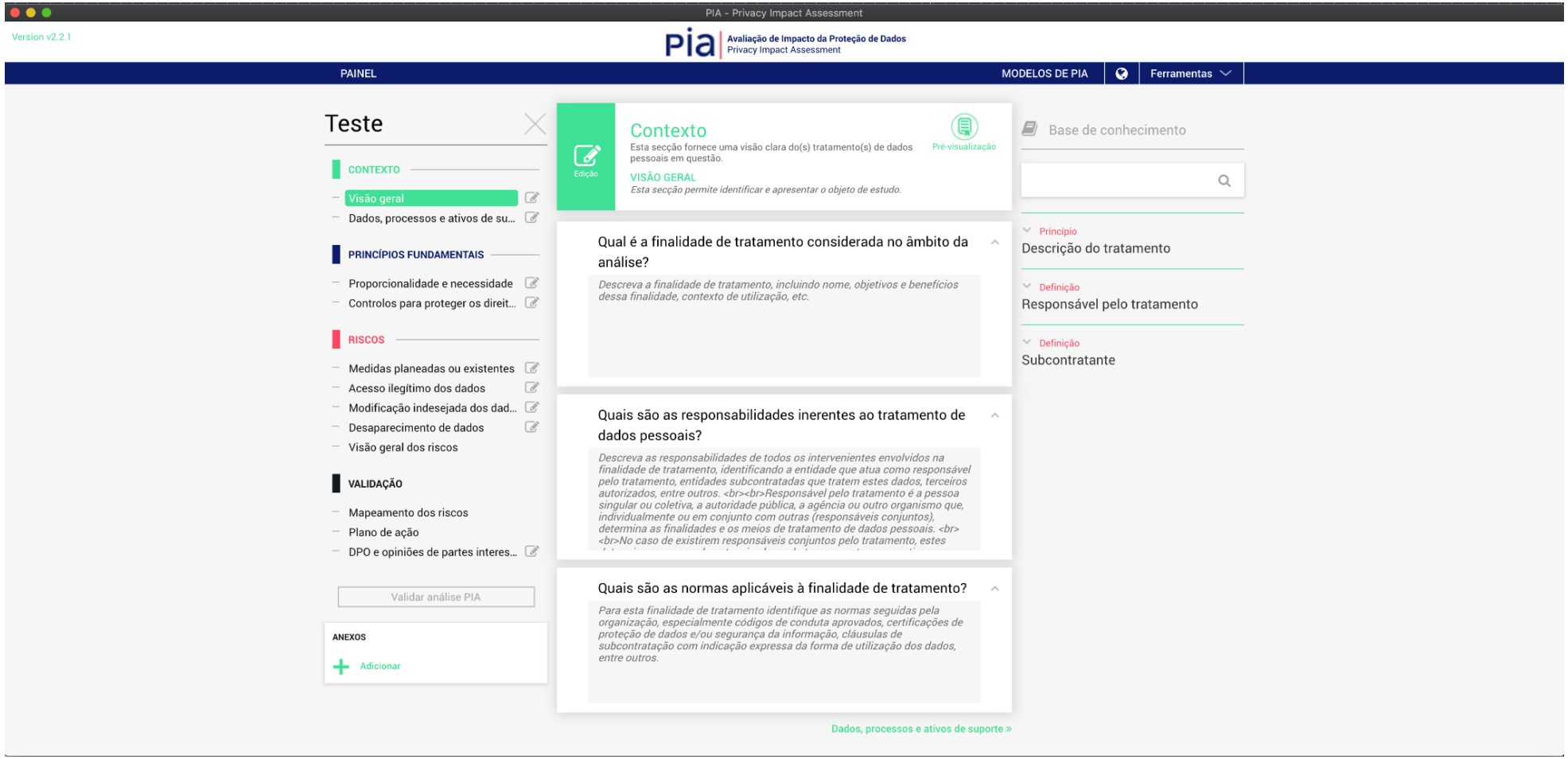
Art. 38. La autoridad nacional podrá exigir al responsable del tratamiento que elabore un informe sobre el impacto en la protección de los datos personales, incluidos los datos sensibles, relativo a sus operaciones de tratamiento de datos, de acuerdo con los términos del reglamento, siempre que se respeten los secretos comerciales e industriales.

- **Párrafo único**. Sin perjuicio de lo dispuesto en el encabezado de este artículo, el informe deberá contener al menos:
  - La descripción de los tipos de datos recolectados
  - La metodología utilizada para tratar y garantizar la seguridad de la información
  - El análisis del responsable del tratamiento en relación con las medidas
  - Salvaguardias y mecanismos de mitigación de riesgos adoptados

Informe de Impacto sobre la Protección de Datos Personales (RIPD)

- Software de código abierto de la CNIL: https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assessment
- Versiones para Mac, Windows, Linux, front-end, back-end.

Informe de Impacto sobre la Protección de Datos Personales (RIPD)



Informe de Impacto sobre la Protección de Datos Personales (RIPD)

Información de PIA

PIA
Análise de Pele com IA

Nome do autor
Dono do Projeto

Nome do assessor
Assessor do Dono do Projeto

Nome do validador
Matheus Silva (DPO)

Data de criação
04/09/2019

Nome do DPO
Matheus Silva

Modificación no deseada de datos

Quais poderiam ser os impactos nos dados dos titulares se o risco ocorrer?
Discriminação social em decorrência do tipo de pele, Uso de email para propaganda indesejada

Quais são as principais ameaças que poderiam levar ao risco?
Colaboradores desonestos, Colaboradores ma
equipamentos, Falhas em estruturas físicas, F

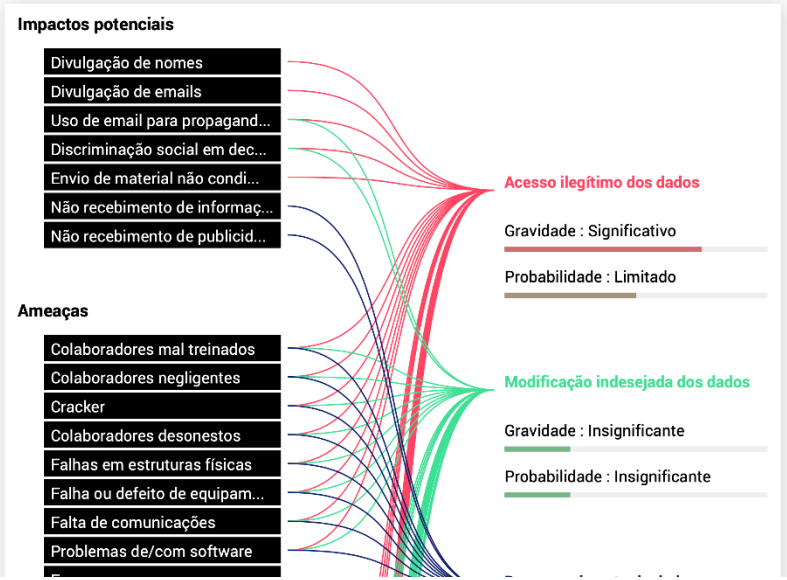
Quais são as fontesde risco?
Humanas intencionais, Humanas não intencio

Quais são os controlos identificados qu
Cifragem, Anonimização, Controlo de acesso
Gerenciamento de violações de dados pessoa

Como estimas a gravidade do risco, esp
planeados?
Insignificante,

Insignificante: os titulares dos dados não sera

Resumen de Riesgo

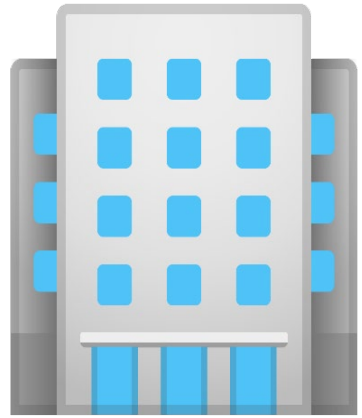


Responsable del Tratamiento y Encargado del Tratamiento

Art. 39. El llevará a cabo el tratamiento de acuerdo con las instrucciones dadas por el Responsable del tratamiento, que verificará el cumplimiento de sus instrucciones y de las normas pertinentes.

Responsable

Datos Personales



Encargado

Otras Obligaciones de los Responsables de los Datos Personales

- Información y transparencia
- Privacidad por diseño
- Contratos entre el Responsable del tratamiento y el Encargado del Tratamiento
- Medidas de seguridad
- Notificaciones en caso de violación de datos personales

Normas de Interoperabilidad

Art. 40. La autoridad nacional podrá establecer normas de interoperabilidad en cuanto a la portabilidad, el libre acceso a los datos y la seguridad, así como en cuanto a la duración de la conservación de los registros, teniendo especialmente en cuenta la necesidad y la transparencia.

El Responsable del Tratamiento de Datos Personales

Será tratado en el próximo módulo

Responsabilidad e Indemnización por Daños y Perjuicios

Reparación de Daños

Art. 42. El responsable del tratamiento o el Encargado que, en virtud del ejercicio de la actividad de tratamiento de datos personales, cause un daño patrimonial, moral, individual o colectivo a otra persona, en violación de la legislación sobre protección de datos personales, está obligado a repararlo.

- 1º Con el fin de garantizar una compensación efectiva al interesado:
  1. El Encargado responde solidariamente de los daños y perjuicios causados por el tratamiento cuando incumpla las obligaciones de la normativa de protección de datos o cuando no haya seguido las instrucciones legales del Responsable del Tratamiento, en cuyo caso el Responsable se equipara al Encargado del Tratamiento, salvo en los supuestos de exclusión previstos en el artículo 43 de esta Ley
  2. Los Responsables del Tratamiento directamente implicados en el tratamiento que causó el daño al interesado son responsables solidarios, salvo en los casos de exclusión previstos en el artículo 43 de esta Ley

Reparación de Daños

- 2º El juez, en el proceso civil, podrá invertir la carga de la prueba a favor del titular de los datos cuando, a su juicio, la alegación sea verosímil, cuando exista falta de suficiencia para la aportación de pruebas, o cuando la aportación de pruebas por parte del titular le resulte excesivamente onerosa
- 3º Las acciones de resarcimiento de daños colectivos que tengan por objeto la rendición de cuentas conforme al encabezado de este artículo podrán ser ejercidas colectivamente ante los tribunales, observando lo dispuesto en la legislación pertinente
- 4º La persona que repara el daño al propietario tiene derecho a volver contra los demás responsables, en la medida de su participación en el hecho dañoso

¿Cuándo no se exigirán responsabilidades a los agentes del tratamiento?

Art. 43. Los agentes del tratamiento no serán responsables cuando demuestren:

1. Que no han realizado el tratamiento de los datos personales que se les atribuyen
2. Que, aunque hayan realizado el tratamiento de los datos personales que se les atribuyen, no se ha infringido la normativa de protección de datos
3. Que el daño se produzca por culpa exclusiva del interesado o de un tercero

¿Cuándo se considera que el tratamiento es ilícito?

Art. 44. El tratamiento de datos personales será ilícito cuando no se ajuste a la ley o cuando no proporcione la seguridad que el interesado pueda esperar de él, teniendo en cuenta las circunstancias pertinentes, entre ellas:

1. La forma en que se lleva a cabo;
2. El resultado y los riesgos que razonablemente se esperan de él;
3. Las técnicas de tratamiento de datos personales disponibles en el momento de su realización.

- **Párrafo único**. El Responsable del Tratamiento o el Encargado del Tratamiento que, al no adoptar las medidas de seguridad previstas en el art. 46 de esta Ley, cause el daño, será responsable de los perjuicios derivados de la violación de la seguridad de los datos

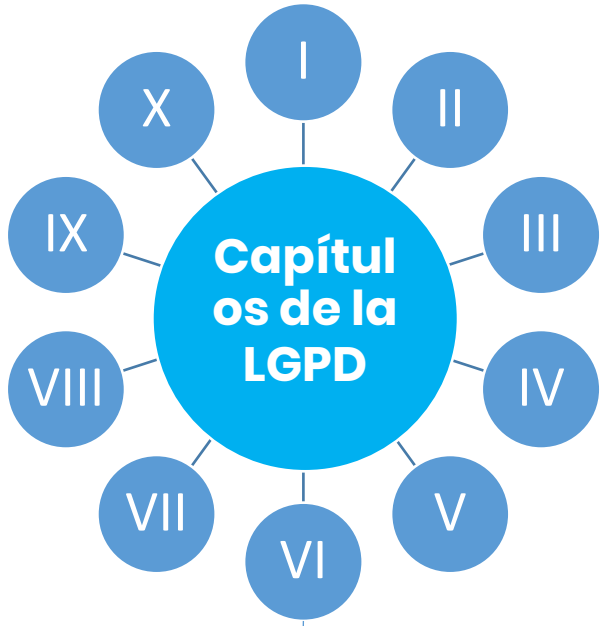
Violación del Derecho del Titular

Art. 45. Los casos de violación del derecho del titular en el ámbito de las relaciones de consumo quedan sujetos a las normas de responsabilidad previstas en la legislación vigente.

Módulo 8: Oficial (DPO)

LGPDF™ Versión 102021

¿En qué parte de la ley estamos?



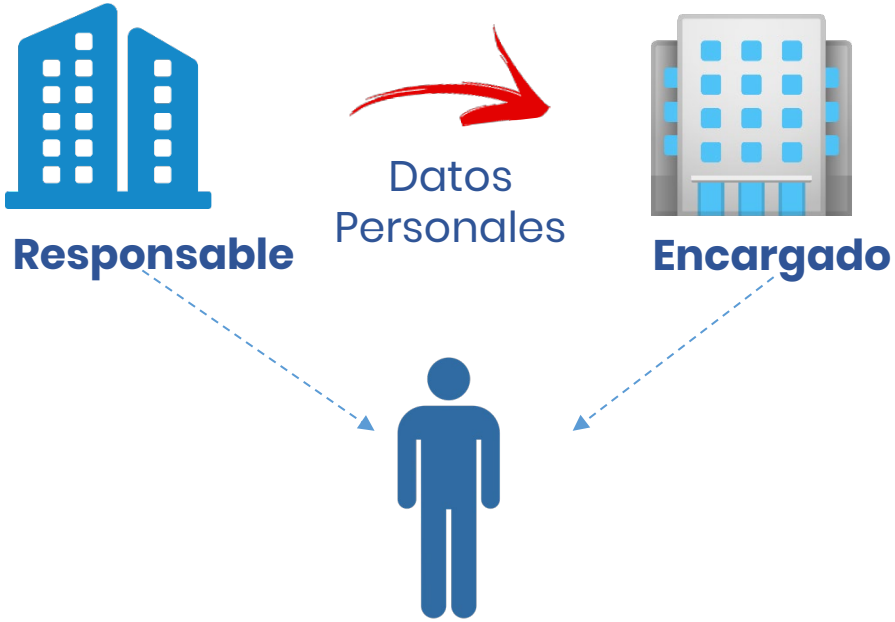
CAPÍTULO VI – AGENTES DE TRATAMIENTO DE DATOS PERSONALES

Artículos 37 a 45 Sección I - Responsable y Encargado - artículos 37 a 40
Sección II - Oficial del Tratamiento de Datos Personales - artículo 41 Sección III - Responsabilidad e Indemnización por Daños - artículos 42 a 45

Recordando

Art. 5º Para los efectos de esta Ley, se considera:

- **VIII – Oficial**: Persona designada por el responsable y el encargado para actuar como canal de comunicación entre el responsable, los interesados y la Autoridad Nacional de Protección de Datos (ANPD)



¡Consejo práctico!

Estudio de Caso Público: ANPPD.org

El Portal de la ANPPD centraliza de forma minimizada la mayor base de datos de Profesionales de la Privacidad de Brasil, en la que se puede buscar el Oficial deseado (DPO) y que ya ha sido evaluado por la ANPPD, que es la mayor asociación de clase de América Latina. Muchas empresas están utilizando esta preevaluación en sus procesos de selección, así como los profesionales que se ofrecen al mercado.

La certificación LGPDF es reconocida y aceptada por la ANPPD para su ingreso.

Nombramiento de un Oficial

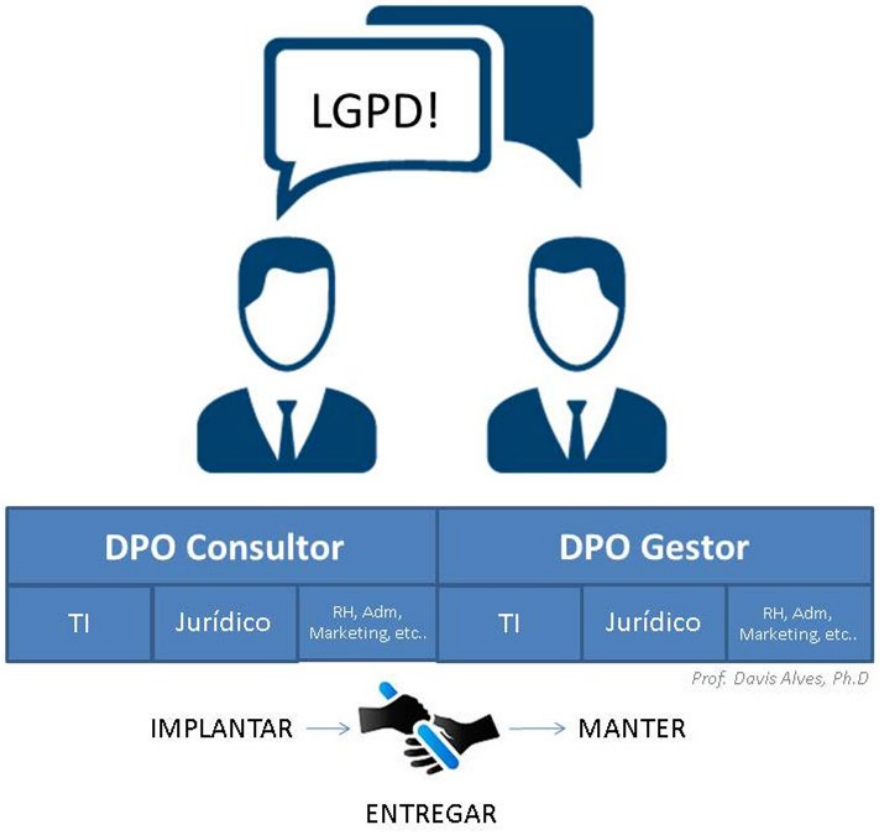
- Art. 41. El responsable del tratamiento nombrará a un Oficial para el tratamiento de los datos personales.

  Inc. 1. La identidad y la información de contacto del responsable del tratamiento deben hacerse públicas, de forma clara y objetiva, preferiblemente en el sitio web del responsable del tratamiento.

  También se habla de otros términos como "responsable de la protección de datos".

  Entre las diferencias técnicas entre el "Oficial" y el "DPO", se destaca que mientras el DPO tiene un carácter más técnico, el Oficial en la LGPD se define positivamente como "Comunicador". Sin embargo, aun así, el término "DPO" es conocido por muchos profesionales de la privacidad de datos en Brasil.

  En este material, lo siguiente es el equivalente del término popular.



Fuente: Davis Alves, Ph.D

Nombramiento de un Oficial

¡#LGPDNews! - No se pierdan la oportunidad.

El 29 de julio de 2021 la ocupación de DPO/Procesador de Datos fue oficialmente incluida y reconocida en la CBO - Clasificación Brasileña de Ocupaciones. Las reuniones, entrevistas y detalles de la nueva profesión, se venían discutiendo desde principios de ese año entre FIPE/CBO del Ministerio de Economía (ahora Ministerio de Trabajo), y ANPPD® - Asociación Nacional de Profesionales de la Privacidad de Datos a través de la presidencia y miembros participantes que ya actúan como DPO en la práctica.

Fuente:https://www.linkedin.com/posts/anppd_lgpdnews-anppdmerepresenta-lgpdconnect2021-activity-6826842880909352960-tKk2

¿Quién puede ser Oficial (DPO)?

Inicialmente, el texto original de la LGPD establecía que el titular sería una "persona física". Sin embargo, la palabra "persona física" fue eliminada por la Medida Provisional Nº 869 y este cambio fue confirmado por la Ley 13.853/2019. Por lo tanto, podemos suponer:

Actividades del Oficial

Art. 41.

- Inc. 2. Las actividades del funcionario Oficial consisten en:
  I. Aceptar las quejas y las comunicaciones de los titulares, aportar aclaraciones y adoptar medidas.
  II. Recibir comunicaciones de la autoridad nacional y tomar medidas.
  III. Orientar a los empleados y contratistas de la entidad sobre las prácticas a adoptar en materia de protección de datos personales.
  IV. Realizar las demás atribuciones que determine el interventor o que se establezcan en normas complementarias.
- Inc. 3. La autoridad nacional podrá establecer normas complementarias sobre la definición y las funciones del responsable, incluidos los casos de exención de la necesidad de indicarlo, de acuerdo con la naturaleza y el tamaño de la entidad o el volumen de las operaciones de tratamiento de datos.

Un DPO Puede Atender a Varias Organizaciones

- Tanto la LGPD como el GDPR permiten que un DPO preste servicio a múltiples organizaciones.
- Es importante que sea fácilmente accesible para todas las organizaciones a las que asiste.

¿Qué conocimientos y habilidades debe tener un DPO?

Calificaciones Recomendadas

- El "mito" del DPO legal y del DPO técnico.
- No hay separación entre lo "legal" y lo "técnico": hay protección de datos. El profesional debe tener sólidos conocimientos en ambas áreas, así como conocer el negocio.
- Ejemplos de multas en la UE en 2019 por incumplimiento de cada uno de los puntos anteriores:
- Infracciones del artículo 6 (bases legales): 27 multas, total 19.257.894 euros.
- Infracciones del artículo 32 (seguridad): 22 multas, total 6.526.027 euros.
- Excluidos: multas a Marriott International (110,4M) y British Airways (204,6M de seguridad) y Google (50M de bases legales) por estar "puntos fuera de la curva" (casos excepcionales) - Marriott y BA aún en juicio, Google - decisión ya definitiva.

Calificaciones Recomendadas

El GDPR y la LGPD no establecen las cualificaciones mínimas requeridas para la actividad. Sin embargo, hay ciertos atributos y conocimientos recomendados para esta función:

Fuente: adaptado del Reglamento General de Protección de Datos de la UE (RGPD). Una guía de implementación y cumplimiento, ITGP

¿Dónde están los DPO en el mundo?

IAPP.org

EADPP.eu

APDPO.pt

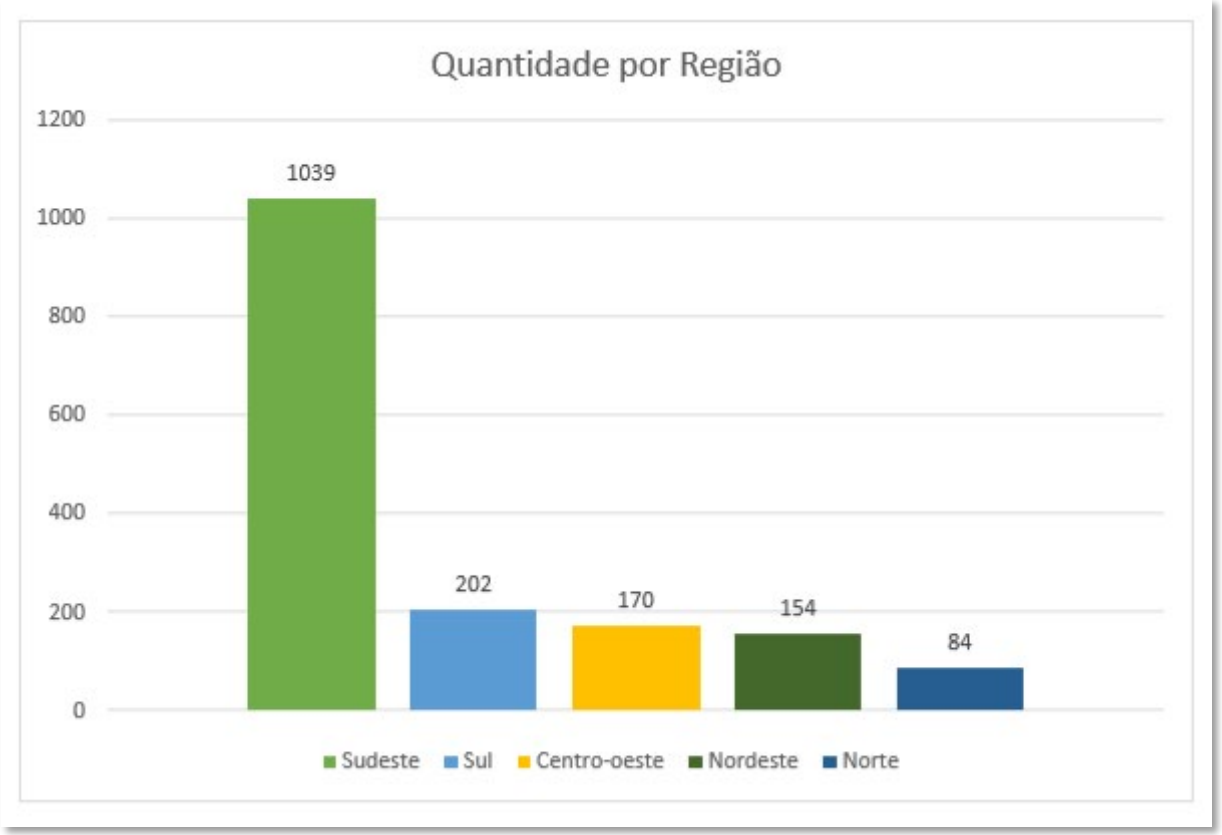
ANPPD.org

=======➔

Asociaciones de profesionales de protección de datos

Perfil de DPO en Brasil (ANPPD, 2020)

Profesionales de privacidad de datos en Brasil

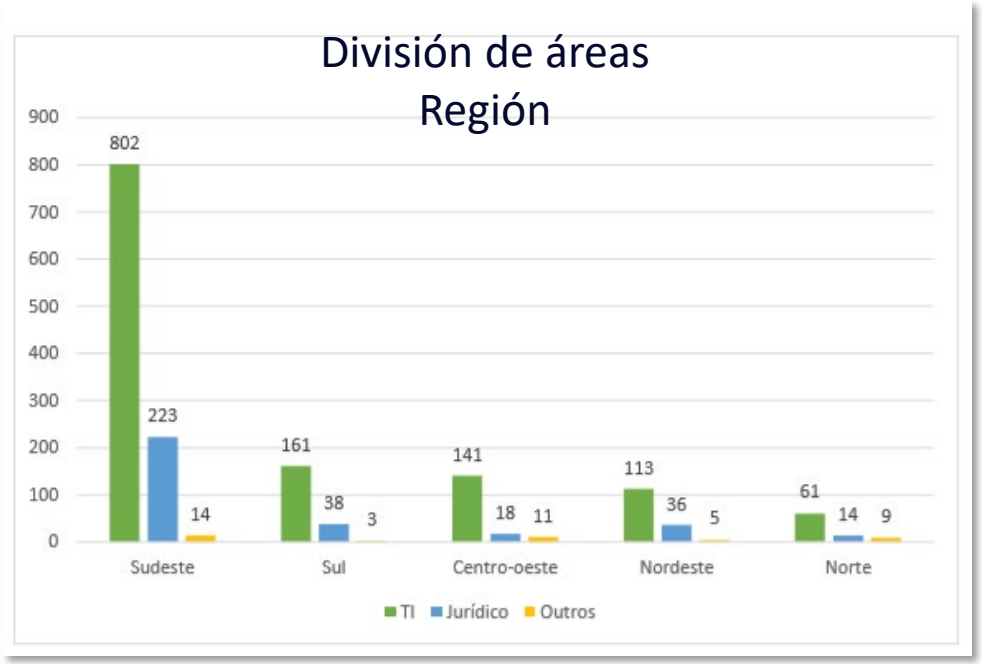


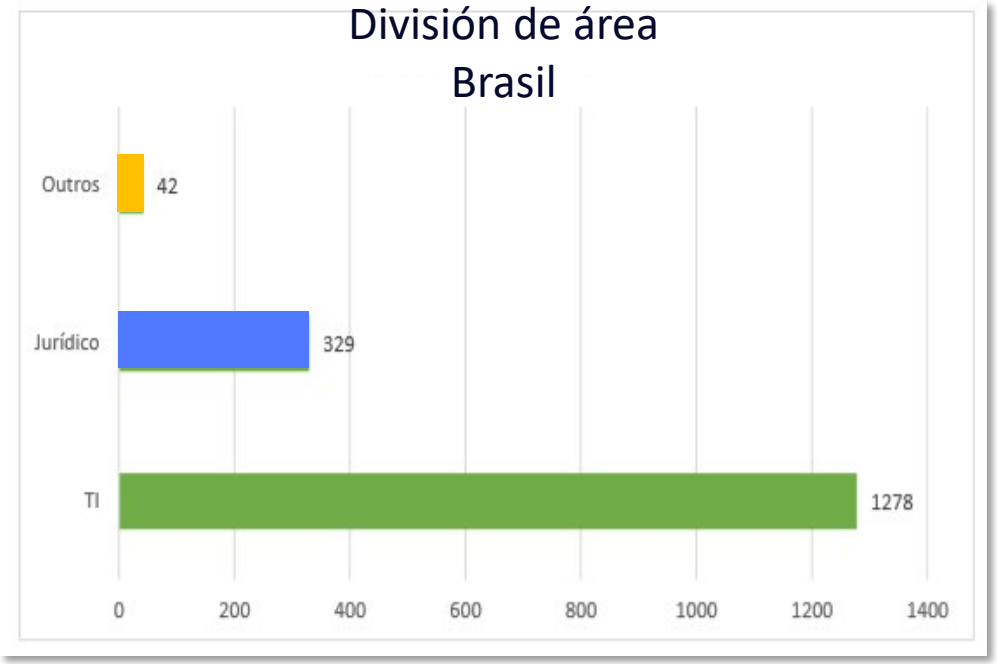
* Más de 30.000 seguidores en LinkedIn en 2021

1.649 aprobados como Miembros de la ANPPD en 2020, y más de 10.000 en 2021.

Perfil de DPO en Brasil (ANPPD, 2020)

Profesionales de la protección de datos en Brasil



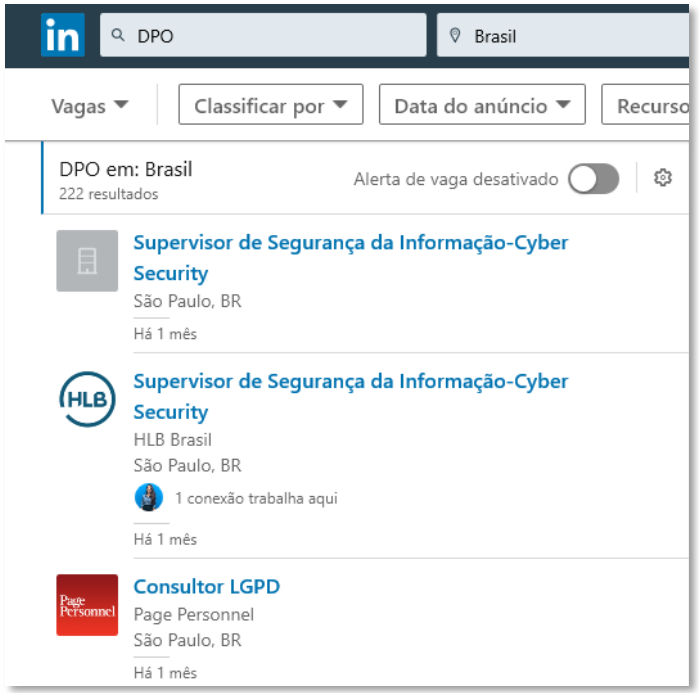


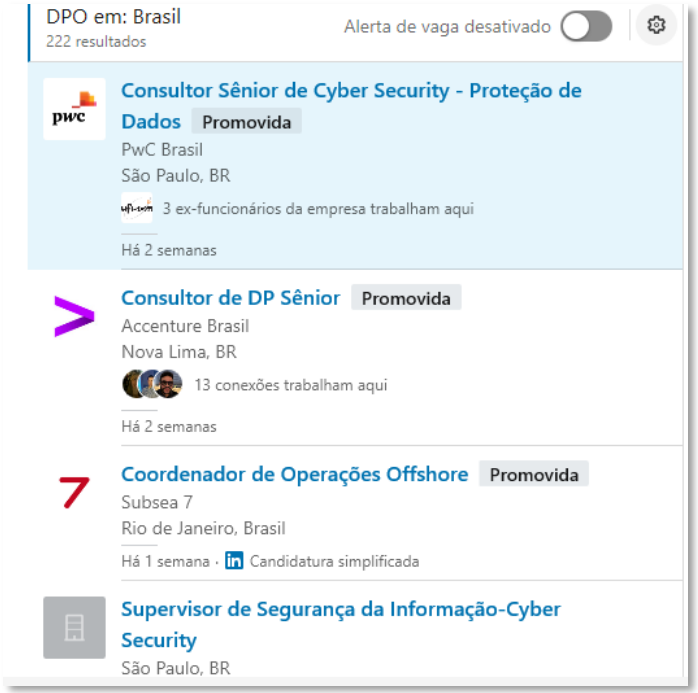
DPOs en Brasil
1649 aprobados en 2020, y más de 10.000 en 2021.
anppd.org

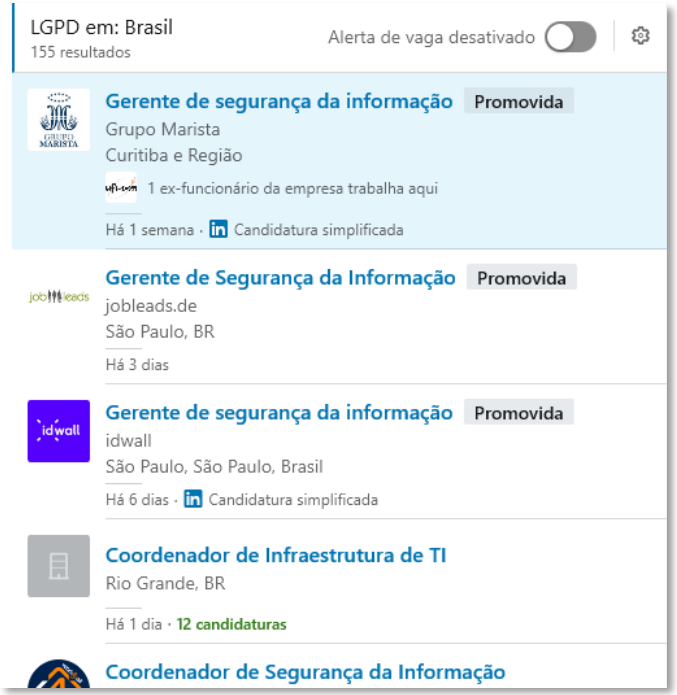
Perfil del DPO en Brasil (ANPPD, 2020)

Ofertas de empleo de DPO, Responsables, Oficiales de Protección de Datos

- Salario medio DPO:
  - Consultor: R$350,00 a R$550,00 p/hora – (referencia OAB, Tabla IBAPE)
  - Gestor interno: R$ 8.000,00 a R$ 20.000,00 – (referencia al GDPR en Números)







04/05/2020

17 Habilidades Específicas para un DPO

Según el esquema de certificación de DPO propuesto por la CNIL (Autoridad de Francia), hay 17 conocimientos específicos que debe tener un DPO:

1. Entender y comprender los principios de legalidad del tratamiento, limitación de la finalidad, minimización de los datos, exactitud de los datos, conservación limitada de los datos, integridad, confidencialidad y responsabilidad
2. Saber identificar la base jurídica de un tratamiento
3. Saber determinar las medidas y el contenido adecuados de la información que se debe proporcionar a los interesados
4. Saber establecer procedimientos para recibir y gestionar las solicitudes de ejercicio de los derechos de los interesados
5. Conocer el marco legal relacionado con la externalización del tratamiento de datos personales
6. Saber identificar la existencia de transferencias de datos fuera del país y determinar los instrumentos legales de transferencia que pueden utilizarse

Fuente: https://www.legifrance.gouv.fr/

17 Habilidades Específicas para un DPO

7. Saber cómo elaborar y aplicar una política o normativa interna de protección de datos
8. Saber organizar y participar en auditorías de protección de datos
9. Conocer el contenido del registro de actividades de tratamiento, la categoría del registro de actividades de tratamiento y la documentación de las violaciones de datos, así como la documentación necesaria para demostrar el cumplimiento de la normativa de protección de datos
10. Saber identificar las medidas de protección de datos por diseño y, por defecto, adaptadas a los riesgos y a la naturaleza de las operaciones de tratamiento
11. Saber participar en la identificación de las medidas de seguridad adecuadas a los riesgos y a la naturaleza de las operaciones de tratamiento
12. Saber identificar las violaciones de datos personales que requieren notificación a la autoridad de control y las que requieren comunicación con los interesados

Fuente: https://www.legifrance.gouv.fr/

17 Habilidades Específicas para un DPO

13. Saber si es necesaria o no una evaluación de impacto sobre la protección de datos (EIPD) y cómo verificar su realización
14. Asesorar sobre la evaluación de impacto de la protección de datos (especialmente sobre la metodología, la posible externalización y las medidas técnicas y organizativas que deben adoptarse)
15. Saber gestionar las relaciones con las autoridades de supervisión, respondiendo a las solicitudes y facilitando las acciones (investigación de quejas y controles en particular)
16. Ser capaz de desarrollar, aplicar e impartir programas de formación y concienciación para el personal y la alta dirección sobre la protección de datos
17. Saber cómo garantizar la trazabilidad de sus actividades, especialmente con la ayuda de herramientas de seguimiento o de informes anuales

Fuente: https://www.legifrance.gouv.fr/

Algunas Normas que debe Conocer un DPO en Brasil

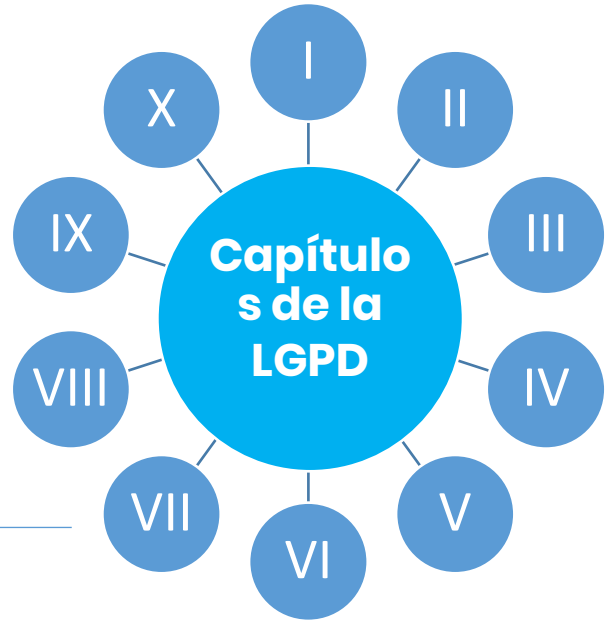
Es imprescindible conocer los plazos de conservación de los documentos fiscales, mercantiles, laborales y de seguridad social de acuerdo con la legislación vigente.

Consulte aquí

Módulo 9: Seguridad y Buenas Prácticas – Teoría y Práctica

LGPDF™ Versión 102021

¿En qué parte de la ley estamos?



CAPÍTULO VII – SEGURIDAD Y BUENAS PRÁCTICAS

Artículos 46 a 51
Sección I - Seguridad y secreto de los datos - artículos 46 a 49
Sección II - Buenas prácticas y gobernanza - artículos 50 y 5

Seguridad y secreto de los datos

Adopción de Medidas

Art. 46. Los Oficiales del tratamiento adoptarán las medidas de seguridad de índole técnica y administrativa para proteger los datos personales del acceso no autorizado y de situaciones accidentales o ilícitas de destrucción, pérdida, alteración, comunicación o cualquier forma de tratamiento inadecuado o ilícito.

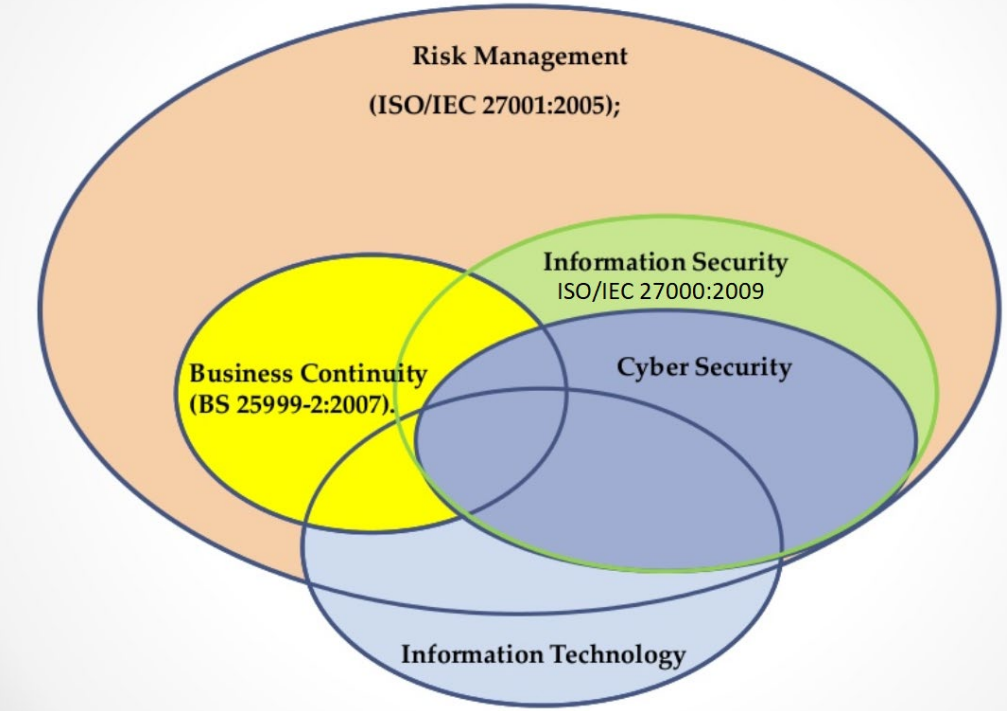
Art. 47. Los Oficiales del tratamiento o cualquier otra persona que intervenga en alguna de las fases del mismo estarán obligados a garantizar la seguridad de la información prevista en esta Ley en relación con los datos personales, incluso después de su cese.

Adopción de Medidas

Seguridad de la información

3 tipos de medidas de seguridad:

- SEGURIDAD FÍSICA
- SEGURIDAD TÉCNICA
- SEGURIDAD DE LA ORGANIZACIÓN



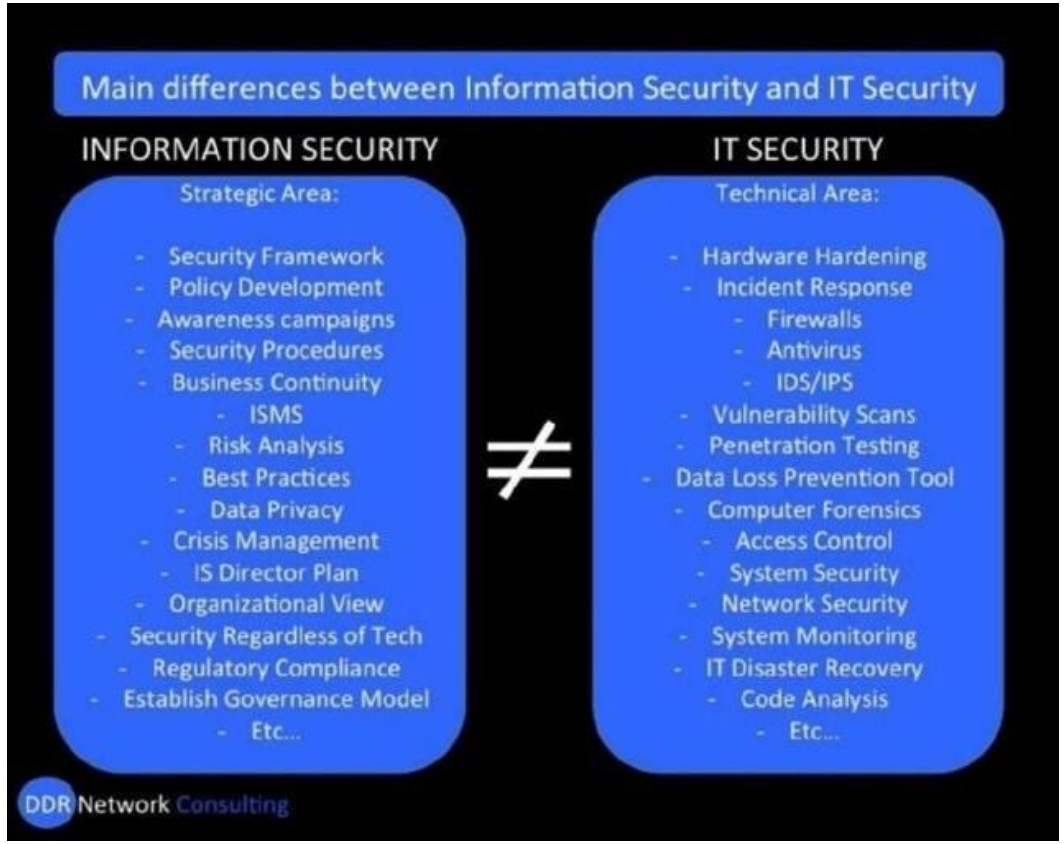
Fuente: 51sec.org (2020)

Adopción de Medidas

Seguridad de la información

3 tipos de medidas de seguridad:

- SEGURIDAD FÍSICA
- SEGURIDAD TÉCNICA
- SEGURIDAD DE LA ORGANIZACIÓN



Notificación de Incidentes de Seguridad

Art. 48 El responsable del tratamiento comunicará a la autoridad nacional y al titular la ocurrencia de un incidente de seguridad que pueda causar un riesgo o daño relevante a los titulares.

Inc. 1 La comunicación se hará en un plazo razonable, definido por la autoridad nacional, y mencionará, como mínimo

1. Una descripción de la naturaleza de los datos personales afectados
2. información sobre los sujetos de los datos implicados
3. indicación de las medidas técnicas y de seguridad utilizadas para la protección de los datos, sin perjuicio de la confidencialidad comercial e industrial
4. Los riesgos relacionados con el incidente
5. los motivos del retraso, en caso de que la comunicación no sea inmediata
6. Las medidas que se han adoptado o se adoptarán para revertir o mitigar los efectos de los daños

Art. 49 - Los sistemas utilizados para el tratamiento de datos personales deberán estar estructurados de forma que cumplan los requisitos de seguridad, las normas de buenas prácticas y gobernanza y los principios generales previstos en esta Ley y demás normas reguladoras.

Buenas Prácticas y Gobernanza

Buenas Prácticas y Gobernanza

Art. 50 - Los responsables y encargados, en el ámbito de sus competencias, del tratamiento de datos personales, individualmente o a través de asociaciones, podrán formular normas de buenas prácticas y de gobernanza que establezcan las condiciones de organización, el régimen de funcionamiento, los procedimientos, incluidas las reclamaciones y peticiones de los interesados, las normas de seguridad, los estándares técnicos, las obligaciones específicas para los distintos intervinientes en el tratamiento, las acciones educativas, los mecanismos de supervisión interna y mitigación de riesgos y otros aspectos relacionados con el tratamiento de datos personales.

Inc. 2 En aplicación de los principios indicados en los puntos VII y VIII de la frase de encabezamiento del artículo 6 de esta Ley, el responsable del tratamiento, observando la estructura, la escala y el volumen de sus operaciones, así como la sensibilidad de los datos tratados y la probabilidad y gravedad de los daños a los interesados, podrá

I - implementar un programa de gobierno de la privacidad que, como mínimo:

a) Demuestra el compromiso del responsable del tratamiento de adoptar procesos y políticas internas que garanticen el cumplimiento, de forma exhaustiva, de las normas y buenas prácticas en materia de protección de datos personales
b) Es aplicable a todo el conjunto de datos personales bajo su control, independientemente de cómo se hayan recogido
c) se adapte a la estructura, escala y volumen de sus operaciones y a la sensibilidad de los datos que se procesan
d) Establece políticas y salvaguardias adecuadas basadas en un proceso de evaluación sistemática de los impactos y riesgos para la privacidad

Buenas Prácticas y Gobernanza

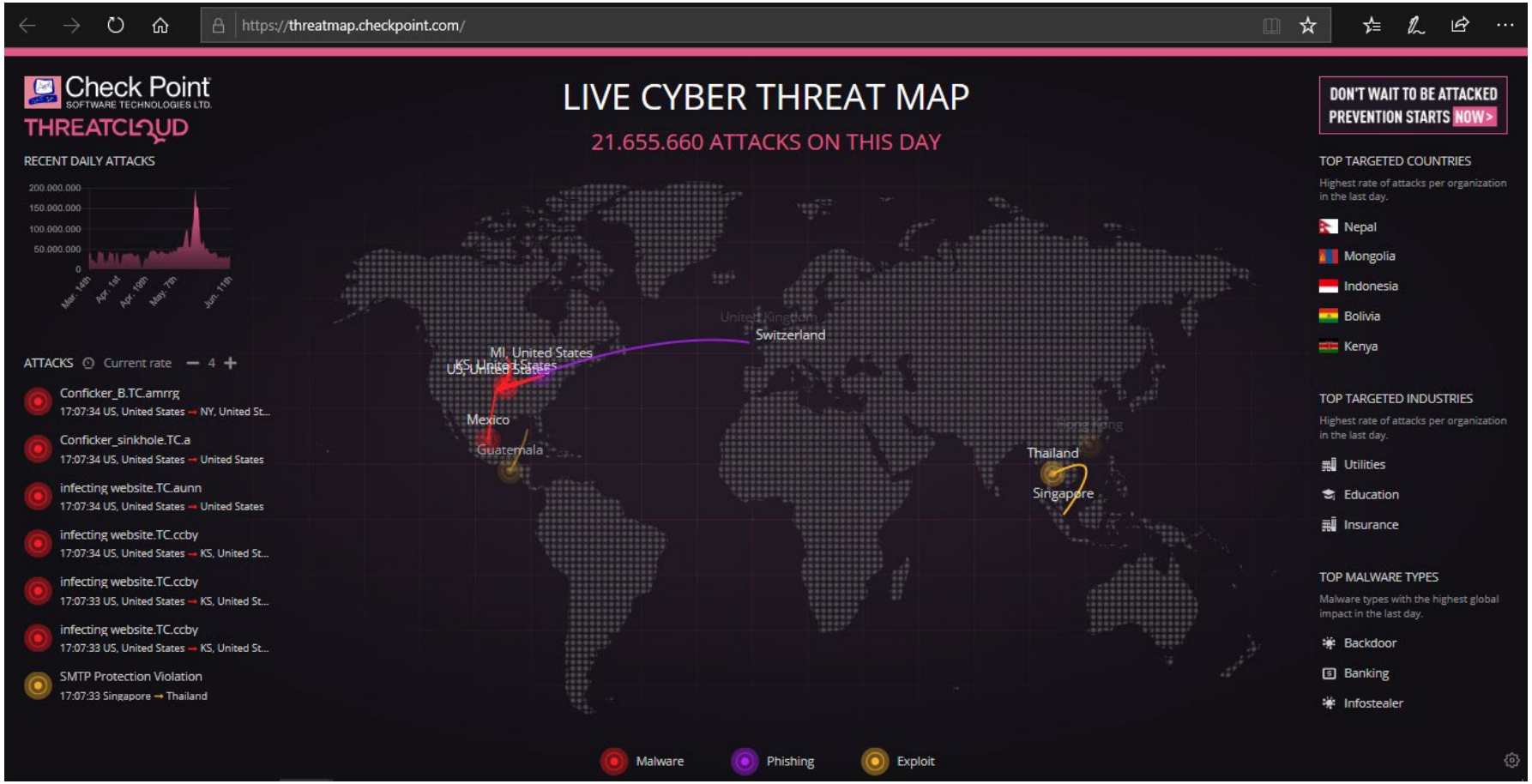
e) Pretende establecer una relación de confianza con el titular de los valores, a través de acciones transparentes que aseguren mecanismos de participación del titular
f) Se integra en su estructura general de gobierno y establece y aplica mecanismos de supervisión interna y externa
g) Tiene planes de respuesta a incidentes y de reparación
h) Se actualiza constantemente sobre la base de la información obtenida a partir del seguimiento continuo y las evaluaciones periódicas

Objetivos de los Controles de la ISO 27001

Los controles son todas las medidas administrativas, de procedimiento y tecnológicas que deben adoptarse.

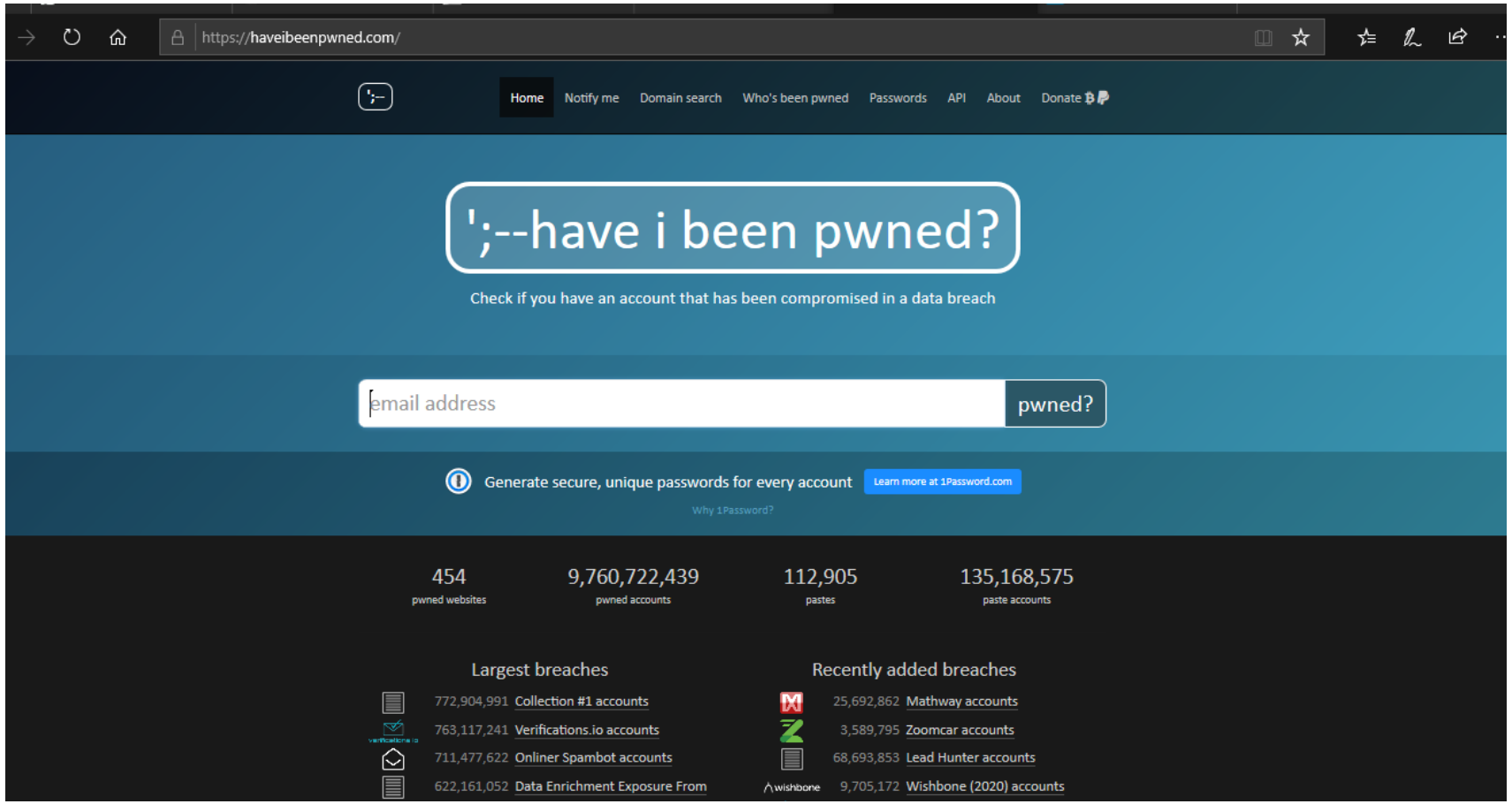
- Implementación de OSM
- Políticas de seguridad
- Organización de la Información
- Gestión de activos
- Control de acceso
- Criptografía
- Seguridad física y ambiental
- Seguridad de las operaciones
- Adquisición, Desarrollo y Mantenimiento de Sistemas
- Transferencia de información
- Relación con Proveedores
- Gestión de incidentes de seguridad
- Continuidad del negocio
- Cumplimiento de los requisitos legales y contractuales

Ciberataques en Tiempo Real



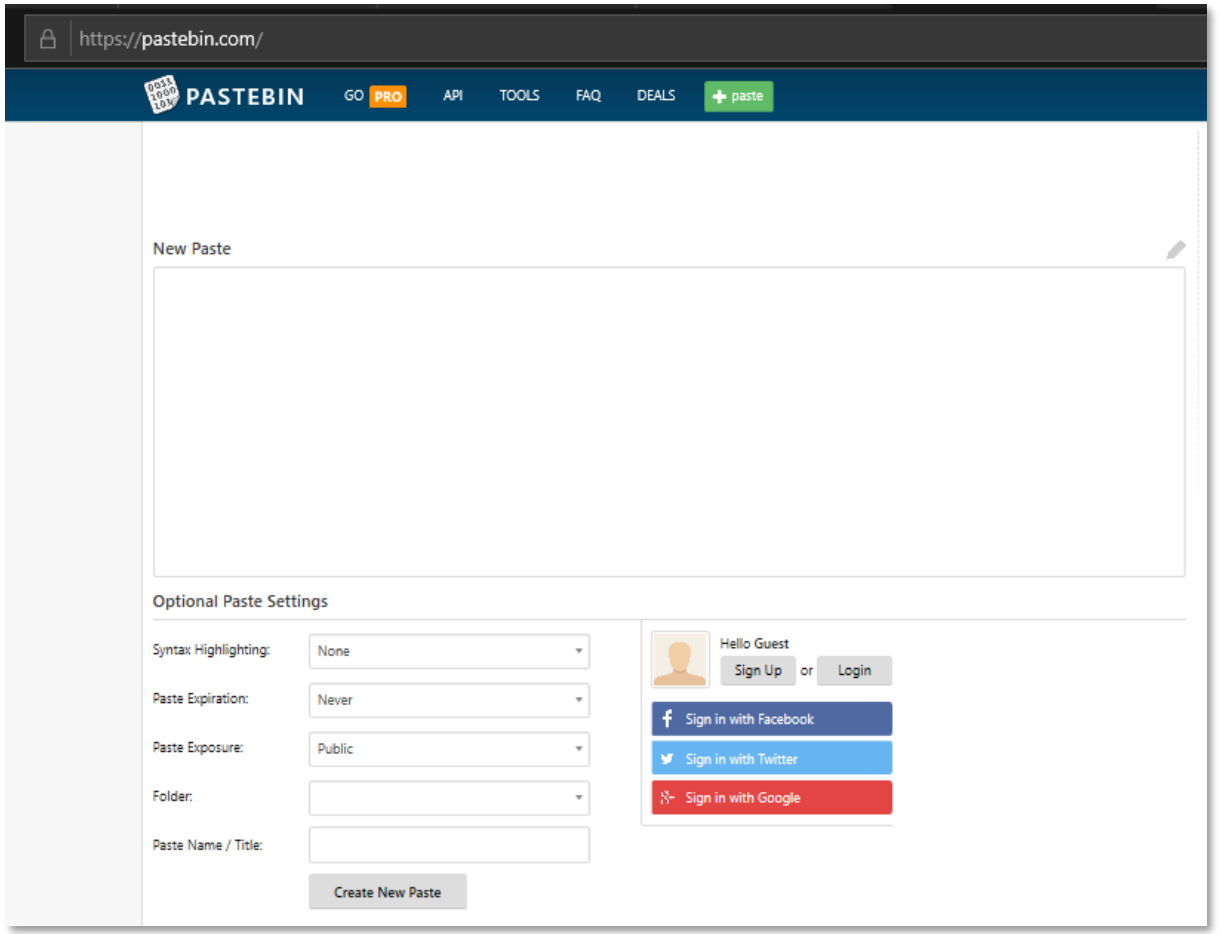
https://threatmap.checkpoint.com/

¿Alguna vez me han filtrado datos personales?



https://haveibeenpwned.com/

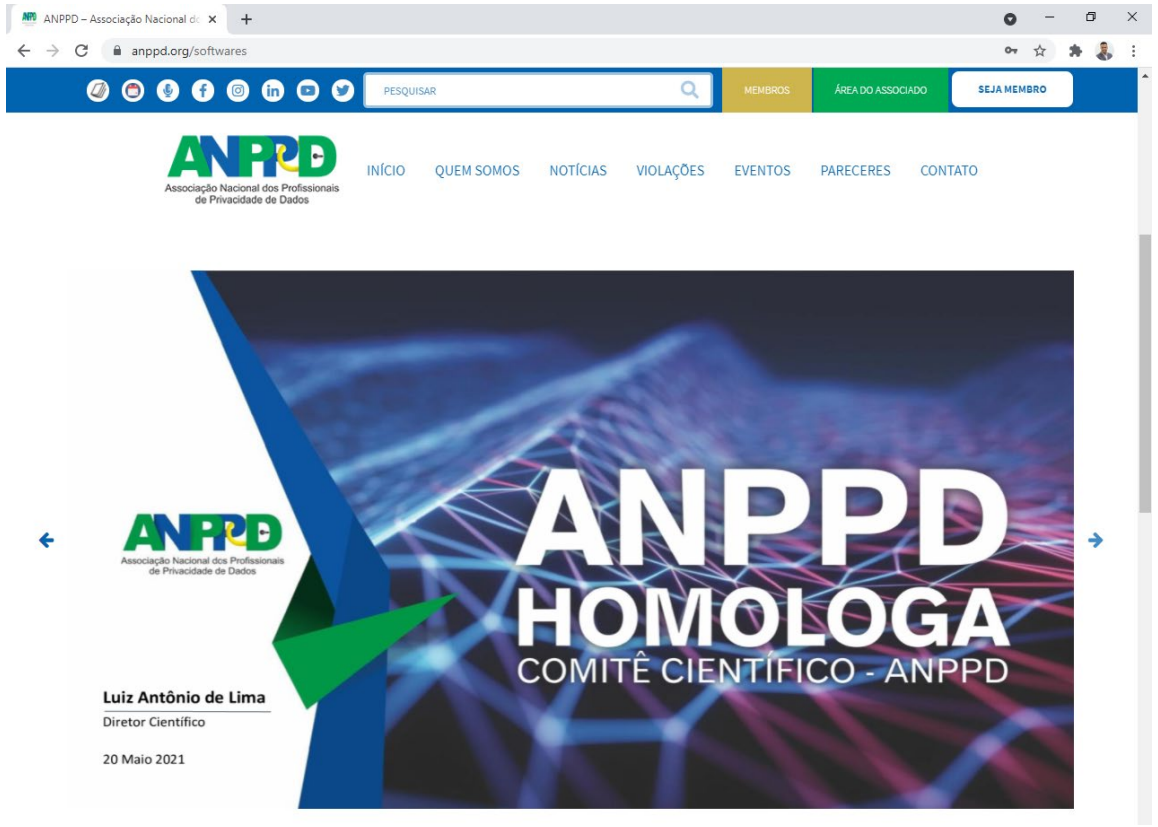
¿Alguna vez me han filtrado datos personales?



https://pastebin.com/

¿Dónde buscar las herramientas de la LGPD?

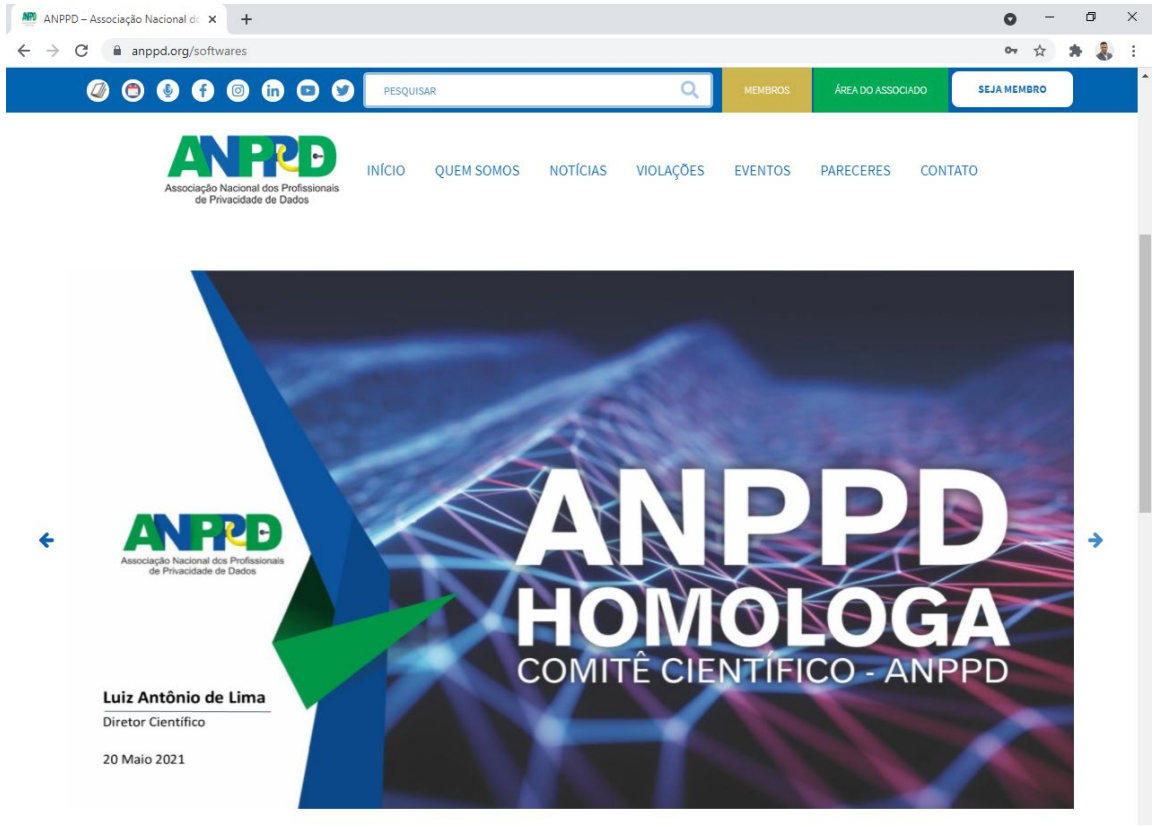
El Programa de Aprobación de Software de la ANPPD es un proceso desarrollado por el Comité Científico reconocido internacionalmente en las revistas científicas: "KES - Knowledge-Based and Intelligent Information & Engineering Systems: Elsevier's Procedia Computer Science Open Access Journal, Science Direct; Web of Science, Scopus". Este proceso verifica a través de las evidencias generadas por el software con la adhesión de la empresa a la LGPD, GDPR, ISO-27001, ISO-27701 y otros indicadores. Después de todo el proceso la herramienta recibe el CHANCEL/Sello que es ANPPD Oro, ANPPD Plata o ANPPD Bronce, dependiendo del resultado verificado.



https://anppd.org/softwares

¿Dónde buscar las herramientas de la LGPD?

Este sello se entrega junto con el Certificado de Homologación, a distancia o en persona en la sede de la empresa propietaria de la herramienta. Las pruebas de cumplimiento están sujetas a verificación pública en la Casa del Software y se registran en la ANPPD, respetando todos los secretos industriales. El Programa de Homologación de la ANPPD está dirigido por maestros y doctores especializados en LGPD/GDPR, y utiliza las metodologías científicas: Investigación en Ciencias del Diseño (HEVNER et al. 2007) y estudio de casos (GIL, 2008), dividiéndose en 3 fases de auditoría: a) Análisis documental, b) Entrevistas y c) Observación directa (GIL, 2008). Este proceso de homologación es un servicio que presta la ANPPD a la sociedad con el fin de mostrar al mercado las mejores opciones de software científicamente verificadas.



https://anppd.org/softwares

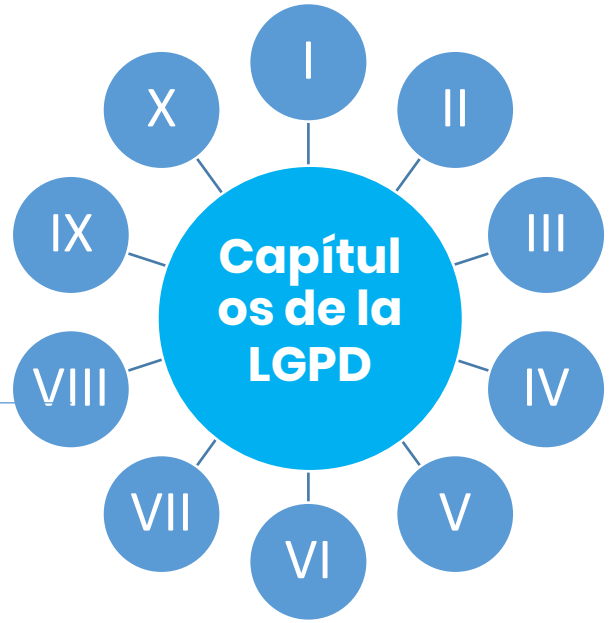
Módulo 10: Sanciones Administrativas

LGPDF™ Versión 102021

¿En qué parte de la ley estamos?

CAPÍTULO VIII – INSPECCIÓN

Sección I - Sanciones administrativas - Artículos 52 a 54



Rendición de Cuentas

Art. 48 El responsable del tratamiento comunicará a la autoridad nacional y al interesado la ocurrencia de un incidente de seguridad que pueda suponer un riesgo o daño relevante para los interesados.

- Una descripción de la naturaleza de los datos personales afectados
- Información sobre los interesados
- Una indicación de las medidas técnicas y de seguridad utilizadas para la protección de datos
- Los riesgos relacionados con el incidente
- Las razones del retraso, cuando la comunicación no fue inmediata
- Las medidas que se han adoptado o se adoptarán para revertir o mitigar los efectos del daño

Aplicación de las Sanciones Administrativas

-> ¿Quién se presenta? Autoridad Nacional de Protección de Datos (ANPD)

Art. 55-K. La aplicación de las sanciones previstas en esta Ley corresponderá exclusivamente a la ANPD, y sus competencias prevalecerán, en materia de protección de datos personales, sobre las competencias conexas de otras entidades u órganos de la administración pública.

Sanciones Previstas

Art. 52 - Los Oficiales del tratamiento de datos, como consecuencia de las infracciones de las normas previstas en la presente Ley, estarán sujetos a las siguientes sanciones administrativas aplicables por la autoridad nacional

I. Advertencia, con indicación del plazo para la adopción de medidas correctoras
II. Multa simple de hasta el 2% (dos por ciento) del volumen de negocios de la persona jurídica privada, grupo o conglomerado en Brasil en su último ejercicio, sin incluir impuestos, con un límite de R USD 9,5M por infracción
III. Multa diaria, con el límite total mencionado en el punto II
IV. Publicación de la infracción después de haber comprobado y confirmado debidamente su ocurrencia
V. Bloqueo de los datos personales a los que se refiere la infracción hasta su regularización
VI. Supresión de los datos personales a los que se refiere la infracción

Criterios de Aplicación de las Sanciones

Art. 52. Inc. 1. Las sanciones se aplicarán tras un procedimiento administrativo que prevea una amplia oportunidad de defensa, de forma gradual, aislada o acumulativa, según las peculiaridades del caso concreto y considerando los siguientes parámetros y criterios:

- La gravedad y la naturaleza de las infracciones y los derechos personales afectados
- La buena fe del infractor
- La ventaja obtenida o pretendida por el infractor
- La situación económica del delincuente
- Reincidencia
- El grado de daño
- La cooperación del delincuente
- La adopción reiterada y comprobada de mecanismos y procedimientos internos capaces de minimizar el daño, orientados al tratamiento seguro y adecuado de los datos, de acuerdo con lo establecido en el sub II del Párrafo 2 del Artículo 48 de esta Ley
- La adopción de una política de buenas prácticas y gobernanza
- La rápida adopción de medidas correctoras
- Proporcionalidad entre la gravedad de la infracción y la intensidad de la sanción

Supervisión por Parte de otros Organismos

Otros organismos ya han actuado como inspectores y han aplicado sanciones:

- PROCON y ANATEL habilitan la oposición en cuanto a la recepción de llamadas de telemarketing - https://www.naomeperturbe.com.br/
- El Ministerio Público ha multado si este procedimiento no es respetado por los Encargadoes - https://www.mpmg.mp.br/comunicacao/noticias/vivo-devera-pagar-multa-de-r-10-4-milhoes-por-desrespeito-ao-sistema-de-bloqueio-de-telemarketing-do-mpmg.htm
- Demanda presentada por los Defensores Públicos de la Unión y de SP, IDEC, Artigo 19 e Intervozes, para la producción de pruebas por el Metro de SP en relación con la lectura facial de los pasajeros, el Poder Judicial requiere la presentación de RIPD. https://www.linkedin.com/pulse/relat%C3%B3rio-de-impacto-prote%C3%A7%C3%A3o-dados-pessoais-%C3%A9-ao-sp-correia-lima/

Destino de los Cobros

Art. 52. Inc. 5º. El producto de la recaudación de las multas impuestas por la ANPD, se registre o no como deuda cobrable, se destinará al Fondo de Defensa de los Derechos Difusos previsto en el art. 13 de la Ley nº 7347 de 24 de julio de 1985 y en la Ley nº 998 de 21 de marzo de 19.

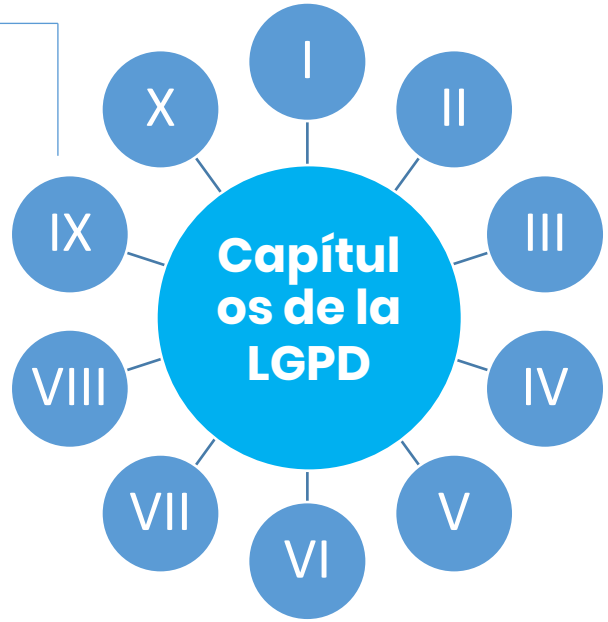
Módulo 11: Autoridad Nacional de Protección de Datos (ANPD)

LGPDF™ Versión 102021

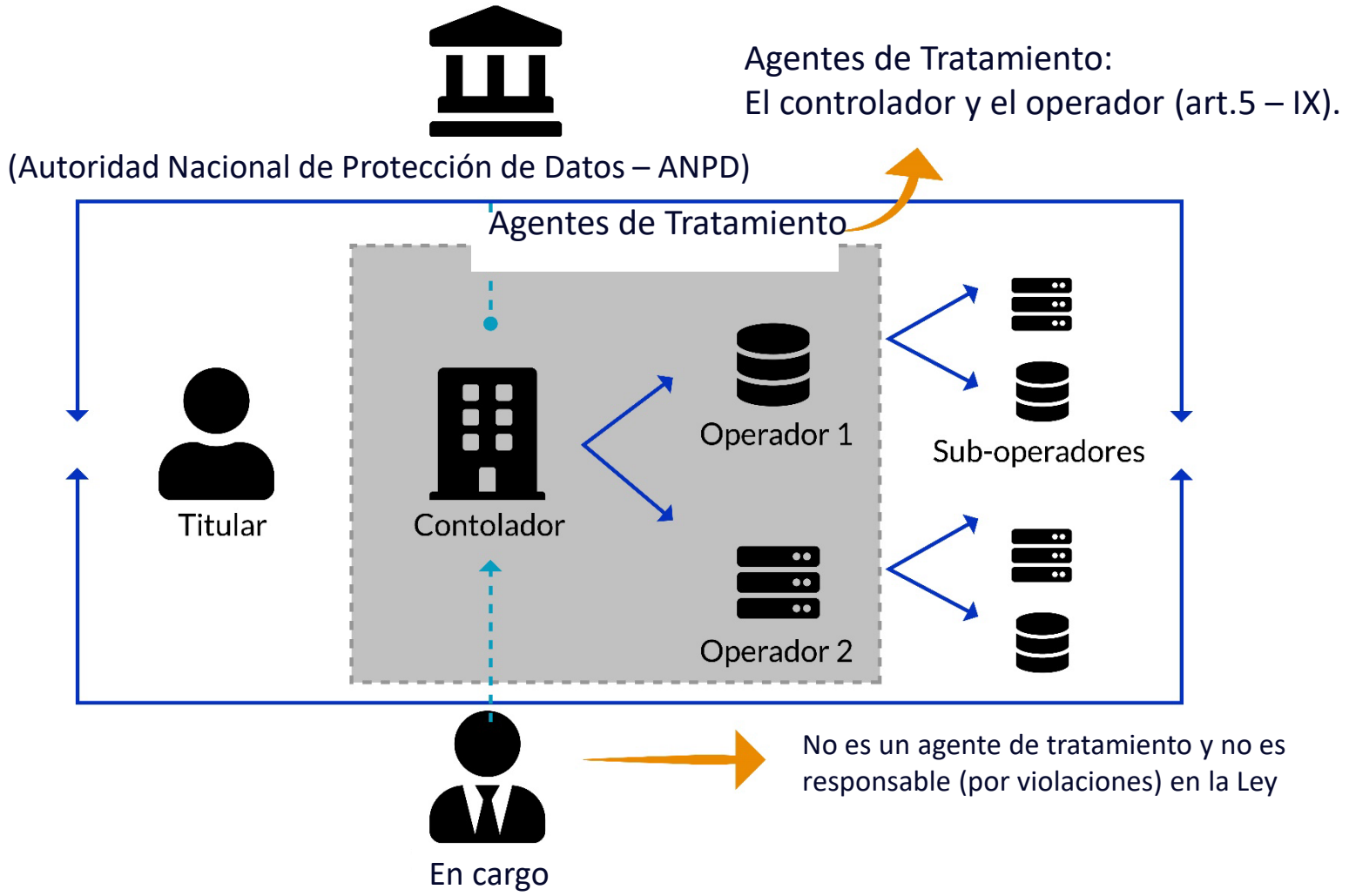
¿En qué parte de la ley estamos?

CAPÍTULO IX - LA AUTORIDAD NACIONAL DE PROTECCIÓN DE DATOS (ANPD) Y EL CONSEJO NACIONAL DE PROTECCIÓN DE DATOS PERSONALES Y PRIVACIDAD

- Artículos 55-A a 58-B
- Sección I - Autoridad Nacional de Protección de Datos (ANPD) - Artículos 55-A a 55-L
- Sección II - Del Consejo Nacional de Protección de Datos Personales y Privacidad - Artículos 58-A a 58-B



Autoridad Nacional de Protección de Datos - ANPD



Creación de la ANPD

Autoridad Nacional de Protección de Datos (ANPD) - Art. 55-A.

Órgano de la Administración Pública Federal, dependiente de la Presidencia de la República.

Inc. 1º. La naturaleza jurídica de la ANPD es transitoria y puede ser transformada por el Poder Ejecutivo en una entidad de la administración pública federal indirecta, sujeta a un régimen autárquico especial y vinculada a la Presidencia de la República
Inc. 2º. La evaluación de la transformación en virtud del apartado 1 de este artículo se realizará en un plazo de 2 (dos) años a partir de la fecha de entrada en vigor de la estructura reglamentaria de la ANPD
Inc. 3º. La provisión de cargos y funciones necesarias para la creación y funcionamiento de la ANPD estará condicionada a la autorización física y financiera expresa en la ley presupuestaria anual y a la autorización en la ley de directrices presupuestarias

Art. 55-B. La ANPD tendrá garantizada su autonomía técnica y de decisión.

Composición de la ANPD

La ANPD está compuesta por:

- Consejo de Administración, máximo órgano de gobierno (director presidente y otros 5 directores)
- Consejo Nacional de Protección de Datos Personales y Privacidad (23 miembros, que no serán remunerados por sus actividades, siendo representantes: de la sociedad civil, de entidades representativas, del Senado Federal, de la Cámara de Diputados y otros)
- Oficina del Inspector General; Oficina del Defensor del Pueblo; órgano asesor jurídico propio; y unidades administrativas y especializadas necesarias para la aplicación de las disposiciones de esta Ley

(Art. 55-C)

Problemática

Al no tener una LGPD vigente ni una ANPD estructurada, Brasil está clasificado como un destino inadecuado en materia de protección de datos personales.

https://www.cnil.fr/en/data-protection-around-the-world

Atribuciones de la ANPD

Atribuciones

- Poderes de investigación. Por ejemplo, para realizar auditorías de protección de datos, para notificar al responsable del tratamiento o al Encargado una presunta infracción
- Poderes correctivos. Por ejemplo, cuando se trata de amonestar, ordenar la comunicación de una violación de datos personales a un interesado, cancelar una certificación o imponer sanciones.
- Poderes consultivos. Ej: adoptar cláusulas contractuales tipo, emitir certificaciones, acreditar organismos certificadores

-> Art. 55-B. Se garantiza la autonomía técnica y de decisión de la ANPD.

Competencias de la ANPD

El responsable es la ANPD (Art. 55-J):

1. Para garantizar la protección de los datos personales, en los términos de la legislación
2. Velar por la observancia de los secretos comerciales e industriales, observando la protección de los datos personales y el secreto de la información cuando estén protegidos por la ley o cuando la violación del secreto viole los fundamentos del Art. 2 de esta Ley
3. Elaborar las directrices de la Política Nacional de Protección de Datos Personales y Privacidad
4. Supervisar y aplicar sanciones en caso de que el tratamiento de datos se lleve a cabo infringiendo la ley, mediante un proceso administrativo que garantice el derecho a la defensa contradictoria y amplia, y el derecho a recurrir
5. Examinar las peticiones del propietario contra el interventor después de que el propietario haya demostrado que la reclamación al interventor no se ha resuelto en el plazo establecido en la normativa

Competencias de la ANPD

El responsable es la ANPD (Art. 55-J):
6. Promover el conocimiento por parte de la población de la normativa y las políticas públicas sobre protección de datos personales y medidas de seguridad
7. Promover y elaborar estudios sobre las prácticas nacionales e internacionales de protección de datos personales y de la privacidad
8. Promover la adopción de normas para los servicios y productos que faciliten el ejercicio del control por parte de los titulares de los datos personales, que deben tener en cuenta la naturaleza específica de las actividades y el tamaño de los responsables
9. Promover acciones de cooperación con las autoridades de protección de datos personales de otros países, de carácter internacional o transnacional
- .....

Cooperación de la ANPD con otros Organismos

3. La ANPD y los organismos y entidades públicas responsables de la regulación de sectores específicos de la actividad económica y gubernamental coordinarán sus actividades, en los correspondientes ámbitos de actuación, con el fin de asegurar el cumplimiento de sus funciones con la mayor eficacia y promover el buen funcionamiento de los sectores regulados, de acuerdo con la legislación específica, y el tratamiento de los datos personales, según lo previsto en esta Ley.

4. La ANPD mantendrá un foro permanente de comunicación, incluso a través de la cooperación técnica, con los organismos y entidades de la administración pública responsables de la regulación de sectores específicos de la actividad económica y gubernamental, con el fin de facilitar los poderes de regulación, supervisión y sanción de la ANPD.

Relación ANPD

Audiencia pública en el STF ref. ADC 51, que debatió, en enero/2020, sobre el acuerdo internacional entre Brasil y los EE.UU. sobre el suministro de pruebas y datos por parte de las empresas de los EE.UU. para las investigaciones penales en Brasil.

Acuerdo de asistencia judicial en materia penal (MLAT) entre BR y EE.UU:

- http://www.planalto.gov.br/ccivil_03/decreto/2001/D3810.htm#:~:text=Promulga%20o%20Acordo%20de%20Assist%C3%AAncia,15%20de%20fevereiro%20de%202001.
- http://www.stf.jus.br/portal/cms/verNoticiaDetalhe.asp?idConteudo=436573

Consejo Nacional de Protección de Datos (CNPD)

El 09 de agosto de 2021 el Presidente de la República, Jair Bolsonaro, nombró a los miembros de la CNPD.

Art. 58-B. El Consejo Nacional de Protección de Datos Personales y Privacidad será responsable de: (Incluido por la Ley Nº 13.853 de 2019)

I. Proponer lineamientos estratégicos y otorgar subsidios para la elaboración de la Política Nacional de Protección de Datos Personales y Privacidad y para las acciones de la ANPD (Incluido por la Ley Nº 13.853, 2019)
II. Elaborar informes anuales de evaluación de la ejecución de las acciones de la Política Nacional de Protección de Datos Personales y Privacidad (Incluida por la Ley Nº 13.853, 2019)
III. Sugerir acciones a realizar por la ANPD (Incluido por la Ley Nº 13.853, 2019)
IV. Elaborar estudios y realizar debates y audiencias públicas sobre la protección de los datos personales y la privacidad; y (Incluido por la Ley Nº 13.853, 2019)
V. Difundir el conocimiento sobre la protección de los datos personales y la privacidad a la población (Incluido por la Ley Nº 13.853 de 2019)

Supervisión por parte de otros Organismos

Otros organismos ya han actuado como inspectores y han aplicado sanciones:

- PROCON y ANATEL habilitan la oposición en cuanto a la recepción de llamadas de telemarketing - https://www.naomeperturbe.com.br/
- El Ministerio Público ha multado si este procedimiento no es respetado por los Encargadoes - https://www.mpmg.mp.br/comunicacao/noticias/vivo-devera-pagar-multa-de-r-10-4-milhoes-por-desrespeito-ao-sistema-de-bloqueio-de-telemarketing-do-mpmg.htm
- Demanda presentada por los Defensores Públicos de la Unión y de SP, IDEC, Artigo 19 e Intervozes, para la producción de pruebas por el Metro de SP en relación con la lectura facial de los pasajeros, el Poder Judicial requiere la presentación de RIPD. https://www.linkedin.com/pulse/relat%C3%B3rio-de-impacto-prote%C3%A7%C3%A3o-dados-pessoais-%C3%A9-ao-sp-correia-lima/

Destino de los Cobros

Art. 52. Inc. 5 El producto de la recaudación de las multas impuestas por la ANPD, se registre o no como deuda cobrable, se destinará al Fondo de Defensa de los Derechos Difusos previsto en el art. 13 de la Ley nº 7347 de 24 de julio de 1985 y en la Ley nº 998 de 21 de marzo de 19.

Referencias

Bibliografía

- LGPD (2018) – Lei 13.709/2018 - Geral de Proteção de Dados Pessoais. Presidência da República do Brasil. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm
- ANPD (2020) – Decreto 10.474.2020 – Estrutura Regimental da Autoridade Nacional de Proteção de Dados. Presidência da República do Brasil. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm
- SGD/ME (2020) –Publicação 16/06/2021 - Guia de Boas Práticas da Lei Geral de Proteção de Dados. Secretaria de Governo Digital do Ministério da Economia do Brasil. Disponível em: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guia-boas-praticas-lgpd
- Encarregados | DPO (2021) – Livro: Encarregados | Data Protection Officer. Davis Alves & Adrianne Lima. Editora Haikai. Disponível em: https://www.amazon.com.br/Encarregados-MS-c-Davis-Alves-Adrianne/dp/6586334888/ref=sr_1_8?__mk_pt_BR=%C3%85M%C3%85%C5%BD%C3%95%C3%91&dchild=1&keywords=DPO&qid=1627076210&s=books&sr=1-8&ufe=app_do%3Aamzn1.fos.fcd6d665-32ba-4479-9f21-b774e276a678
- Proteção de Dados Pessoais (2020) – Livro: Proteção de Dados Pessoais: Comentários à Lei n. 13.709/2018 -LGPD. Patricia Peck Pinheiro. Editora Saraiva. Disponível em: https://www.amazon.com.br/Prote%C3%A7%C3%A3o-Dados-Pessoais-Coment%C3%A1rios-13-709/dp/8553617483/ref=sr_1_3?__mk_pt_BR=%C3%85M%C3%85%C5%BD%C3%95%C3%91&dchild=1&keywords=dpo+PECK&qid=1627076355&s=books&sr=1-3-catcorr

Referencias

Referencias técnicas y académicas

- ABNT NBR ISO-27001 (2013) – Norma técnica – Sistema de Gestão de Segurança da Informação - Requisitos. Associação Brasileira de Normas Técnicas (ABNT). Disponível em: https://www.abntcatalogo.com.br/norma.aspx?ID=306580
- ABNT NBR ISO-27002 (2013) – Norma técnica – Sistema de Gestão de Segurança da Informação – Código de Práticas. Associação Brasileira de Normas Técnicas (ABNT). Disponível em: https://www.abntcatalogo.com.br/norma.aspx?ID=306582
- ABNT NBR ISO-27701 (2020) – Norma técnica – Sistema de Gestão da Privacidade da Informação. Associação Brasileira de Normas Técnicas (ABNT). Disponível em: https://www.abntcatalogo.com.br/norma.aspx?ID=437612
- ABNT NBR ISO-27701 (2020) – Norma técnica – Sistema de Gestão da Privacidade da Informação. Associação Brasileira de Normas Técnicas (ABNT). Disponível em: https://www.abntcatalogo.com.br/norma.aspx?ID=437612

COMPARTE Y VERIFICA TUS LOGROS DE APRENDIZAJE FÁCILMENTE

#LGPDF #certiprof

certiprof®

¡Síguenos, ponte en contacto!

www.certiprof.com