

 ALESSANDRI 130 AÑOS
Ayer.Hoy.Mañana.

20
24

www.alessandri.legal



Ley 21.663 marco de ciberseguridad

09 - mayo - 2024

Contexto



80%

De los líderes encuestados creen que los datos son importantes para su organización.



32%

De las organizaciones ha hecho esfuerzos relevantes en el uso de datos.



66%

De los líderes afirman que crecerán las inversiones para uso de datos.



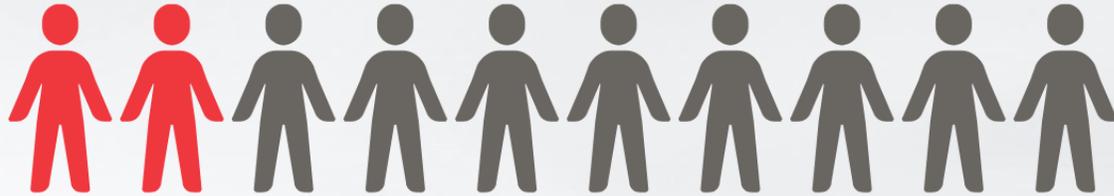
50%

De las empresas están alcanzando niveles avanzados en prácticas de Data-Driven.

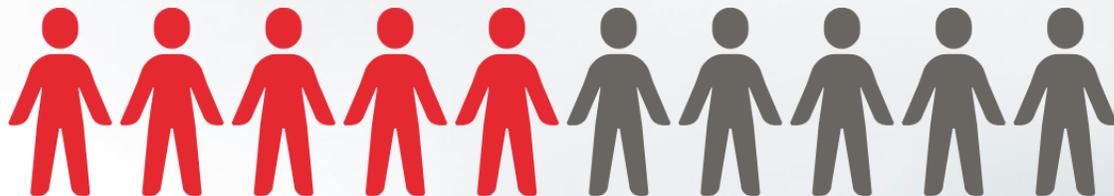
Fuente: "El uso de los datos" Data-Driven 2024

Autorregulación de la industria

Solo el 21,8% de los profesionales encuestados declara tener “conocimiento del proyecto” que modifica la Ley N°19.628 sobre la protección de datos personales.



El 53,3% de los líderes empresariales declara hacer uso responsable de datos, bajo los principios de confidencialidad, integridad y disponibilidad, garantizando el correcto tratamiento de la información que proporciona el cliente



Chile

47% de los internautas de Chile proporciona sus datos personales a cambio de descuentos o cupones, sin verificar si estos son reales o se trata de una estafa.

76% de los usuarios estarían abierto a publicar información comprometedor a cambio de un beneficio o pago.

28% declara que comparte datos sensibles en redes sociales.

Ciberataques



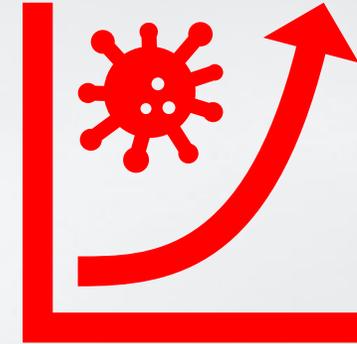
Latam

Malware aumentó un 617%
Phishing y troyano bancario 50%



Chile

Troyano bancario aumentó 95%



Fuente: KAPERSKY Agosto 2023. (Se considera el período junio 2022 a julio 2023)

Ciberataques

Chile

Se detectaron 741.152- 84%

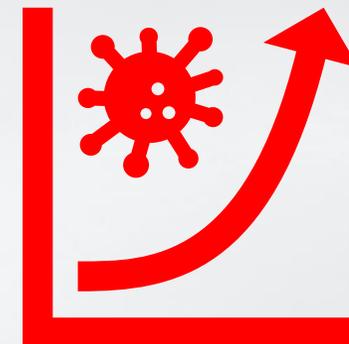


Servicios financieros 51,8%

Sector público 20,6%



frecuencia
sofisticación



Fuente: TRELIX Chile Cyber Threat Activity . (Período enero a septiembre 2023)

Regulaciones

- Ley marco de ciberseguridad.
- Normas sectoriales.
- Proyecto de ley de protección de datos personales.
- Proyecto de ley sobre IA.

Ley marco ciberseguridad

Objetivos de la ley

Establecer institucionalidad

-

- Agencia de Ciberseguridad.
- CSIRT Nacional y de Defensa
- Comité interministerial

Mínimos de prevención y de respuesta de incidentes.

-

Ámbito de aplicación



Servicios esenciales



Operadores de importancia vital OIV

Servicios esenciales

Aquellos provistos por los organismos de la Administración del Estado y por el Coordinador Eléctrico Nacional.

Los prestados bajo concesión de servicio público.

Los proveídos por instituciones privadas que realicen las siguientes actividades:

- Generación, transmisión o distribución eléctrica.
- Transporte, almacenamiento o distribución de combustibles.
- Suministro de agua potable o saneamiento.
- Infraestructura digital;
- Servicios digitales y servicios de tecnología de la información gestionados por terceros.
- Transporte terrestre, aéreo, ferroviario o marítimo, así como la operación de su infraestructura respectiva.
- Banca, servicios financieros y medios de pago.
- Administración de prestaciones de seguridad social.
- Servicios postales y de mensajería.
- Prestación institucional de salud por entidades tales como hospitales, clínicas, consultorios y centros médicos, y la producción y/o investigación de productos farmacéuticos.

Operadores de importancia vital (OIV)

La Agencia calificará como OIV a quienes cumplan los siguientes requisitos:

1. Que la prestación de dicho servicio dependa de redes y sistemas informáticos; y
2. Que la afectación, interceptación, interrupción o destrucción de sus servicios tenga un **impacto significativo** en la seguridad y el orden público, en la **provisión continua y regular de servicios esenciales**, en el efectivo cumplimiento de las funciones del Estado o, en general, de los servicios que éste debe proveer o garantizar.

Aunque no sean servicios esenciales, por haber adquirido un rol crítico en el abastecimiento de la población, distribución de bienes o la producción de indispensables o estratégicos para el país.

Deberes generales

Aplicar de manera permanente las medidas para prevenir, reportar y resolver incidentes de ciberseguridad. Estas medidas podrán ser de naturaleza tecnológica, organizacional, física o informativa, según sea el caso.

Reportar al CSIRT Nacional los ciberataques e incidentes de ciberseguridad que puedan tener efectos significativos.

Deberes específicos de los OIV

Implementar un **sistema de gestión de seguridad** de la información continuo con el fin de determinar riesgos.

Mantener un **registro de las acciones ejecutadas** que compongan el sistema de gestión de seguridad de la información.

Elaborar e implementar **planes de continuidad operacional y ciberseguridad**.

Realizar continuamente operaciones de **revisión, ejercicios, simulacros** y análisis de las redes, sistemas informáticos y sistemas.

Adoptar de forma oportuna y expedita las **medidas necesarias para reducir el impacto y la propagación de un incidente** de ciberseguridad.

Contar con **certificaciones**.

Informar a los potenciales afectados.

Contar con programas de **capacitación, formación y educación continua** de sus trabajadores y colaboradores, que incluyan campañas de ciberhigiene.

Designar un **delegado de ciberseguridad**.

Obligación de reportar

- ¿A quién?** : CSIRT Nacional
- ¿Qué?** : Ciberataques e incidentes de ciberseguridad que puedan tener efectos significativos.
- ¿Cuándo?** : Lo antes posible.

Efectos significativos : Si es capaz de interrumpir la continuidad de un servicio esencial o afectar a la integridad física o a la salud de las personas, así como en el caso de afectar a sistemas informáticos que contengan datos de carácter personal.

Para determinar la **importancia de los efectos de un incidente**, se tendrán en cuenta los siguientes criterios:

- Número de personas afectadas.
- Duración del incidente.
- Zona geográfica afectada.

Obligación de reportar

Alerta temprana: máximo de 3 horas.

Actualización de la ocurrencia del evento: 72 horas.

- Evaluación inicial del incidente,
- Gravedad e impacto.

Informe final: plazo máximo 15 días.

Agencia de ciberseguridad

Organismo público de carácter técnico y especializado.

Asesorar al Presidente en asuntos relacionados con la Ciberseguridad.

Funciones (entre otras):

- Regulatorias: emitir protocolos y normas, interpretación y aplicación de la ley.
- Coordinación: CSIRT Nacional y otros organismos públicos, así como con instituciones privadas.
- Clasificación: servicios esenciales y OIVs.
- Sancionatorias: velar por el cumplimiento de las disposiciones de la ley y sus reglamentos.

Sanciones

Hasta 40.000 UTM en el caso de OVIs (aprox. USD \$2,800,000).

Para la fijación de la multa se tendrá en consideración:

El grado en que el infractor adoptó las medidas necesarias para resguardar la seguridad informática de las operaciones.

La probabilidad de ocurrencia del incidente.

El grado de exposición del infractor a los riesgos.

La gravedad de los efectos de los ataques incluidas sus repercusiones sociales o económicas.

La reiteración en la infracción dentro del plazo de tres años, contado desde el momento en que se produjo el incidente.

El tamaño y la capacidad económica del infractor.

Sanciones

Cuando por unos mismos hechos y fundamentos jurídicos el infractor pudiese ser sancionado con arreglo a esta ley y a otra u otras leyes, de las sanciones posibles, se le impondrá la de mayor gravedad.

Non bis idem.

Prescripción: 3 años.

Recursos: Reclamo ante superior jerárquico, reposición e ilegalidad.

Entrada en vigencia

Decreto del Presidente de la República. (Un plazo de un año desde la publicación de la ley (8 de abril de 2024).

La entrada en vigencia no podrá ser inferior a seis meses desde la publicación de la ley.



6 meses: Ministerio del interior y seguridad pública dictará reglamentos.



Macarena Gatica L
mgatica@alessandri.cl

Socia



El Regidor 66, piso 10, Las Condes,
Santiago, Chile - Casilla 136-34 Las
Condes - Tel. (56 2) 2787 6000

alessandri@alessandri.cl
www.alessandri.legal