Vol. Nº 5
Diciembre/2020
www.csirt.gob.cl

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

CIBER SUCESOS

Investigación, Tendencia y Concientización

NAVIDAD CIBERSEGURA

Consejos para compras online seguras

Videojuegos

Todo lo que tienes que saber para regalar seguridad

Cooperación Internacional

Uruguay: La evolución del principio de seguridad de los datos

Tendencias

Descubrimiento Pasivo: los riesgos de la exposición de datos.

Comunidad Hackers

Fundación Datos Protegidos.

Legal

Los Derechos Sobre Nuestros Datos.

CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

145 8712 7864
096 4321 5541

CSIRT es el Equipo de Respuesta ante Incidentes de Seguridad Informática del Gobierno de Chile. Su misión es reducir los riesgos de la ciberseguridad en las redes del Gobierno de Chile, asesorando a las diferentes organizaciones que lo componen, actuando como socio estratégico en la defensa de las amenazas y colaborando para brindar mayor seguridad y robustez a las infraestructuras del Estado.

Cómo lo **hacemos?**

Contamos con un equipo multidisciplinario de profesionales y las tecnologías para proveer de asistencia técnica y logística a nuestros beneficiarios, así como prevenir la explotación de vulnerabilidades y actuar oportunamente frente a amenazas y ciberataques.

- MONITOREO DE LAS PLATAFORMAS DE INTERNET DE ORGANISMOS PÚBLICOS Y PRIVADOS **24/7**
- INVESTIGACIÓN Y CAPACITACIÓN PARA ENFRENTAR LAS AMENAZAS DEL FUTURO
- DETECCIÓN DE VULNERABILIDADES DE SITIOS Y SISTEMAS WEB DEL ESTADO
- GESTIÓN DE INCIDENTES Y DIFUSIÓN DE MEDIDAS PREVENTIVAS
- INCORPORACIÓN DE NUEVAS TECNOLOGÍAS Y HERRAMIENTAS DE SEGURIDAD INFORMÁTICA
- MEJORA CONTINUA DE LOS ESTÁNDARES DE CIBERSEGURIDAD DEL PAÍS

Alianza del Pacífico · FIRST · CSIRTamericas.org · MERIDIAN Connecting and Protecting

INDICE

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

CIBER SUCESOS

Investigación, Tendencia y Concientización

cibersucesos@interior.gob.cl

Director: Carlos Landeros Cartes
Jefa de contenidos y edición:
Katherina Canales Madrid

Colaboradores equipo CSIRT:
Carolina Covarrubias
Cristobal Hammersley
Ramón Rivera

Diseño y diagramación: Jaime Millán

EDITORIAL

Carlos Landeros Cartes
Director Nacional
CSIRT de Gobierno

Si bien cada año parece más difícil abstraerse de la vorágine de las compras navideñas, este año sería irresponsable para nosotros como CSIRT siquiera intentar hacerlo. Porque ante la crisis sanitaria, y para mantener el necesario distanciamiento social, esta Navidad habrá una explosión de compras digitales, campo fértil para estafas y fraudes por parte de agentes maliciosos.

Por eso, como pieza central en esta edición recordamos los pasos clave para unas fiestas de fin de año sin exponernos de más a fraudes y ataques cibernéticos. Es clave recordar cuando hagamos clic en un enlace o alguna transacción, asegurarnos de realizarlo solo en sitios oficiales y con empresas de confianza, para reducir el riesgo de estafas.

En la misma línea y por ser los regalos más populares para Navidad, repasamos los principales conceptos para entender el mundo de los videojuegos en línea, junto con los riesgos que corren los niños que los usan y cómo prevenirlos, por ejemplo, a través de herramientas de control parental.

Más allá de las fiestas, en la sección Tendencias de este mes se explica el denominado descubrimiento pasivo, una técnica con la que agentes maliciosos hacen más efectivos sus ataques gracias a la revisión de las redes sociales de sus víctimas y otra información disponible en internet.

Comunidad Hacker trae el testimonio de Datos Protegidos, fundación dedicada a la defensa de la privacidad de la información personal en Chile. Matus nos cuenta sobre sus más recientes proyectos, como la investigación de la moderación de contenidos en internet en Chile, y la campaña “No doy mi RUT”.

Sigue en igual tono el apartado Legal, que describe los denominados derechos ARCO, de acceso, rectificación, cancelación y oposición, consignados en el artículo 19° de nuestra Constitución. También se explican dos nuevos derechos nacidos en Europa, denominados derecho al olvido y de portabilidad.

Con el mismo foco en la privacidad llega el aporte de Uruguay. Gonzalo Sosa, coordinador de URCDP e Ignacio Lagomarsino, gerente del CERTuy nos detallan la evolución de la protección de datos personales en ese país en términos legales y administrativos, lo que podría ser en un modelo a seguir para Chile.

En definitiva, nuestros mejores deseos de parte de todo el CSIRT de Gobierno, que tengan una hermosa Navidad y un feliz año nuevo, aunque deba ser a la distancia de nuestros seres queridos, y, sin nunca olvidar los consejos que les presentamos en este trabajo, #PorUnaNavidadCibersegura.

NAVIDAD
CIBERSEGURA

Consejos para compras online seguras

Realizar las compras online siempre ha sido una buena alternativa para evitar largas filas en los centros comerciales, y este año con la pandemia sigue siendo una opción, pero esta vez, para disminuir los riesgos de contagio. Sin embargo, en internet también hay algunos peligros como phishing, malware, fraudes, entre otros. ¿Cómo comprar ciberseguros esta Navidad?

CIBERDATO

El Departamento de Estudios de la Cámara Nacional de Comercio, realizó una encuesta a 185 locales para conocer cómo se estaba preparando el retail para esta Navidad. Un **63%** de los encuestados contará con ventas online y un **52,6%** mencionó que probablemente realizará promociones en su canal digital..

El comercio electrónico durante los últimos años ha sido un importante canal para realizar las compras de forma más cómoda, y ahora en época navideña y con la crisis sanitaria, es una buena alternativa para evitar aglomeraciones y disminuir el riesgo de contagio.

Si bien, la tendencia en Navidad de comprar a través de los canales digitales es cada vez más común, este año, reviste una situación particular, ya que hemos visto cómo se ha producido un proceso de digitalización importante en el comercio minorista, ello en gran parte para poder seguir ofreciendo productos y servicios a sus clientes.

Aunque parezca que es un fenómeno reciente adoptado en nuestro país, y que se ha visto precipitado debido a la situación actual, el comercio electrónico en estas fechas supone cada año una cifra importante de la facturación anual de las empresas, haciendo que estas últimas semanas del año sean las de mayor facturación del sector

#YoComproSeguroOnline

Aunque los sistemas para proteger nuestros datos cada vez son más seguros, los ciberdelincuentes siguen desarrollando formas de evadirlos.

¿Es esta tienda online fraudulenta? ¿Debería confiar en esta oferta? Son preguntas que muchos nos hemos hecho a la hora de comprar algo en Internet.

Por ello, es importante saber que no todas las páginas son seguras ni todas las ofertas son reales. No obstante, este motivo no debe impedirnos comprar online sino que servirnos de advertencia para no comprar en cualquier sitio web o anuncio que veamos en Internet sin antes asegurarnos de que no es una tienda fraudulenta.

¿Cómo comprar **seguro**?

1. **Evita WiFi Público**
No uses el Wifi público para compras, transacciones bancarias o trámites que involucren la entrega de información privada, podrías ser víctima de una estafa.

2. **Verifica el HTTPS**
Al buscar sitios para comprar, asegúrate que inicien con "HTTPS". Algunos incluso llevan un candado de color verde. Son más confiables.

3. **Usa canales formales**
Si vas a comprar en línea asegúrate de utilizar canales de pago formales o hazlo directamente desde el sitio oficial de la tienda.

4. **No compartas información**
No compartas la información de tus tarjetas de créditos, claves dinámicas o cuentas bancarias. Son datos personales y secretos.

5. **Desconfía de ofertas y concursos**
No te dejes engañar por ofertas demasiado buenas para ser verdad. Cuidado con mensajes, correos y ventanas emergentes tentadoras, podrían guiarte a sitios maliciosos.

6. **Actualiza antivirus**
Si realizas compras desde un equipo desprotegido, tu información está en riesgo. Asegúrate de que las actualizaciones, el antivirus y sistema operativo, estén al día.

7. **No guardes información**
No guardes datos bancarios en la web cuando compres en línea, porque si sufres un robo o pérdida de tu dispositivo, estarás más desprotegido.

8. **Actualiza Aplicaciones**
Antes de comprar, actualiza las aplicaciones y la seguridad de tus dispositivos. Un equipo seguro te da mayor tranquilidad para adquirir productos y servicios desde internet.

9. **No abras links dudosos**
No hagas clic en los enlaces que llegan por correos o en una publicación. Esos links te pueden redirigir a sitios de phishing y podrías ser víctima de un fraude.

10. **Usa distintas claves**
Configura distintas claves para tus cuentas. Si te roban una de tus contraseñas, los cibercriminales no podrán tener acceso a las restantes.

11. **Revisa otras opiniones**
Antes de introducir la información de tu tarjeta de crédito, comprueba las opiniones de otros usuarios sobre los sitios de compra online para decidir si son seguros.

12. **Compara precios**
No compres de manera apresurada. Cotiza en distintos sitios los productos que necesitas. Verifica los precios para hacer más expedita la compra. Has que la experiencia de compra en línea sea cibersegura.

13. **Verifica tus transacciones**
Después de comprar en línea, revisa que el estado de tu cuenta refleje la transacción exacta que hiciste. Mientras más rápido detectes un error, más rápido podrá resolver el problema.

14. **Revisa la reputación de la tienda**
Si el sitio de compras tiene un perfil en redes sociales, revisa su reputación y comentarios de los usuarios. El número de seguidores y la actualización de contenidos son buenas referencias.

Ciberdelitos identificados **en el mundo**

Las estafas cibernéticas ocurren en todas partes del mundo y la principal técnica utilizada son las campañas de phishing, a través del correo electrónico.

¿Cuáles son los móviles que aprovechan **los ciberdelincuentes en navidad**?

Promociones: Nos llegan correos electrónicos, donde se ofrecen productos de buena calidad y a precios muy rebajados y adicionan un enlace que nos puede dirigir a un sitio fraudulento para robar las credenciales.

Facturas y entrega de paquetes falsos: Aprovechando la oportunidad de la entrega de regalos de Navidad por reconocidas empresas de mensajería, los ciberdelincuentes se aprovechan de esto para enviar campañas de phishing con supuestas facturas o inconvenientes en la entrega, para lo cual se necesita confirmar los datos personales. Sin embargo, los archivos adjuntos pueden contener un malware y así infectar los computadores o dispositivo móvil.

Por eso, sigue nuestras recomendaciones **#PorUnaNavidadCibersegura.**

GAMER
GAMER
GAMER

VIDEO JUEGOS

Todo lo que tienes que saber para regalar seguridad en esta navidad

Los juegos en línea son un atractivo para los niños de todas las edades. Las ventas de videojuegos crecen cada año en Chile y en el mundo, y la Navidad es una fecha donde probablemente está en la lista de pedidos de más de un niño. Y si bien es una instancia muy entretenida, es importante que los padres tengan también en cuenta que los juegos tienen calificaciones por edad.

Imágenes más reales, la posibilidad de jugar y conversar con personas de todo el mundo y en cualquier lugar, son sólo algunos de los atributos que hoy tienen los juegos en línea y que se popularizan cada año entre los niños, jóvenes e incluso adultos de nuestro país. Más aún, con la crisis sanitaria los usuarios de los videojuegos han aumentado, es así como hoy cerca de 2.700 millones de personas en el mundo se consideran gamer.

En vista de lo anterior, es importante que aquellos padres que quieran regalarle a sus hijos un videojuego para esta Navidad se informen sobre las tendencias, qué tipos de juegos existen, riesgos y cómo prevenir.

JUEGOS **POPULARES**

En el mundo de los videojuegos existe una gran cantidad de alternativas, pero es importante considerar que no todos están desarrollados para que los jueguen niños pequeños.
A continuación, entregamos un listado de los títulos más conocidos entre los jóvenes, pero que se recomiendan usar solo a partir de los 10 años, ya sea por contenido violento o acceso a chats donde pueden interactuar con otros jugadores:

- Minecraft
- Roblox
- Fortnite
- Valorant
- League of Legends
- Animal crossing
- Call of Duty Warzone
- Garena Free Fire
- Among Us
- Fall Guys: Ultimate Knockout

PLATAFORMAS **DE JUEGO**

En la actualidad, no sólo es posible realizar este tipo de actividad mediante una consola de juegos, sino que hay varias otras alternativas:

Juegos integrados en otros servicios, como por ejemplo en redes sociales. Son aplicaciones de terceros que ofrecen sus servicios dentro del de otra compañía, y suelen estar sincronizados con aplicaciones.

Dispositivos móviles. Hoy, es posible jugar tanto en una Tablet como en un Smartphone en reemplazo de las consolas. Por lo general, son juegos más simples.

Juegos para computadores o consolas. Para este tipo de plataforma hay más posibilidades de juegos, siendo más completos, complejos y diversos.

Plataformas de distribución de juegos. Algunas de las alternativas, tanto pagadas como gratuitas sonSteam, Origin, Uplay y Google Play, las cuales están disponibles para computadores, consolas o dispositivos móviles.

RIESGOS

A pesar de que los videojuegos pueden ser una instancia muy entretenida para los menores, también existen ciertos peligros que se deben tener en consideración:

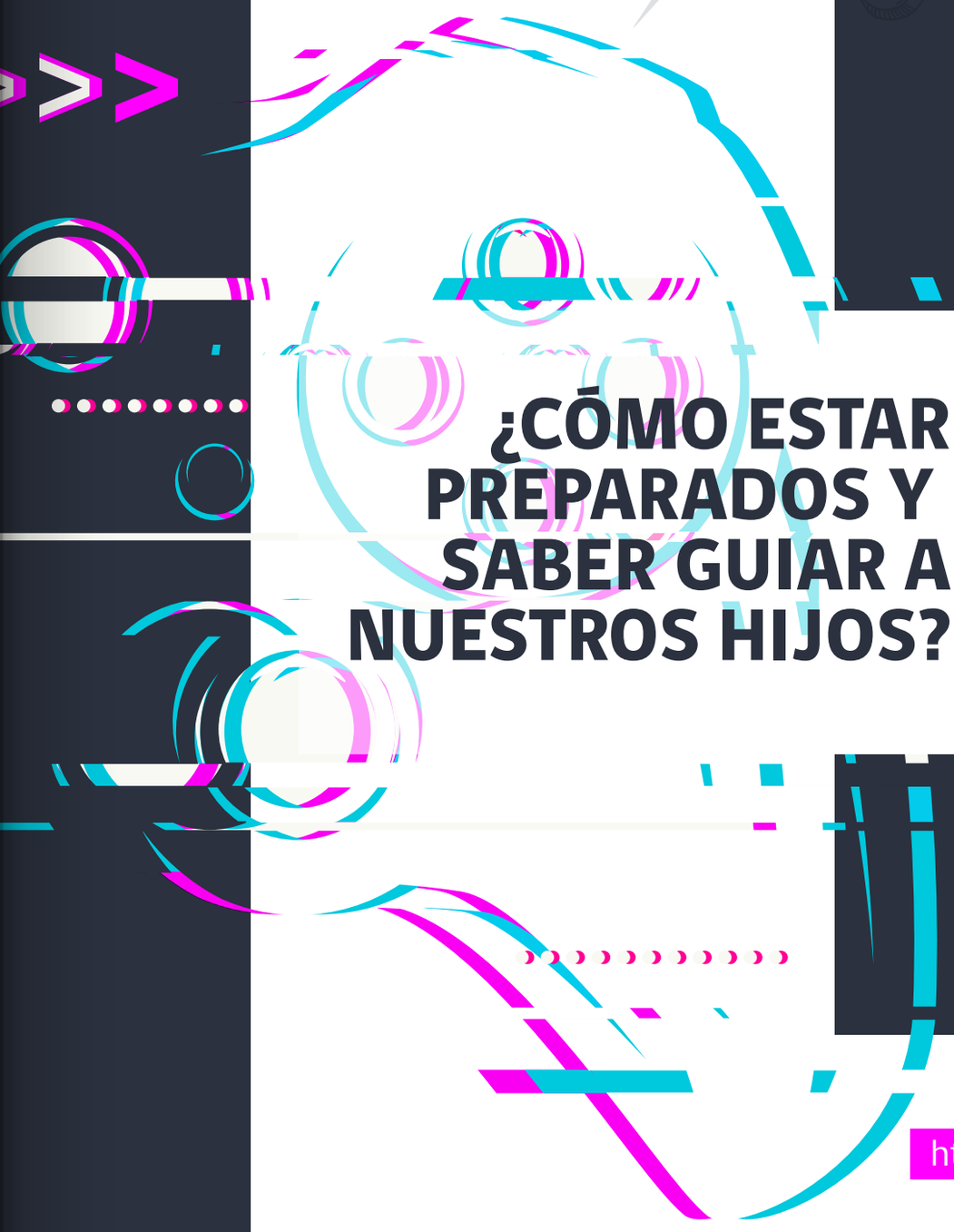
ACOSO EN LÍNEA O CIBERBULLYING:A través de mensajes ofensivos por el chat del juego u hostigamiento constante del jugador.

CONTENIDO INAPROPIADO: En ocasiones, comunidades peligriosas se comparte contenido violento, sentimientos de odio o potencian la autolesión o el suicidio.

GROOMING: Es un delito y consiste en que un adulto se hace pasar por un menor para engañar a jóvenes o niños y ganar su confianza, crear lazos emocionales y poder abusar de ellos sexualmente u obtener contenido pornográfico.

PRIVACIDAD: La privacidad de los datos del jugador puede verse afectada de diversas maneras, por ejemplo mediante los permisos que otorgan las aplicaciones (acceso a fotografías, contactos y datos de navegación, entre otros) o los perfiles que se utilizan en redes sociales pueden ser compartidos con otros usuarios de la plataforma.

ARCHIVOS MALICIOSOS: Los videojuegos se pueden ver afectados por algún tipo de malware, ya sea descargando aplicaciones maliciosas, modificaciones (mods) desarrolladas por los usuarios o al adquirir copias pirateadas.



¿CÓMO ESTAR PREPARADOS Y SABER GUIAR A NUESTROS HIJOS?

- Acompañar a los niños, especialmente si son menores, y conocer sus gustos y preferencias.
- Establecer un horario y límite de tiempo de juego.
- Explicar a los hijos los riesgos de hablar con extraños y entregar información confidencial a otros jugadores.
- Nunca entregar datos personales como nombre, dirección, colegio, etc.
- Incentivar el respeto propio y el de los demás.
- Crear contraseñas robustas y seguras, y configurar la privacidad de los perfiles.
- Contar con doble factor de autentificación para mayor seguridad.
- Evitar que los hijos descarguen aplicaciones o programas piratas, sólo aceptar aquellos provenientes de sitios de confianza.
- Mantener actualizados los sistemas operativos.

Para saber más sobre mediación parental, puedes descargar la guía elaborada por el **CSIRT** en el siguiente enlace:

https://www.csirt.gob.cl/recomendaciones/ciberguia-de-mediacion-parental/

HERRAMIENTAS **DE CONTROL PARENTAL**

Una alternativa para saber a qué juegan los niños en internet y el tiempo al que están expuestos es mediante el uso de herramientas de control parental. Éstas permiten tener un registro de las actividades que realizan sus hijos en los dispositivos móviles o plataformas de streaming. Sirve de apoyo para los padres, pero no reemplaza el hecho de que los adultos deban acompañar a los menores. Existen varias aplicaciones, las que de acuerdo al plan que se contrate o la app que se descargue es posible:

- Filtrar contenido para limitar el acceso a contenido inapropiado.
- Limitar el horario y bloquea las aplicaciones o dispositivo una vez transcurrido el tiempo.
- Llevar un registro de las actividades en línea.

En su sitio web, Entel entrega un listado de este tipo de aplicaciones de control parental disponibles para descargar. Aquí Puedes encontrar el detalle:
https://informacioncorporativa.entel.cl/control-parental

LA EVOLUCIÓN DEL PRINCIPIO DE **SEGURIDAD DE LOS DATOS**

En la normativa uruguaya

Gonzalo Sosa, coordinador de la URCDP e Ignacio Lagomarsino, gerente del CERTuy

La Ley uruguaya en protección de datos personales y acción de habeas data Nº 18.331 de 2008 se estructura en base a un conjunto de derechos, obligaciones, y princi pios que regulan todas las operaciones de tratamiento realizadas por responsables y encargados. El fundamento de esta regulación está en el reconocimiento expreso (en su artículo 1º) del derecho a la protección de datos como un derecho fundamental, inherente a la personalidad humana.

La ley prevé además las acciones que pueden plantear los titulares de los datos ante el Poder Judicial, o en vía administrativa ante el órgano de control, la Unidad Regu ladora y de Control de Datos Personales (URCDP), única autoridad encargada de resolver controversias, imponer sanciones y asesorar en materia de protección de datos personales.

Por su parte, el conjunto de principios se establecen en los artículos 6º a 12º de la ley: principio de legalidad, de veracidad, de finalidad, de consentimiento informado, de seguridad de los datos, de reserva y de responsabilidad.

Es importante señalar que los principios deben ser vistos como un conjunto armónico, y por ello las operaciones de tratamiento requieren el cumplimiento de todos ellos.

No obstante, nos concentraremos en la regulación del principio de seguridad de los datos, y en las nuevas dispo siciones que significan una evolución en línea con las normas europeas en la materia.

En concreto, el artículo 10º de la Ley prevé el principio de seguridad de los datos, estableciendo la obligación de los responsables de tratamiento de adoptar medidas para garantizar la seguridad y confidencialidad de los datos personales, con objetivos expresamente previstos, además de formas de almacenamiento de la información que garanticen el ejercicio del derecho de acceso por parte del titular.

Es decir, la ley no sólo impone la adopción de determina das medidas sino que establece su objeto y condiciona la forma de almacenamiento de la información al correcto ejercicio del derecho de acceso por parte de los titulares (previsto en el artículo 14).

Uruguay Presidencia | agesic | CERTuy

Este artículo 10° no preveía la comunicación de vulneraciones de seguridad, limitándose a indicar la obligación, como dijimos, de establecer los medios para su prevención.

Pero en 2009 y por la vía reglamentaria, se estableció la obligación de comunicar la ocurrencia de vulneraciones de seguridad a las personas que hayan sido potencialmente afectadas de forma significativa en sus derechos. La comunicación debían hacerla no sólo los responsables sino también los encargados del tratamiento, se realizaría solo a los potenciales afectados, y dicha afectación quedaba en la práctica a la valoración interna de responsables o encargados.

La Ley N° 18.331 también prevé un análisis de riesgos de seguridad, y una especie de comunicación vinculada a esos riesgos, para el tratamiento de los datos de telecomunicaciones. El artículo 20° establece que los operadores de redes públicas o que presten servicios de comunicaciones electrónicas deben adoptar las medidas adecuadas para preservar la seguridad y garantizar determinados niveles de protección de los datos personales. Y en caso de riesgos de violación de la seguridad de la red pública de comunicaciones electrónicas, deberá informar a los abonados sobre ese riesgo y las medidas a adoptar.

Aquel régimen de medidas de seguridad y de comunicación de vulneraciones fue modificado por el artículo 38 de la Ley N° 19.670 de 2018, que impone a responsables y encargados la notificación de vulneraciones de seguridad en forma inmediata y pormenorizada a los titulares de los datos y al URCDP También prevé una actuación conjunta del URCDP con el Centro Nacional de Respuesta a Incidentes de Seguridad Informática (CERTuy).

Así, esta modificación se alinea con las tendencias internacionales en la materia, fundamentalmente reflejadas en el Reglamento General de Protección de Datos del Parlamento Europeo y el Consejo, y en los Estándares en Protección de Datos para los Estados Iberoamericanos der la Red Iberoamericana de Protección de Datos.

El artículo 38 precitado fue reglamentado por los artículos 3° y 4° del decreto N° 64/020, de 2020.

El artículo 3° reitera la obligación del responsable y del encargado del tratamiento de adoptar las medidas técnicas y organizativas necesarias para conservar la integridad, confidencialidad y disponibilidad de la información, de forma de garantizar la seguridad de los datos personales.

El decreto plantea la necesidad de que se consideren estándares nacionales e internacionales en materia de seguridad de la información, y menciona específicamente el Marco de Ciberseguridad elaborado por la Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento (Agesic).

El Marco de Ciberseguridad constituye un documento de referencia que provee un enfoque integral para reducir el riesgo vinculado a las amenazas cibernéticas que puedan comprometer la seguridad de la información de las organizaciones del país.
Asimismo, contiene buenas prácticas para organizaciones que requieran gestionar los riesgos a la seguridad de la Información y al uso de las infraestructuras tecnológicas que les dan soporte, así como adoptar en forma urgente políticas de gestión de incidentes, implementar centros de datos seguros y cumplir con la normativa vigente en la materia.

Por otra parte, en el decreto 3° se define que ante incidentes de seguridad se deberán iniciar los procedimientos previstos necesarios para minimizar su impacto dentro de las primeras 24 horas de constatados.

El artículo 4° del decreto establece un plazo de 72 horas de conocido el incidente para comunicarlo a la Unidad Reguladora y de Control de Datos Personales, conjuntamente con un informe que contenga al menos fecha cierta o estimada de la ocurrencia de la vulneración, su naturaleza, los datos personales afectados, y los posibles impactos generados.

Esta obligación de comunicación recae en el responsable del tratamiento, en tanto el encargado que haya tomado conocimiento cumple comunicándole en su caso a éste. No obstante, la URCDP ha aceptado comunicaciones realizadas directamente a ésta por parte de encargados.

También establece el decreto que aquellos titulares de los datos que hayan sufrido una afectación significativa en sus derechos deberán recibir la comunicación por parte del responsable en un lenguaje claro y sencillo.

Finalmente, el responsable se encuentra obligado a elaborar para la URCDP un informe pormenorizado de la vulneración, una vez solucionada ésta, incluyendo las medidas adoptadas.

Gracias a ello, la URCDP valorará con el CERTuy las medidas a adoptar, siendo este último el referente técnico que permitirá considerar su pertinencia, si se realizó una adecuada valoración por parte del responsable y si se requieren nuevas medidas.

El involucramiento del CERTuy a los efectos de dicha valoración resulta de particular interés para la protección de datos, debido a que el centro de respuesta es el órgano competente y el más experimentado en la contención de incidentes de ciberseguridad y mitigación de vulnerabilidades.

Creemos que en conjunto, las herramientas normativas previstas significan un importante avance en el cumplimiento del principio de seguridad de los datos, y permiten poner a nuestro país en línea con los nuevos desarrollos en la materia, dando mayores garantías a los titulares de los datos y permitiendo a los responsables y encargados del tratamiento obtener un análisis objetivo de las medidas adoptadas, que los ayude, en su caso, a realizar las adaptaciones necesarias para el cumpli miento de las normas vigentes.

DESCUBRIMIENTO **PASIVO**

Cada vez resulta más habitual compartir nuestro día a día mediante las redes sociales, y esto nos lleva a analizar la sobreexposición de datos en internet, que no es ilegal, pero puede tener graves consecuencias.

A este tipo de conductas se les denomina OVERSHARING (publicar en exceso detalles de nuestra vida privada) y SHARENTING, término que proviene de conjugar las palabras inglesas "share" (compartir) y "parenting" (crianza), que es la práctica realizada por muchos padres y familiares consistente en mostrar continuamente la vida de sus hijos menores de edad en las redes sociales.
El problema radica en que cuando publicamos información en internet, perdemos automáticamente el control sobre ella, quedando expuestos a desconocidos, lo cual supone un riesgo para nuestra seguridad. De tal manera que, con tanta información personal publicada en las redes sociales, le facilitamos el trabajo a quienes pretenden aprovecharse de ello mediante determinadas conductas que nos pueden ocasionar daños materiales, morales y físicos.

¿QUÉ ES EL **DESCUBRIMIENTO PASIVO**?

El descubrimiento pasivo consiste en la búsqueda de información pública existente en internet acerca de una persona u organización. Hoy en día es posible encontrar diversa información debido a la exposición que tenemos en internet y el uso masivo de redes sociales.

Prácticamente se podrían reconstruir las actividades de muchas personas a través de sus posteos en RR.SS., Sin darnos cuenta compartimos nuestros gustos, preferencias, nuestras amistades, familiares, a dónde solemos ir, dónde trabajamos, a qué hora, dónde vamos, nuestros nombres, o dónde vivimos, por tanto, hay que tomar conciencia que "no hay nada 100% privado en la web".

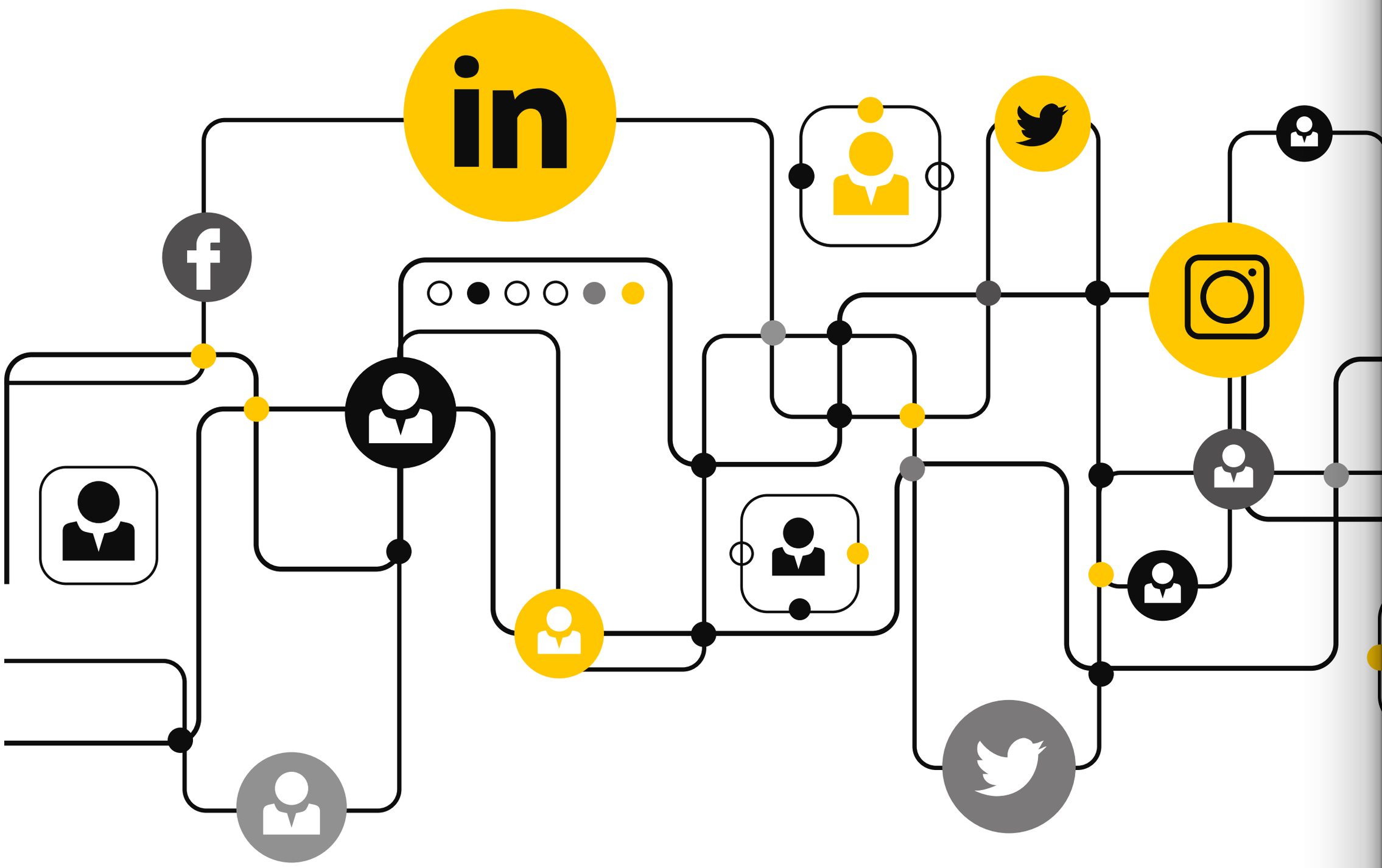
LOS **RIESGOS**

Cuanta más información se comparta en la red, más riesgo hay de robo o suplantación de identidad, ello en la medida de la exposición que hacemos de nuestra información, la configuración de privacidad dentro de nuestras redes sociales y la presencia que tenemos online.

Los riesgos asociados no se limitan solamente a la explotación de sistemas y accesos no autorizados, ya que, combinando técnicas de recolección de información de personas y enumeración de infraestructura, un ciberatacante podría generar un gran impacto tanto a la continuidad del negocio como a la privacidad de los usuarios.

Lo cierto es que las técnicas y herramientas para la recopilación y análisis de información son cada vez más populares y son un aspecto clave de la seguridad de la información.

OSINT significa Open Source Intelligence (Inteligencia de Fuentes Abiertas), y se trata de un conjunto de técnicas y herramientas para recopilar información pública, correlacionar los datos y procesarlos. Es decir, aplicarle análisis e inteligencia a la gran cantidad de información públicamente accesible en Internet con el objetivo de extraer conclusiones útiles para una investigación, un monitoreo o una campaña de marketing. Pero es necesario recordar que esa misma información puede ser mal usada por cibercriminales y con ella entregarle herramientas que le faciliten el ataque dirigido contra algún blanco elegido, explotar sistemas, cometer estafas, phishing o doxxing (divulgación de información privada hacia el público con la intención de intimidar o amenazar)



CIBERDATO

Google almacena información de **30 billones de páginas web**, lo que supone más de **1.000 terabytes** de información.

Facebook tiene **1.100 millones de usuarios**, **50 millones de páginas y 240.000 millones de fotos subidas** a su página.

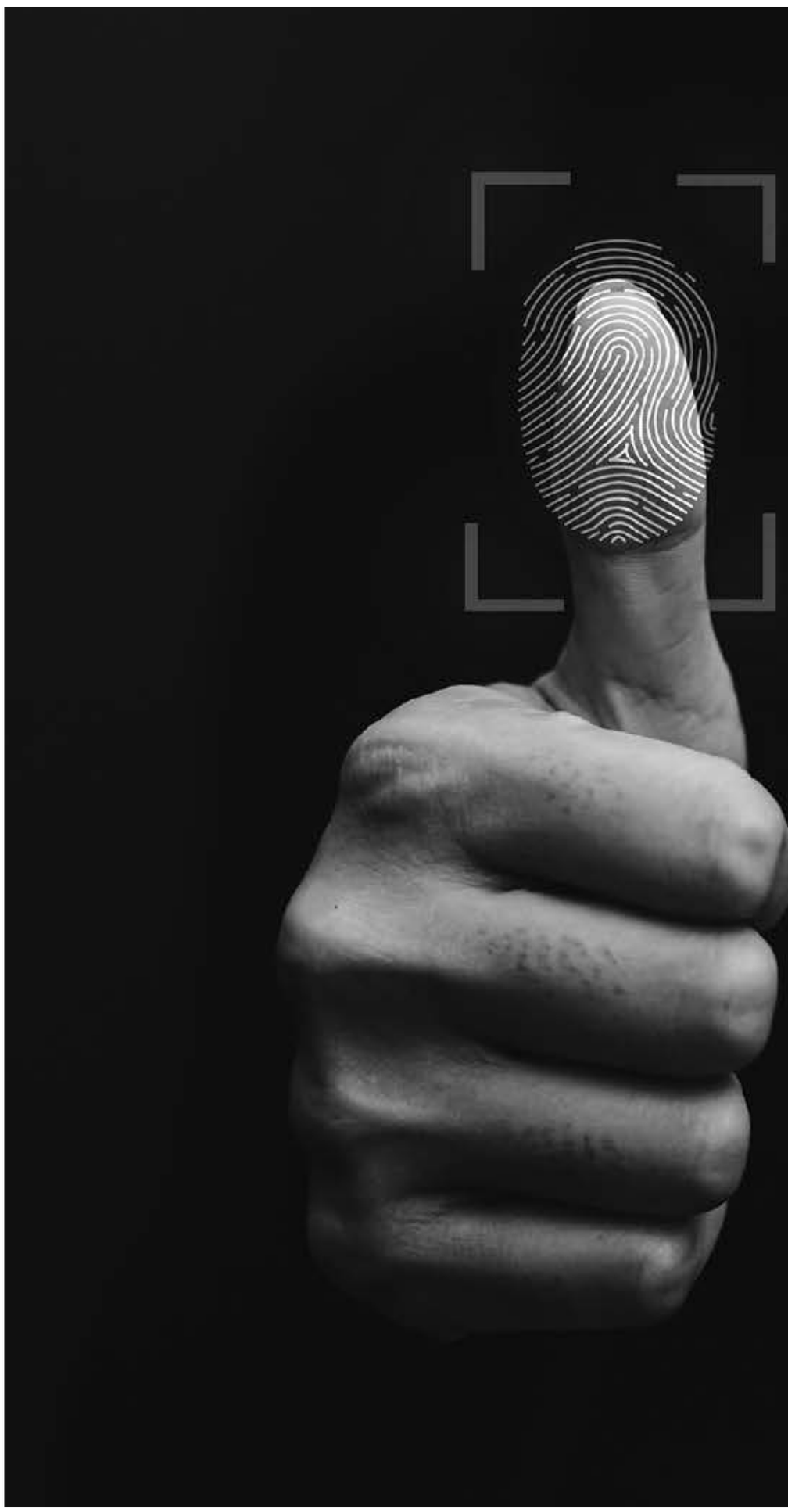
Twitter tiene más de **230 millones de usuarios activos** que escriben diariamente más de 500 millones de tweets.

Flickr tiene **84 millones de usuarios y más de 8.000 millones de fotos**.

Recomen**daciones**

Algunas medidas que pueden tomar tanto organizaciones como individuos para mejorar la privacidad del usuario son las siguientes:

- No utilizar mismos nombres de usuario en distintas plataformas.
- Implementar el uso de doble factor de autenticación (2FA) cuando el servicio/plataforma lo permita.
- Emplear contraseñas distintas y únicas para cada plataforma.
- No utilizar una dirección de correo corporativa para el registro en sitios de uso personal.
- No divulgar información o fotografías en redes sociales que puedan exponer información geográfica o personal.
- Evitar compartir públicamente y con terceros números telefónicos y/o correos electrónicos
- No exponer nombres completos en redes sociales ni en registro de aplicaciones de mensajería como WhatsApp.
- Configurar la privacidad en redes sociales de manera tal que un tercero no pueda acceder a la información o fotografías personales
- Evitar publicar correos electrónicos abiertamente
- Cambiar las credenciales de inicio de sesión predeterminadas para todos sus dispositivos conectados a Internet
- Desactivar el reenvío de puertos y la administración remota en sus enrutadores.
- Tanto organizaciones como usuarios deben validar que los dispositivos conectados a Internet han sido autorizados y que las configuraciones de seguridad han sido aplicadas correctamente.
- En el caso de una organización, establecer un monitoreo de inteligencia de amenazas continua, activa y predictiva, es un aspecto esencial para mitigar las amenazas y los riesgos asociados a la constante evolución de las mismas y los potenciales vectores de ataque.



FUNDACIÓN DATOS **PROTEGIDOS**

Fundación Datos Protegidos, preocupada por los derechos digitales de las personas.

A través de campañas e investigaciones esta organización sin fines de lucro busca velar por la protección de los datos personales en Chile, abordando distintas ámbitos: protección de datos y privacidad; ciberseguridad; libertad de expresión y temas vinculados a la tecnología y el género.

Datos Protegidos

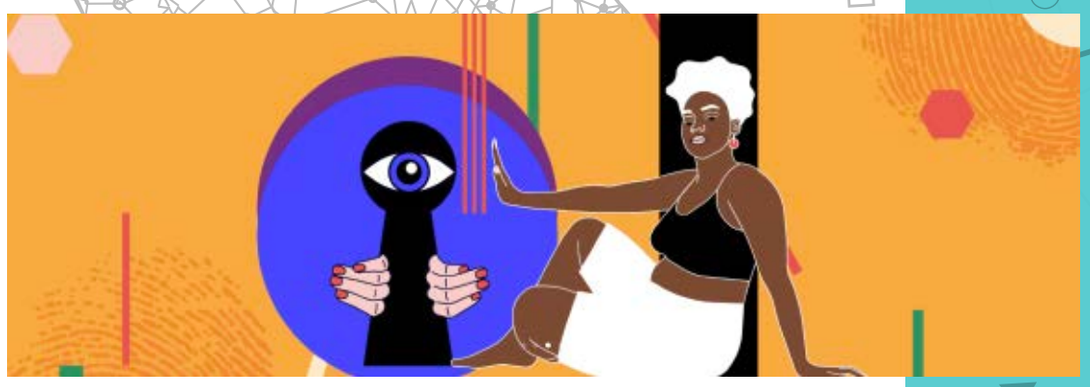
Ante la que considera la desactualizada legislación en materia de protección de datos con la que cuenta nuestro país, Jessica Matus, abogada de la Universidad de Chile, tuvo la inquietud de crear una organización que permitiera informar, asesorar legalmente y capacitar sobre este tema a la ciudadanía. Fue como el año 2015 nació la Fundación Datos Protegidos.

Con el correr de los años, la Fundación ha ido creciendo y consolidándose para velar por los derechos humanos en el mundo digital, conformando un equipo multidisciplinario que resuelva las distintas problemáticas que surgen en los entornos digitales. Es así, como los principales objetivos de la fundación son la defensa de los derechos humanos en materias digitales, abordando cuatro aristas:

- Protección de datos y privacidad, con litigiosestratégicos y difusión de material.
- Ciberseguridad desde el análisis de casos y el levantamiento de minutas para apoyar políticas públicas.
- Libertad de expresión, con el proyecto **"Testigo En Línea",** junto a casos de censura en internet.
- Tecnología y género, levantando talleres, capacitaciones y entregando asesorías a personas que vivan algún tipo de vulne ración o acoso en línea.

Estos cuatro ámbitos son abordados por la fundación a través de distintas instancias, realizando investigaciones, incidencia legislativa y capacitaciones, junto con difundir información educativa en redes sociales en torno a nuestras aristas de acción. Las actividades y estudios son presentadas en diversas instancias, incluso han realizado charlas para niños y adolescentes.

CAMPAÑAS Y **PROYECTOS**



Con el objetivo de educar a la ciudadanía, una de las últimas campañas desarrolladas por la fundación fue "No doy mi RUT", que busca crear conciencia sobre la importancia de este número de identificación de cada una de las personas y a tener claro a quiénes y en qué circunstancias debemos entregar realmente nuestro RUT. Así también, han realizado otras acciones como un informe sobre la violencia de género en Internet en Chile, siendo la primera publicación sobre este tema el año 2018.

Sumado a lo anterior, la abogada señala que en Datos Protegidos “estamos investigando la moderación de contenidos en las plataformas de internet en Chile, en conjunto con otras organizaciones de Latinoamérica. Otra iniciativa que está llevando a cabo esta fundación es una investigación colaborativa con la organización Infomigra en torno a las implicancias del proceso de modernización tecnológica del Departamento de Migración y Extranjería del Gobierno de Chile”.

Asimismo, sobre aspectos de género, están levantando el proyecto ‘Reconectadas’ junto con la Universidad Abierta de Recoleta, en el marco del fondo Juntas en Acción de Comunidad Mujer y Corporación Humanas, cofinanciado por la Unión Europea. En este proceso, se está construyendo un piloto de red comunitaria de Internet, colaborativo de principio a fin con la organización de mujeres de la población Ángela Davis de Recoleta.

Por otra parte, en octubre de este año se consolidó la creación del Capítulo Chileno de Internet Society, experiencia inédita en nuestro país que cuenta con un directorio conformado por Jessica Matus, Patricia Peña, Humberto Carrasco, Claudio Magliona, María Paz Canales, Margarita Valdés y Jocelyn Simmonds.

Equipo

El equipo directivo está compuesto por Jessica Matus, experta en privacidad y protección de datos personales, ciberseguridad y tecnologías de la información. Junto a ella están Danny Rayman, experto en materias de propiedad intelectual, protección de datos, derecho internacional y derechos humanos y Patricia Peña, experta en tecnologías, género e implicancias de violencia digital.

Además, gracias al crecimiento de la Fundación y su posicionamiento dentro de nuestro país, hoy la organización cuenta con un equipo de 12 personas, entre ellos informáticos, activistas, abogados y periodistas, todos vinculados a distintas áreas de las tecnologías y los derechos humanos.

Si quieres conocer más de Datos Protegidos y sus campañas, actividades, columnas opinión, puedes ingresar a su sitio web www.datosprotegidos.org

LOS DERECHOS **SOBRE NUESTROS DATOS**

Todos hemos leído y escuchado en estos días la preocupación en torno a los datos personales, principalmente debido a las medidas tecnológicas implementadas para el control de la actual crisis sanitaria y los distintos incidentes de ciberseguridad registrados. Se trata de un tema jurídico relevante que cobra importancia cada cierto tiempo, quedando al descubierto en épocas de crisis y que solo despiertan asombro e interés cuando se extreman ciertas discusiones públicas, tal como la producida por el Covid-19.

Es así que frente a estas nuevas herramientas de tra zabilidad han surgido preguntas tales como si son una forma de control de las personas y sus movimientos, que a su vez permiten prevenir riesgos a la salud pública, o más bien un control que afecta la autodeterminación del ser humano, impactando su libertad y derechos? ¿Cuál ha sido la decisión de cada país respecto de esta disyuntiva? ¿Es posible afirmar que aquellos países que han sacrificado sus controles en torno a la autonomía del movimiento de sus ciudadanos han sido más exitosos en el combate de la pandemia?

Pero la preocupación en cuanto al uso de nuestros datos personales debiera ser mucho mayor y más amplia que el para el caso recién expuesto, sobre todo en el contexto actual en que estamos conectados virtualmente a clases o teletrabajando, lo que lleva a estar más expuestos a visibilizar los nuestros datos personales y por lo mismo es esencial saber cuáles son nuestros derechos respecto de su tratamiento.

¿DÓNDE ESTÁN **REGULADOS**?

En nuestro país la protección de los datos de carácter personal se encuentra consagrada en la ley N° 19.628. El ámbito material de su aplicación es el tratamiento de datos de carácter personal en general, cualquiera sea la forma en que dicho tratamiento se lleve a cabo. En esta materia, la Ley 19.628 sigue la tendencia moderna a circunscribir en su ámbito de aplicación no solo el tratamiento de datos personales realizado de forma automatizada, sino también aquel realizado de forma manual. En cuanto al ámbito subjetivo de aplicación, esto es, los individuos respecto de quienes es aplicable la legislación y el cumplimiento de las obligaciones allí contenidas, la ley distingue entre quienes son los titulares de los datos y quienes hacen tratamiento de estos, respecto de los cuales se establecen distintos derechos y obligaciones.

En Chile, a partir de una reforma de julio de 2018, la protección de los datos personales es un derecho consagrado en el artículo 19° de la Constitución Política.

TUS DATOS, **TUS DERECHOS**

Los derechos a través de los cuales una persona puede ejercer el control sobre sus datos personales son los denominados derechos ARCO y están constituidos por los derechos de acceso, de rectificación, de cancelación y de oposición. Estos derechos están contemplados en los artículos 12°, 13°, 14° y 15° de la ley 19.628 como la expresión de la "autodeterminación informativa", entendiendo por tal el control que el sujeto puede ejercer respecto del conocimiento que de su persona tengan terceros.

CONCEPTOS **ESENCIALES**

1.-DATOS PERSONALES:

Son los relativos a cualquier información concerniente a personas naturales, identificadas o identificables.

2.-DATOS SENSIBLES:

Aquellos datos personales que se refieren a las características físicas o morales de las personas o a hechos o circunstancias de su vida privada o intimidad, tales como los hábitos personales, el origen racial, las ideologías y opiniones políticas, las creencias o convicciones religiosas, los estados de salud físicos o psíquicos y la vida sexual.

3.-REGISTRO O BANCO DE DATOS:

El conjunto organizado de datos de carácter personal, sea automatizado o no y cualquiera sea la forma o modalidad de su creación u organización, que permita relacionar los datos entre sí, así como realizar todo tipo de tratamiento de datos.

4.-RESPONSABLE DEL REGISTRO O BANCODE DATOS:

La persona natural o jurídica privada, o el respectivo organismo público, a quien compete las decisiones relacionadas con el tratamiento de los datos de carácter personal.

LOS DERECHOS **ARCO**

1. **DERECHO DE ACCESO:**
Es el que tiene todo titular de datos para exigir del responsable del banco de datos información que le permita saber si se tratan datos suyos, y de ser así, cerciorarse de su exactitud y de la licitud de su tratamiento.

2. **DERECHO DE RECTIFICACIÓN:**
Es el que tiene todo titular de datos para exigir la rectificación de aquellos que le conciernen cuando se trate de datos erróneos, inexactos, equívocos o incompletos.

3. **DERECHO DE CANCELACIÓN**:
Es el que tiene todo titular de datos para exigir la destrucción de datos almacenados, cualquiera fuere el procedimiento empleado para ello.
Respecto de este derecho en particular, la ley señala que sin perjuicio de las excepciones legales, toda per sona tiene derecho a exigir a quien sea responsable de un banco de datos, que se eliminen, en caso de que su almacenamiento carezca de fundamento legal o cuando estuvieren caducos, como también, cuando haya proporcionado voluntariamente sus datos perso nales o ellos se usen para comunicaciones comerciales y no desee continuar figurando en el registro respecti vo, sea de modo definitivo o temporal.

4. **DERECHO DE OPOSICIÓN:**
Es la facultad de todo titular de datos para exigir la suspensión temporal de cualquiera de las operaciones del tratamiento de datos, cuando la exactitud de los datos no pueda ser establecida o su vigencia sea dudosa y siempre que no proceda la cancelación.

Finalmente, es necesario precisar que a los derechos recién enunciados se han agregado dos nuevos como parte del Reglamento General de protección de Datos de la Unión Europea, los cuales no existen en Chile y son el "derecho de portabilidad" y el "derecho al olvido". El primero consiste en derecho del titular de datos a solicitar y obtener del responsable, una copia de sus datos personales en un formato electrónico estructurado, genérico y común, que permita ser operado por distintos sistemas, y poder comunicarlos o transferirlos a otro responsable de datos. El segundo, consiste en la supresión de los datos personales del interesado sin dilación siempre y cuando se cumplan determinados requisitos.

¿CÓMO EJERCER **LOS DERECHOS ARCO**?

Los derechos recién enunciados son exigibles a quien sea responsable de un banco de datos que se dedique en forma pública o privada al tratamiento de datos personales y para ello se debe dirigir una solicitud al mismo.

Para el caso de que el responsable del registro o banco de datos no se pronunciara sobre la solicitud del requirente dentro de dos días hábiles, o la denegara por una causa distinta de la seguridad de la Nación o el interés nacional, el titular de los datos tendrá derecho a recurrir al juez de letras en lo civil del domicilio del responsable del registro o banco que se encuentre de turno, según las reglas correspondientes, solicitando amparo a sus derechos. Este es un procedimiento especial que se conoce con el nombre de "habeas data", y que contempla la aplicación de multas a beneficio fiscal.

Sin perjuicio de la existencia de este procedimiento, su aplicación es considerablemente baja, debido entre otros a su larga demora y bajas multas. Es por ello que el recurso más utilizado para hacer valer estos derechos por parte de sus titulares es el recurso de protección, en virtud de la garantía constitucional establecida en el artículo 19 N°4.

CSIRT

Equipo de Respuesta ante Incidentes
de Seguridad Informática

CSIRT
https://www.csirt.gob.cl/

Teatinos 92 piso 6
Santiago, Chile

CONTÁCTANOS

+(562) 2486 3850

registra un incidente

Síguenos

Twitter de CSIRT
https://twitter.com/csirtgob/

LinkedIn
https://www.linkedin.com/company/csirt-gob/

Youtube
https://www.youtube.com/channel/UCua0E5Jz9V1Rn-VtLHPP4Nw/

Instagram
https://www.instagram.com/csirtgobcl

Ministerio del Interior y Seguridad Pública

Gobierno de Chile

CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

Teatinos 92 piso 6
Santiago, Chile
www.csirt.gob.cl