EM ESTUDIO DE MERCADO

2023

ICEX España Exportación e Inversiones

El mercado de la ciberseguridad en Chile

Oficina Económica y Comercial
de la Embajada de España en Santiago de Chile

EM ESTUDIO DE MERCADO

29 de noviembre de 2023
Santiago de Chile

Este estudio ha sido realizado por
Jorge Calle Merillas

Bajo la supervisión de la Oficina Económica y Comercial
de la Embajada de España en Santiago de Chile

http://chile.oficinascomerciales.es

Editado por ICEX España Exportación e Inversiones, E.P.E.

NIPO: 114-23-010-0

Índice

1. Resumen ejecutivo

El propósito de este estudio de mercado es examinar la industria de la ciberseguridad en Chile, con el fin de asistir a las empresas del sector español en sus iniciativas de internacionalización y penetración en el mercado chileno. En este contexto, se busca presentar la situación actual de la ciberseguridad en Chile y anticipar su posible desarrollo futuro, proporcionando las herramientas esenciales para facilitar la incursión de las empresas españolas en este mercado.

La ciberseguridad, una rama esencial de las Tecnologías de la Información y Comunicación (TIC), se centra en proteger la información digital. En Chile, la economía digital representó aproximadamente el 25 % del Producto Interno Bruto (PIB) en 2021, liderando la región según el informe de Accenture y Oxford Economics sobre *El Avance de la Economía Digital en Chile*. Este destacado rendimiento se traduce en un primer puesto en el Índice de Valor Económico Digital regional, superando a países como Brasil, Argentina y México. Según estimaciones de IDC, el mercado de ciberseguridad en Chile alcanzó un tamaño de 282 millones de USD en 2022, y se espera que experimente una tasa de crecimiento anual del 10,5 % hasta el año 2024. Asimismo, de acuerdo con las proyecciones de Mordor Intelligence, se anticipa que el mercado mantendrá un crecimiento constante en los próximos años, con una tasa de crecimiento medio anual compuesta del 9,8 % hasta el año 2028.

El segmento de la ciberseguridad emerge como uno de los subsectores de las TIC con un crecimiento más acelerado en Chile. Este impulso se atribuye al aumento de los ataques cibernéticos, siendo evidente en el caso de Chile, que se enfrentó a 14.000 millones de intentos de ciberataques en el año 2022, con un incremento del 50 % en comparación con el año anterior. La proliferación del trabajo remoto, una consecuencia de la pandemia de COVID-19, ha aflorado vulnerabilidades significativas. A pesar del notorio aumento en la presencialidad durante este último año, aproximadamente el 26 % de los trabajadores continúa participando en alguna modalidad de teletrabajo, ya sea total o parcial. Este panorama de crecimiento se ve acentuado por la creciente priorización en la Administración Pública chilena a través de la promulgación de un marco normativo en ciberseguridad, y la expansión generalizada de Internet y el comercio electrónico.

A pesar de la presencia de diversos participantes, el mercado chileno de ciberseguridad se considera moderadamente consolidado, con una destacada influencia de actores globales, principalmente estadounidenses. Aunque hay numerosas empresas compitiendo en este sector, un grupo reducido, entre las que destacan Leonardo, AVG Technologies, Check Point Software Technologies Ltd., Cisco Systems Inc. y Dell Technologies Inc., ejerce una importante influencia en una parte significativa del mercado.

Los clientes principales se agrupan en tres categorías: Administración Pública; empresas y operadores críticos; micro, pequeñas y medianas empresas (mipymes) y particulares. La Administración Pública busca soluciones integrales para proteger la información crítica, mientras que las empresas y operadores críticos requieren soluciones personalizadas según sus sectores, destacando la importancia de la seguridad en industrias especializadas. A nivel gubernamental, la marcada vulnerabilidad se evidenció en eventos de 2022, como los ataques al Estado Mayor Conjunto y al Poder Judicial, subrayando la necesidad de fortalecer las capacidades de ciberseguridad en la Administración Pública. En el sector privado, el comercio minorista y mayorista se ha vuelto especialmente vulnerable. Según el informe *X-Force Threat Intelligence Index 2022* de IBM Security, el comercio minorista y mayorista superó a los sectores financiero y de seguros como blanco principal de ataques cibernéticos en Chile, representando el 28 % de los casos en 2022. El estudio resalta la importancia de fortalecer las medidas de ciberseguridad en todas las empresas, independientemente de su sector, para mitigar riesgos y proteger la información crucial. Las mipymes, esenciales para la economía chilena, se enfrentan a un riesgo significativo, con un tercio de los ataques globales dirigidos hacia ellas, subrayando la urgencia de implementar medidas efectivas de ciberseguridad para salvaguardar su integridad y contribuir a la estabilidad económica general.

La variabilidad de precios en el mercado chileno de ciberseguridad se atribuye a la diversidad de productos y servicios. Grandes empresas, Administración Pública y *startups* liderarán las inversiones, y la negociación de precios para soluciones empresariales dependerá del nivel de riesgo asumido. Las empresas españolas, reconocidas por su capacidad y liderazgo en Responsabilidad Social Corporativa, disfrutan de una percepción positiva en Chile, fortalecida por el Memorándum de Entendimiento sobre Cooperación en Materia de Ciberseguridad firmado por España y Chile en julio de 2023, que abre nuevas oportunidades de colaboración.

En términos de canales de distribución, tanto el canal directo como el indirecto desempeñan un papel crucial. El canal directo, caracterizado por contratos directos con clientes finales, requiere una mayor participación en eventos especializados. El canal indirecto, a través de distribuidores como mayoristas, distribuidores y minoristas, facilita la exportación de servicios y reduce riesgos.

En cuanto al acceso al mercado, las importaciones de productos de ciberseguridad están sujetas a aranceles y al Impuesto sobre el Valor Añadido (IVA). En el ámbito de aranceles, las importaciones de productos (*hardware*) están sujetas al pago del arancel general del 6 %, si bien el Tratado de Libre Comercio con la Unión Europea exime a los productos de ciberseguridad de este arancel. Además, desde enero de 2004, el valor aduanero de los programas informáticos importados en soporte físico considera únicamente el valor del soporte físico, reduciendo significativamente los pagos por derechos aduaneros en el caso del *software*. Sin embargo, también existen barreras no arancelarias, como regulaciones complejas, piratería de *software* y conciencia limitada sobre ciberseguridad.

Respecto a las perspectivas del sector, la ciberseguridad en Chile se encuentra en un momento de crecimiento y consolidación impulsado por la creciente digitalización, el aumento de las amenazas cibernéticas y la concienciación sobre la importancia de la seguridad digital. Tendencias como la evolución hacia la nube segura, la expansión del Internet de las Cosas y la integración de la Inteligencia Artificial para la defensa cibernética marcarán avances cruciales tanto a nivel global como nacional.

En resumen, a pesar de los desafíos, el sector de ciberseguridad en Chile presenta oportunidades para las empresas españolas. La colaboración público-privada, la cooperación internacional y el fortalecimiento de las políticas de ciberseguridad ofrecen un terreno fértil para la expansión y liderazgo de empresas españolas en este dinámico mercado.

2. Definición del sector

En los últimos años, la sociedad ha establecido una fuerte dependencia del mundo digital debido al avance y desarrollo de nuevas tecnologías, lo cual ha dado lugar a la evolución digital y al surgimiento del ciberespacio. Sin embargo, este crecimiento también ha provocado un aumento exponencial en el número de amenazas y ataques cibernéticos, debido al rápido proceso de digitalización. En consecuencia, empresas, instituciones y particulares han adquirido conciencia sobre la importancia de proteger la información sensible generada y compartida a través de medios digitales. Además, la cantidad de amenazas y su complejidad para ser detectadas y prevenidas continúan en aumento.

La ciberseguridad se ha convertido en un tema prioritario a nivel mundial, ya que nadie está exento de ser víctima de un ciberataque. Empresas, gobiernos, hospitales, instituciones financieras, pymes y usuarios finales se encuentran expuestos a las amenazas que existen en la red. Comprender la importancia de este movimiento proporciona una perspectiva más amplia sobre las estrategias, planes y buenas prácticas que deben implementarse en las organizaciones.

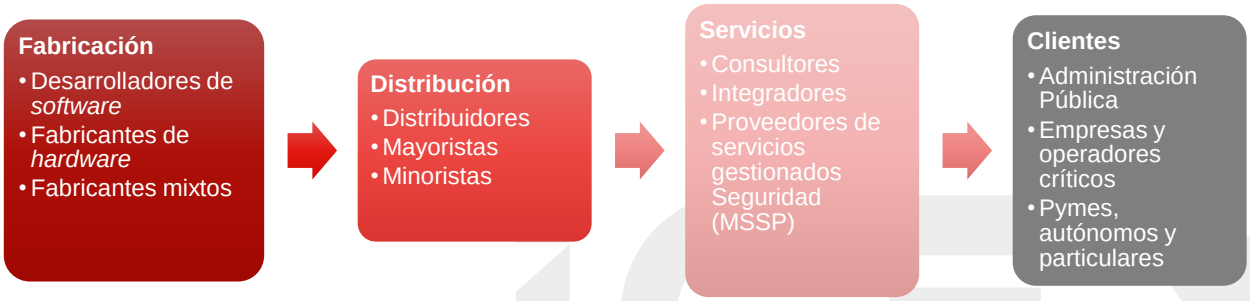
Es común utilizar el término “seguridad de la información” como sinónimo de “ciberseguridad”, pero es importante aclarar las diferencias existentes entre estos dos conceptos íntimamente relacionados. La **seguridad de la información** se refiere a las medidas preventivas que permiten almacenar y preservar la información de una empresa, institución o particular. Por otro lado, la ciberseguridad se centra específicamente en la protección de datos digitales y los sistemas interconectados que los procesan, almacenan o transmiten, frente a ataques maliciosos en el entorno cibernético. Mientras que la **ciberseguridad** se basa en realizar ataques ofensivos contra las amenazas existentes, la seguridad de la información contempla aspectos defensivos para proteger los sistemas de información.

Según ENISA (The European Union Agency for Cybersecurity), la ciberseguridad abarca todos los aspectos de prevención, previsión, tolerancia, detección, mitigación, eliminación, análisis e investigación de ciberincidentes[1]. Teniendo en cuenta los diferentes tipos de componentes del ciberespacio, la ciberseguridad debe cubrir: Disponibilidad, Fiabilidad, Seguridad, Confidencialidad, Integridad, Mantenibilidad (para sistemas tangibles, de información y redes); Robustez, Supervivencia y Resistencia (para soportar la dinamicidad del ciberespacio); y Responsabilidad, Autenticidad y No Rechazo (para apoyar la seguridad de la información).

[1] Cualquier suceso que pueda suponer un riesgo para la seguridad de las redes y sistemas de información de un usuario u organización, bien sea provocado por un agente de forma intencionada o debido a una mala práctica.

2.1. Cadena de valor

La ciberseguridad forma parte del sector de las Tecnologías de la Información y la Comunicación (TIC). En este sector, se distinguen tres actores clave: los fabricantes de *hardware* y *software*, los distribuidores de productos de ciberseguridad y las empresas que brindan servicios de ciberseguridad. Estas actividades suelen coexistir y es común que los fabricantes de *software* vendan directamente tanto a minoristas como a los usuarios finales.



En cuanto a la fabricación, los **desarrolladores de *software*** ofrecen soluciones y aplicaciones que aseguran la protección de redes y facilitan el control de acceso web e identidad de usuarios. Por otro lado, los **fabricantes de *hardware*** desarrollan herramientas físicas para garantizar la seguridad en la movilidad y en redes criptográficas. Finalmente, los fabricantes mixtos ofrecen soluciones tanto de *software* como de *hardware*.

En lo tocante a la distribución, los **mayoristas** se encargan de distribuir productos de ciberseguridad a consultoras, integradoras y proveedores de servicios de ciberseguridad. Los **distribuidores** venden las soluciones directamente a empresas de ciberseguridad o a clientes finales, pudiendo trabajar con varios fabricantes. Por último, los **minoristas**, como tiendas de informática o grandes superficies, se dirigen principalmente a pymes y particulares como puntos de venta de productos de ciberseguridad.

Los servicios de ciberseguridad incluyen **consultoras tecnológicas,** ofrecen asesoramiento, soporte y respuesta a temas de seguridad informática, implementando estrategias de seguridad, formación a empleados y servicios SaaS[2]; los **integradores** resuelven problemas complejos de seguridad TIC, adaptándose a las necesidades de los usuarios mediante soluciones propias y productos de diversos fabricantes; los **proveedores de servicios gestionados** ofrecen servicios

[2] *Software as a Service.*

de seguridad externalizados, incluyendo consultoría, desarrollo e integración de servicios como la monitorización de cortafuegos y el control de cuentas de usuario y acceso a la red.

Los clientes o demandantes de soluciones y servicios de ciberseguridad se pueden clasificar en tres grandes grupos:

- **Administraciones Públicas**, debido a la naturaleza de la información sensible que manejan, necesitan soluciones de seguridad integral, ciberinteligencia y ciberdefensa. Para ofrecer servicios a este tipo de clientes, es posible participar en licitaciones o establecer contratos directos.
- **Empresas y operadores críticos,** requieren una amplia gama de soluciones para abordar sus necesidades de seguridad. Estas soluciones incluyen auditorías técnicas, gestión de incidentes, seguridad integral y en la nube, así como soluciones industriales altamente especializadas.
- **Pymes, autónomos y particulares,** las soluciones de ciberseguridad demandadas suelen ser más básicas (antivirus). Por ello, la distribución y prestación de servicios se realiza generalmente a través de licencias o mediante la entrega de productos físicos.

2.2. Tipología de ataques y soluciones

2.2.1. Tipos de ciberamenazas

Algunos de los ciberataques más comunes son:

- ***Malware*: *software*** malicioso, como *spyware*, *ransomware*, virus y gusanos. Se introduce en las redes aprovechando vulnerabilidades, a menudo cuando un usuario hace clic en un enlace peligroso o descarga un archivo que instala un *software* de riesgo. Una vez dentro del sistema, el *malware* puede realizar varias acciones, como bloquear el acceso a componentes clave de la red (*ransomware*), instalar más *malware* o *software* dañino, robar información confidencial mediante la transmisión de datos del disco duro (*spyware*) y alterar componentes específicos para hacer que el equipo sea inoperable.
- **Suplantación de identidad (*Phishing*):** envió de comunicaciones fraudulentas que parecen ser confiables, generalmente a través del correo electrónico. Su objetivo es robar datos sensibles o instalar *malware* en el dispositivo de la víctima. El *phishing* se ha vuelto una amenaza cibernética frecuente.
- **Ataque de intermediario:** también conocidos como ataques de escucha secreta, se producen cuando los atacantes se infiltran en transacciones entre dos partes, interceptando y robando datos. Estos ataques se producen a través de redes WiFi públicas no seguras, donde los atacantes pueden insertarse entre el dispositivo del usuario y la red. Una vez dentro, el atacante puede instalar *software* para acceder y procesar toda la información de la víctima.

- **Ataque de denegación de servicio:** tiene como objetivo sobrecargar los sistemas, servidores o redes mediante un alto volumen de tráfico, agotando así los recursos y el ancho de banda disponibles. Esto provoca que el sistema no pueda atender las solicitudes legítimas. Además, los atacantes pueden utilizar múltiples dispositivos comprometidos para llevar a cabo un ataque, conocido como ataque por denegación de servicio distribuido (DDoS).
- **Ataques de día cero:** se produce cuando los atacantes aprovechan una vulnerabilidad recién descubierta en un sistema antes de que se implemente un parche o solución para corregirla. Durante esta ventana de tiempo, los atacantes dirigen sus esfuerzos hacia la vulnerabilidad expuesta. La detección de amenazas relacionadas con estas vulnerabilidades de día cero requiere una vigilancia constante.
- **Tunelización de DNS:** utiliza consultas y respuestas del sistema de nombres de dominio (DNS) para evadir las medidas de seguridad convencionales y transportar datos y códigos dentro de una red. Al infectar un sistema, el atacante puede llevar a cabo actividades de control y comando de manera discreta. Este tipo de túnel proporciona una vía para distribuir *malware* o extraer datos, IP y otra información confidencial, codificándolos en respuestas DNS de manera progresiva.
- **Inyección de SQL:** se produce cuando un atacante inserta código malicioso en un servidor que utiliza SQL, lo que obliga al servidor a revelar información que normalmente no se revelaría. El atacante puede llevar a cabo esta inyección de SQL enviando simplemente un código malicioso a través de un campo de búsqueda de un sitio web vulnerable.

2.2.2. Tipos de soluciones

Las soluciones para los destinatarios finales pueden clasificarse en tres grandes tipos según el ONTSI[3]:

1. **Soluciones de prevención**, con el fin de prevenir los incidentes. Dentro de ellas se pueden distinguir: *antimalware*, protegen sistemas informáticos mediante la detección y eliminación de *software* malicioso; antifraude, protege a los usuarios de actividades fraudulentas en la red; de prevención de fuga información, se encargan de identificar, detectar y prevenir la divulgación no autorizada de información, mediante la implementación de políticas de uso y protección de datos; para la protección de las comunicaciones, aseguran la seguridad de los sistemas y dispositivos conectados a una red al monitorear el tráfico generado y recibido; y de seguridad en dispositivos móviles.

2. **Soluciones de control**, destinadas a la gestión y cumplimiento de la legislación. Se incluyen las soluciones de auditoría técnica, auditar sistemas, aplicaciones y datos para determinar posibles fallos de seguridad; de certificación normativa, para garantizar el cumplimiento

[3] Observatorio Nacional de Tecnología y Sociedad.

normativo aplicable y la obtención de certificados; de cumplimiento legal, para facilitar el cumplimiento legal aplicable; y de control de acceso y autentificación, administrar de manera eficiente y segura la información y los perfiles de los usuarios en un entorno organizacional. Estas soluciones incluyen la implementación de políticas de seguridad y control de acceso a los recursos, lo que garantiza que solo los usuarios autorizados tengan acceso a la información y los recursos adecuados.

3. **Soluciones de mitigación**, orientadas a la recuperación y continuidad tras la existencia de un incidente. Dentro de este tipo se pueden distinguir dos soluciones: de contingencia y continuidad, su objetivo es mitigar el impacto de los incidentes de seguridad y facilitar la recuperación rápida mediante medidas y procedimientos claros para responder, contener y resolver los incidentes, así como estrategias de recuperación y pruebas periódicas para evaluar su efectividad; y de inteligencia de seguridad, para gestionar incidentes de ciberseguridad en cualquiera de sus fases y ayudar en la detección de amenazas de forma rápida, identificando vulnerabilidades, priorizando riesgos y automatizando actividades de cumplimiento normativo.

2.3. El sector de la ciberseguridad en Chile

2.3.1. Marco Normativo

Chile Digital 2035

La preocupación del Gobierno en Chile por adaptarse a los nuevos cambios en el paradigma digital apareció a principios del s. XXI. Hace casi 20 años que se adoptó la primera agenda digital, que proponía una serie de medidas con el fin de impulsar el acceso a Internet y el uso de TIC en las empresas, promover el comercio electrónico, modernizar los servicios públicos, así como adoptar nuevos marcos reguladores en el ámbito digital.

Desde ese momento, diversos gobiernos han creado e impulsado distintas agendas y planes de acción (2004, 2007, 2013 y 2020). Sin embargo, estas agendas carecieron de un marco estratégico a largo plazo que trascendiera los ciclos presidenciales y se integre con planes de desarrollo más amplios. Por ello, el Gobierno de Gabriel Boric presentó en 2022 un proyecto resultado de la unión de los intereses del Estado, de los actores del sector privado y de la sociedad civil, *Chile Digital 2035*. Este documento contiene los fundamentos de la Estrategia Digital 2035, la cual servirá como guía del sector TIC y de una sociedad altamente digitalizada.

La estrategia de transformación digital para Chile se sustenta en dos pilares interdependientes: **Chile conectado sin brechas** y **Chile digitalizado**. El primero busca garantizar un acceso equitativo y sin discriminación a la tecnología, mientras que el segundo promueve la adopción generalizada y sostenible de tecnologías digitales en todas las áreas. Dentro del pilar “Chile Digitalizado” se localiza la rama de la ciberseguridad, la cual constituye un elemento central de la política digital y donde, a pesar de haber realizado avances en materia de políticas y acuerdos

internacionales, todavía existe un gran margen de mejora. De acuerdo con el Índice de Ciberseguridad desarrollado por la UIT[4], Chile presenta un nivel de ciberseguridad significativamente inferior a los países de la OCDE, ocupando el puesto 74.º del mundo por detrás de otros miembros de la región como Brasil, México y Uruguay.

Según la UIT, Chile presenta fortalezas significativas en ciberseguridad, destacándose la solidez de su marco legal y los mecanismos de cooperación establecidos. Sin embargo, se identifican como principales debilidades los aspectos técnicos y la capacidad de implementación en este ámbito. Para mejorar sus niveles de ciberseguridad, el Chile Digital ha definido una serie de objetivos y metas:

- **Objetivos:** establecer un ecosistema de ciberseguridad nacional dinámico, robusto y resiliente; cultura integral de ciberseguridad nacional; marcos legales y regulatorios efectivos y dinámicos, protección de derechos en el ciberespacio, y persecución del cibercrimen; cooperación internacional y liderazgo regional, entre otros.

- **Metas:**
  - Creación del Instituto Nacional de Ciberseguridad y del Centro de Capacidades de Ciberseguridad de Iberoamérica antes de 2024.
  - Creación de las nuevas agencias nacionales de Protección de Datos Personales y de Ciberseguridad y Protección de Infraestructura Críticas de la Información antes de 2026.
  - Creación de la totalidad de los CSIRT sectoriales y COC Nacional al 2030.
  - Inversión del gasto en I+D+i de ciberseguridad como porcentaje del PIB en un 0,1 % al 2025 y en un 0,2 % al 2030.
  - Formación de 10.000 profesionales certificados en ciberseguridad al 2035, donde al menos el 30 % de ellos sean mujeres.

Política Nacional de Ciberseguridad (PNCS)

En 2017, Chile promulgó su primera Ley de Ciberseguridad, diseñada para durar hasta 2022. Con el objetivo de fortalecer aún más las defensas digitales del país, en mayo de 2023 se presentó la propuesta de una nueva Política Nacional de Ciberseguridad (PNCS) por parte del Gobierno de Chile. Esta actualización busca adaptarse a las cambiantes amenazas cibernéticas y promover un entorno digital más seguro y resiliente.

A finales de 2023 se publicó en el *Diario Oficial* el Decreto que aprueba la PNCS 2023-2028. Durante la presentación de la propuesta de la PNCS, se destacó su importancia, subrayando que la política está diseñada para proteger tanto a las personas como al país en su conjunto. Además, se señaló que la implementación exitosa de la PNCS podría situar a Chile en los primeros lugares de los

[4] Unión Internacional de Telecomunicaciones.

rankings mundiales de ciberseguridad, lo que podría influir en las decisiones de inversión de las empresas.

La nueva PNCS fue elaborada a lo largo de nueve meses por el Comité Interministerial de Ciberseguridad, que incluye la participación del Coordinador Nacional de Ciberseguridad, la Agencia Nacional de Inteligencia (ANI) y diversas subsecretarías gubernamentales. La política se estructura en torno a cinco ejes fundamentales:

1. **Infraestructura resiliente:** Establecer una infraestructura de la información sólida y resistente, capaz de resistir y recuperarse de incidentes de ciberseguridad.

2. **Derechos de las personas:** Promover la protección en Internet, fortaleciendo la institucionalidad en ciberseguridad para integrar a cada individuo en la sociedad digital de manera segura.

3. **Cultura de ciberseguridad:** Desarrollar una cultura en torno a la educación, buenas prácticas y responsabilidad en materia de ciberseguridad.

4. **Coordinación nacional e internacional:** Impulsar una gobernanza pública para coordinar a nivel internacional y prevenir y enfrentar acciones maliciosas e incidentes en el ciberespacio.

5. **Fomento a la industria y la investigación científica:** Promover el desarrollo de una industria de la ciberseguridad y fomentar la investigación científica aplicada a la ciberseguridad.

Esta propuesta de PNCS refleja el compromiso de Chile con la protección digital y la creación de un entorno cibernético seguro, estableciendo las bases para el desarrollo tecnológico y la participación en la comunidad internacional en el ámbito de la ciberseguridad.

2.3.2. Principales ataques cibernéticos en Chile

En el año 2022, los países de América Latina y el Caribe se enfrentaron a una cifra alarmante de más de 360.000 millones de intentos de ciberataques, según información proporcionada por FortiGuard Labs, el laboratorio de análisis e inteligencia de amenazas de Fortinet. Entre los países de la región, México fue el más afectado, registrando la mayor cantidad de intentos de ataques, con un total de 187.000 millones de ataques. Brasil le siguió en segundo lugar con 103.000 millones de intentos, mientras que Colombia reportó alrededor de 20.000 millones y Perú cerca de 15.000 millones.

De acuerdo con el último informe semestral sobre el panorama de amenazas globales publicado por Fortinet, América Latina y el Caribe experimentaron un incremento cercano al 30 % en los ataques cibernéticos anuales en comparación con 2021, ubicándose como la segunda región con el mayor aumento relativo de ataques. En el caso de Chile, recibió 14.000 millones de intentos de

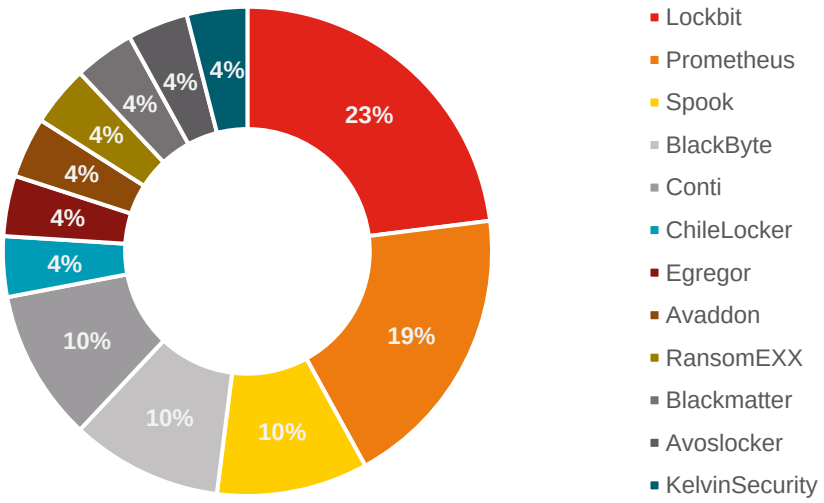
ciberataques durante el año 2022, lo que representa un **incremento del 50 %** en comparación con el año anterior.

Durante el año 2022, hubo un aumento significativo de eventos que comprometieron la seguridad en Latinoamérica. En este panorama se identificaron organizaciones delictivas globales responsables de ataques de ***ransomware***, ***data leak*** y ***phishing*** en la región. El *Reporte de Ciberseguridad 2022 y Tendencias 2023 en Chile y Latinoamérica* de Entel Ocean profundiza en este tipo de ataques y organizaciones.

Ransomware

Según el Reporte, se identificaron 29 actores vinculados con *ransomware* en la región, de los cuales solo 12 llevaron a cabo actos delictivos en Chile. Entre estos, Lockbit se destacó como el principal responsable de vulnerar los sistemas de seguridad en el país, representando aproximadamente el 50 % de las incidencias registradas en 2022, lo que perfila a Lockbit como la mayor amenaza de *ransomware* para el año 2023.

INCIDENCIA DE *RANSOMWARE* EN CHILE
Periodo 2020-2022



Fuente: elaboración propia a partir de datos de Enel Ocean.

Data leak

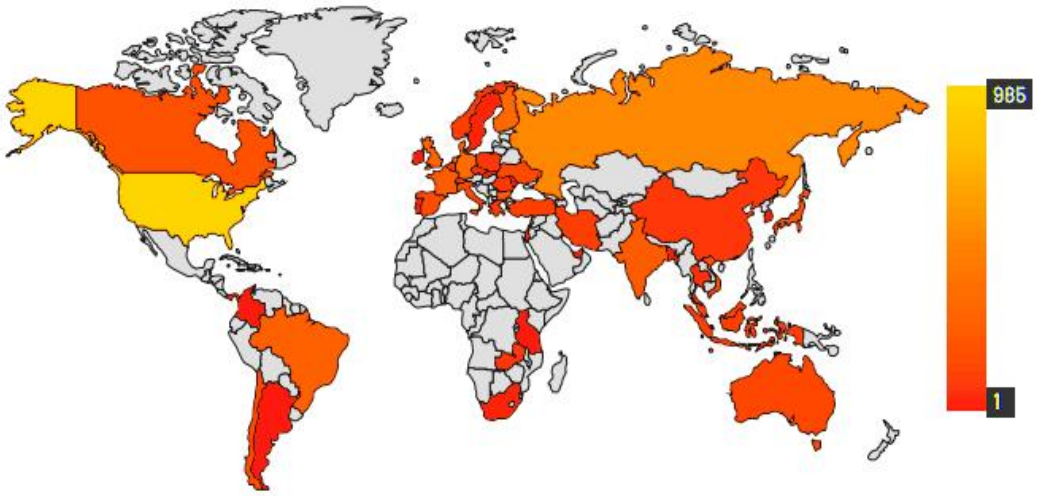
Durante el año 2022, las filtraciones de datos o *data leaks* en Chile alcanzaron un total de 24 incidencias, experimentando un crecimiento del 50 % en comparación con las cifras registradas en 2021. Este incremento se atribuye principalmente a la aparición de nuevos actores en el panorama

de amenazas. Se proyecta que para el año 2023, el número de incidentes relacionados con filtraciones que involucran a organizaciones chilenas se acercará a 26.

Entre los principales responsables de estos ataques en Chile durante 2022, destacan Kelvin Security con 3 ataques; Sombraman1919, d3c0d3x, anony y PwnSec, con dos ataques cada uno. El resto de actores realizaron un ataque cada uno, entre los que sobresale Kristina, quien desempeñó un papel protagonista en el panorama chileno en 2021 con 5 filtraciones, aunque perdió relevancia en el último año.

Phishing

GEOLOCALIZACIÓN DE IP ORIGEN DE ATAQUES *PHISHING* EN CHILE
2022



Fuente: elaboración propia a partir de datos de Enel Ocean.

Las campañas de *phishing* han experimentado un crecimiento acelerado a nivel global, y Chile no es una excepción. Identificar a los actores involucrados en estas campañas resulta difícil debido a la gran oferta de *hosting* gratuitos o de bajo costo que utilizan para ocultar sus operaciones. Aunque la mayoría de las IP donde se alojan las campañas de *phishing* dirigidas a Chile y Latinoamérica están geolocalizadas en Estados Unidos, no se puede asegurar que hayan comenzado allí, ya que este país alberga la mayoría de los *hosting* a nivel mundial. A pesar de las medidas adoptadas por los ciberdelincuentes para ocultar su ubicación e identidad, el mapa anterior proporciona una idea de cómo se distribuyen las campañas de *phishing* que han afectado a Chile a nivel global.

2.3.3. Economía digital en Chile

La economía digital[5] en Chile representó aproximadamente el 25 % del PIB en 2021 según el informe de Accenture y Oxford Economics *El Avance de la Economía Digital en Chile*, situando a Chile en primer lugar del Índice de Valor Económico Digital en la región por su nivel actual de adopción de tecnologías digitales, aceleradores y talento digital, por delante de Brasil (24,5 %), Argentina (18,5 %) y México (17,9 %). Además, es importante destacar que Chile exhibe un índice de Valoración Económica Digital (VED) de 33,1, lo cual lo sitúa por encima de otros países de la región en este aspecto. No obstante, hay que resaltar que este valor se encuentra considerablemente distante del líder global, Estados Unidos, cuyo índice duplica la cifra de Chile, alcanzando los 71,4 puntos. A pesar de esta disparidad cuantitativa, tanto Chile como Estados Unidos presentan un equilibrio en los tres pilares que componen el VED: tecnologías digitales, aceleradores digitales y talento digital.

Al realizar un análisis más exhaustivo de cada uno de los tres pilares, se revelan resultados de interés para Chile. El país se distingue por contar con el talento requerido para evolucionar hacia una economía fundamentada en el conocimiento. Sin embargo, es importante no descuidar la recalificación de aquellos empleos que presentan un alto riesgo de automatización, así como apostar por adquirir nuevas capacidades digitales que darán forma al trabajo del futuro.

Tecnologías digitales

En Chile, el empleo de **tecnologías habilitadoras** como Cloud, Big Data (BD) e Internet de las Cosas (*IoT*) aún no está ampliamente difundido, con una adopción limitada de la nube y la mayoría de las organizaciones utilizando un enfoque híbrido. En términos de **participación digital**, Chile ha experimentado un crecimiento notable en transacciones tecnológicas, especialmente en el ámbito empresarial B2B, ubicándose en el puesto 38 a nivel global del índice de preparación digital en transacciones B2B, y superando así a otros países de la región. Aunque Chile es el líder en América Latina en términos de **contribución del capital TIC** al PIB, ha experimentado una disminución relativa en el capital tecnológico en los últimos años, lo que ha afectado las oportunidades de expansión de la economía digital en el país.

Aceleradores digitales

En el ámbito de los **negocios digitales**, Chile destaca por su estabilidad económica y ocupa el segundo lugar en la región en el *ranking* de facilidad para hacer negocios. Aunque aún se deben mejorar el entorno regulatorio y las políticas de acceso a financiamiento para impulsar la transformación digital. La Fundación País Digital desempeña un papel importante en la coordinación entre el sector público y privado para promover la economía digital. En cuanto a la **priorización digital por parte del Gobierno**, Chile ha invertido en tecnología para modernizar el sector público,

[5] Valor que aporta la tecnología digital a todos los sectores de la economía a partir del uso de talento, equipos y bienes intermedios digitales empleados en la producción. Para determinar su valor se utilizan tres impulsores de Valor Digital: tecnología, aceleradores digitales y talento digital.

ocupando el puesto 36.º en el *ranking* global de gobierno electrónico. Además, los gobiernos locales y municipales están avanzando en la digitalización, aprovechando el potencial del IoT, el *BD* y la analítica. En términos de **infraestructura de comunicaciones**, Chile ha logrado avances significativos en el ancho de banda internacional, la cobertura 4G y la fibra óptica, impulsados por el Plan Nacional Digital y la colaboración público-privada. De hecho, en 2020 se produjo una adopción acelerada en fibra óptica (62 %) y en 4G (12 %) respecto al año anterior. El país cuenta con una alta tasa de conectividad, lo que sienta las bases para el desarrollo del *IoT* en áreas clave como la salud, la minería, las ciudades inteligentes y el transporte conectado.

Talento digital

En Chile, el desarrollo de **nuevas formas de trabajo digital** ha sido impulsado por el avance de Internet, la proliferación de dispositivos móviles y la integración de la tecnología en la vida cotidiana. A pesar de este progreso, muchas empresas chilenas aún enfrentan obstáculos para adoptar plenamente estas modalidades debido a barreras como la falta de conocimiento, regulaciones sectoriales y barreras culturales. Para mantenerse competitivo en la era digital, el país debe centrarse en la transformación del **sector educativo**, ya que el atraso en formación y educación en comparación con otros países puede generar desafíos en términos de habilidades digitales. Además, aunque Chile muestra un ***stock* de trabajadores digitales** por encima del promedio, se requiere un esfuerzo acelerado en la digitalización de la fuerza laboral para adaptarse a la automatización y aprovechar las habilidades humanas más valiosas. Mediante el reentrenamiento, el rediseño del trabajo y la adquisición de talento diversificado, el país puede mitigar los riesgos y maximizar las oportunidades en este entorno en constante evolución.

La destacada posición de Chile como líder latinoamericano en términos de digitalización y su madurez en el ámbito de la economía digital presentan buenas perspectivas para el mercado de la ciberseguridad en el país. A medida que las tecnologías digitales continúan avanzando, la necesidad de proteger los sistemas y datos se vuelve cada vez más crucial. La intensa adopción de tecnologías digitales en Chile crea una demanda creciente de soluciones y servicios de ciberseguridad para garantizar la protección de la información y mitigar los riesgos asociados a las amenazas cibernéticas. Esto brinda oportunidades para el desarrollo y crecimiento de empresas especializadas en ciberseguridad, así como para la formación de profesionales en este campo. Chile, con su liderazgo en digitalización, está bien posicionado para capitalizar estas oportunidades y fortalecer aún más su seguridad digital.

3. Oferta – Análisis de competidores

3.1. Mercado global

Según Mordor Intelligence, se estima que el mercado global de seguridad cibernética alcance un valor de 182,86 miles de millones de USD en 2023. Además, se espera que experimente un crecimiento medio anual compuesto del 11,44 % y alcance los 314,28 miles de millones de USD para el año 2028. Este crecimiento se impulsa principalmente por las plataformas emergentes de comercio electrónico en línea y la adopción de tecnologías fundamentales como Internet de las Cosas (IoT), Inteligencia Artificial (IA) y Seguridad en la Nube, entre otras.

Se estima que para el año 2025, las pérdidas asociadas a delitos de ciberseguridad alcanzarán la alarmante cifra de 10.500 miles de millones de USD, equivalente a la suma de las economías de Japón, Alemania y Suiza, según cifras de Cybersecurity Ventures. Además, se proyecta que en 2031 se producirá un ataque de *ransomware* cada dos segundos dirigido a negocios, usuarios y dispositivos. Ante esta creciente amenaza, los responsables de la seguridad de la información y los equipos de ciberseguridad, así como las personas en general, deberán dedicar más tiempo y esfuerzo para protegerse de los delincuentes cibernéticos.

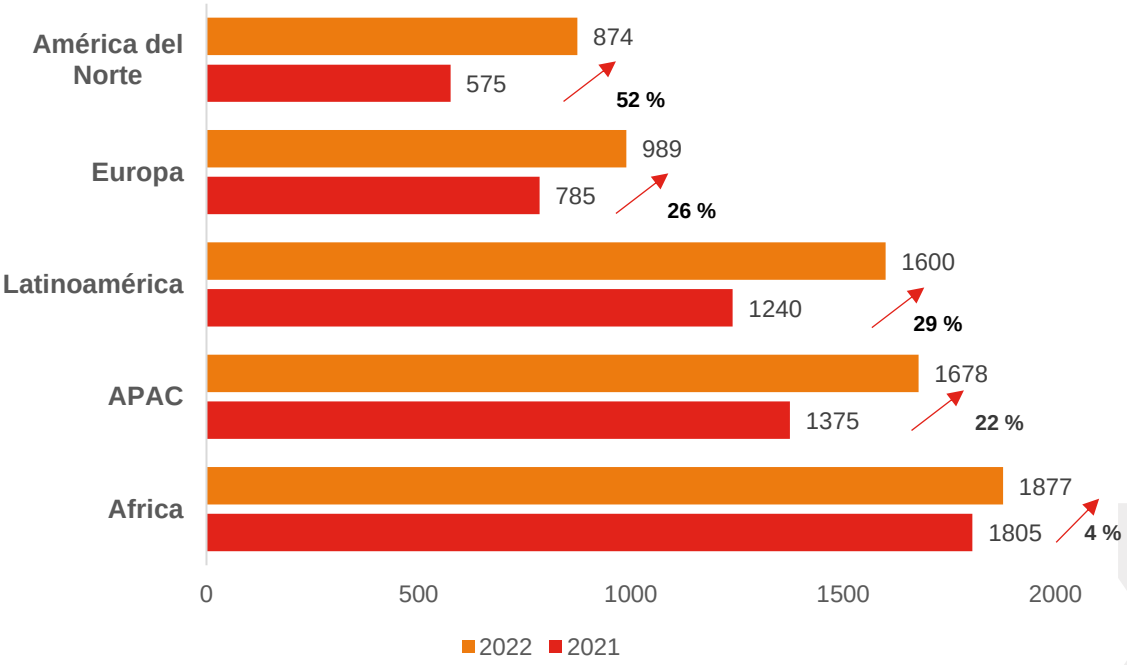
Los ciberataques están sufriendo un aumento a nivel mundial, con un incremento del 38 % en ataques semanales a redes corporativas en 2022. Se observan tres tendencias principales: la evolución del *ransomware* con grupos criminales más ágiles, el enfoque de los *hackers* hacia herramientas de colaboración empresarial y el aumento de ataques dirigidos a instituciones académicas debido a la rápida digitalización durante la pandemia. Este escenario plantea desafíos adicionales debido al trabajo remoto y a la falta de preparación en seguridad de las instituciones educativas.

Según las estadísticas proporcionadas por Check Point, el volumen global de ciberataques alcanzó un máximo histórico en el último trimestre de 2022, con un promedio de 1.168 ataques semanales por organización. Durante el año 2022, los sectores más afectados fueron la educación/investigación, la administración pública y la sanidad. En términos de geografía, África experimentó el mayor volumen de ataques, con 1.875 ataques semanales por organización, seguida por APAC[6] con 1.691 ataques semanales por organización. América del Norte (+52 %), **América Latina (+29 %)** y Europa (+26 %) fueron las regiones que experimentaron los mayores incrementos de ciberataques en comparación con el año anterior.

[6] Asia-Pacífico.

ATAQUES RECIBIDOS POR UNA ORGANIZACIÓN EN CADA REGIÓN

Ataques semanales en 2021 y 2022



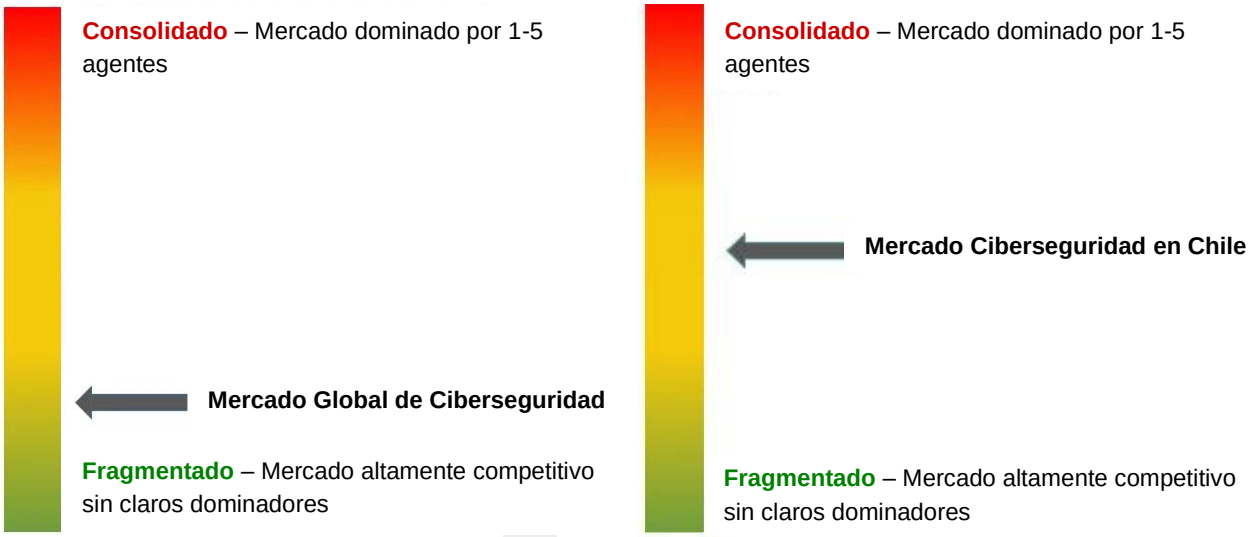
Fuente: elaboración propia a partir de datos de Check Point.

El crecimiento del mercado de la ciberseguridad presenta disparidades regionales. Estados Unidos, China, Alemania, Reino Unido y Japón son los principales mercados nacionales de ciberseguridad, sin embargo, se espera que países con menor mercado como Brasil o EAU[7] experimenten un crecimiento considerablemente mayor en comparación con estos líderes. Aunque el mercado global presenta desafiantes barreras de entrada, varios nuevos operadores han logrado destacar y establecerse en este competitivo espacio. Los principales actores en el mercado mundial de la ciberseguridad son Cisco Systems, Inc. (EE. UU.), IBM Corporation (EE. UU.), Fortinet, Inc. (EE. UU.), Check Point Software Technologies (Israel), CrowdStrike Holdings, Inc. (EE. UU.) y Microsoft Corporation (EE. UU.), entre otros.

[7] Emiratos Árabes Unidos.

CONCENTRACIÓN DEL MERCADO DE CIBERSEGURIDAD – GLOBAL Y CHILE

Datos 2022



Fuente: elaboración propia a partir de datos de Mordor Intelligence.

3.2. El mercado de la ciberseguridad en Chile

A pesar de que América Latina y el Caribe tienen una tasa de penetración de acceso a Internet menor —74,63 % en enero de 2023 según datos de Statista—, Chile sobresale en la región con una alta penetración del 90,2 %, contando con 17,7 millones de usuarios permanentes en 2022. En la última década, el país ha experimentado un notable crecimiento, pasando de un 42 % en 2012 hasta la cifra actual. Sin embargo, este rápido aumento en la conectividad también ha conllevado un aumento significativo en los ciberataques debido a la falta de preparación ante estas amenazas.

En comparación con el resto de la región, la penetración de Internet ha seguido un proceso similar en América Latina y el Caribe, aunque en un nivel algo inferior. Según el Banco Mundial, en 2012 solo el 43 % de la población tenía acceso a Internet. Este masivo proceso de adopción ha convertido a los países latinoamericanos en objetivos frecuentes de ciberataques, destacando la figura de Brasil como segundo país del mundo con el mayor número de ataques registrados, según el mapa en tiempo real de amenazas de la compañía Kaspersky.

El mercado de ciberseguridad en Chile está experimentando un significativo crecimiento debido a la adopción masiva de Internet y el aumento de los ciberataques. En este contexto, se han generado numerosas oportunidades para actores tanto globales como nacionales, lo que ha contribuido al desarrollo y expansión del sector en el país.

3.2.1. Tamaño y estructura del sector

Según estimaciones de IDC, el mercado de ciberseguridad en Chile alcanzó un tamaño de 282 millones de USD en 2022, y se espera que experimente una tasa de crecimiento anual del 10,5 % hasta el año 2024. Asimismo, de acuerdo con las proyecciones de Mordor Intelligence, se anticipa que el mercado mantendrá un crecimiento constante en los próximos años, con una tasa de crecimiento medio anual compuesta del 9,8 % hasta el año 2028.

A pesar de la presencia de múltiples actores, el mercado chileno de ciberseguridad se considera moderadamente consolidado. Un número significativo de empresas compite en este sector; sin embargo, una parte importante del mercado está dominada por un grupo reducido de participantes, entre los cuales destacan Leonardo, AVG Technologies, Check Point Software Technologies Ltd., Cisco Systems Inc. y Dell Technologies Inc., entre otros.

Sin embargo, atendiendo a la cadena de valor del sector de ciberseguridad, se pueden encontrar actores importantes en los distintos eslabones de la misma. Aunque algunos agentes operan en varios segmentos, como fabricantes de *software* que venden tanto a minoristas como directamente a clientes finales y también ofrecen servicios de ciberseguridad. IBM es un ejemplo de compañía presente en los cinco eslabones. Telefónica y Entel, además de ser proveedores, también actúan como integradores y ofrecen servicios de consultoría. Por tanto, al clasificar estas empresas se ha tenido en cuenta su actividad principal o el segmento en el que destacan.

Fabricantes

En el análisis se contemplan tres tipos de fabricantes: *software*, *hardware* y mixtos. Las empresas líderes en el desarrollo de soluciones de ciberseguridad son corporaciones tecnológicas de alcance global, que no se limitan a operar en un país en particular. En cuanto a la fabricación de productos relacionados con la seguridad perimetral, destacan las compañías estadounidenses e israelíes, las cuales poseen una sólida posición en el mercado.

En el contexto de los fabricantes de ciberseguridad en Chile, destacan AVG, Check Point, Dell y Cisco, junto con menciones adicionales como Mcafee, RSA y Microsoft. A continuación, se presenta una tabla con los principales fabricantes:

PRINCIPALES FABRICANTES PRESENTES EN CHILE

Compañía	Descripción
AVG Technologies	Empresa tecnológica especializada en *software* de seguridad informática. Se dedica al desarrollo y distribución de soluciones antivirus, anti-*malware* y herramientas de protección en línea para usuarios y empresas. Sus productos abarcan desde antivirus básicos hasta suites de seguridad más completas, diseñadas para proteger dispositivos y redes contra amenazas cibernéticas (virus, *malware*, *ransomware*, *phishing*, entre otros tipos de ataques maliciosos).

Barracuda Networks Inc.	Empresa americana líder en el sector tecnológico, la cual ofrece soluciones altamente efectivas y rentables para abordar los principales desafíos de TI. Su enfoque se centra en tres mercados clave: - Seguridad del contenido: soluciones robustas para garantizar la seguridad de los datos y proteger el contenido en línea. Estas herramientas son fundamentales para prevenir amenazas cibernéticas, detectar *malware* y salvaguardar la integridad de la información en el entorno digital. - Redes y entrega de aplicaciones: soluciones avanzadas para optimizar el rendimiento de las redes y garantizar la entrega eficiente de aplicaciones en diversos entornos. Esto incluye herramientas de aceleración de aplicaciones, balanceo de carga y optimización de ancho de banda, lo que contribuye a una experiencia más fluida y una mayor eficiencia operativa. - Almacenamiento de datos, protección y recuperación ante desastres: soluciones de almacenamiento de datos altamente confiables y escalables, junto con capacidades integrales de protección y recuperación ante desastres. Estas herramientas garantizan la disponibilidad y la continuidad del negocio en caso de fallos o pérdidas de datos.
Check Point Software Technologies Ltd.	Empresa líder en soluciones de seguridad informática, fundada en Israel y con reconocimiento global. Se especializa en brindar protección a empresas y organizaciones de todos los tamaños mediante *firewalls* de próxima generación, sistemas de prevención de amenazas, protección de *endpoints* y soluciones de gestión unificada de amenazas (UTM). Su enfoque en la innovación tecnológica y la rápida respuesta a las amenazas cibernéticas le ha permitido establecer una sólida reputación en la industria de la ciberseguridad a nivel mundial.
Cisco Systems Inc.	Cisco Systems es una empresa estadounidense que se enfoca en proporcionar soluciones de ciberseguridad avanzadas. Se dedica a proteger redes, sistemas y datos de empresas y organizaciones en todo el mundo. Su amplia cartera de productos y servicios incluye *firewalls*, sistemas de prevención de intrusiones, soluciones de seguridad para *endpoints*, herramientas de análisis de amenazas y más. Cisco utiliza tecnologías de vanguardia, como aprendizaje automático y análisis de comportamiento, para detectar y mitigar amenazas cibernéticas en tiempo real. Además, la empresa ofrece servicios de asesoramiento, monitoreo y respuesta a incidentes para ayudar a sus clientes a mantenerse seguros frente a las crecientes y sofisticadas amenazas en el panorama digital actual.
Crowstrike	Compañía estadounidense especializada en ofrecer soluciones avanzadas de protección contra amenazas cibernéticas basadas en la nube. Su enfoque se centra en la detección y respuesta en tiempo real, utilizando inteligencia artificial y aprendizaje automático para identificar y mitigar rápidamente las amenazas. Además, proporciona servicios de monitoreo y asesoramiento para ayudar a sus clientes a mantenerse seguros frente a las sofisticadas y en constante evolución amenazas cibernéticas.
Dell Technologies Inc.	Dell, con sede en Estados Unidos, se enfoca en soluciones integrales de ciberseguridad para proteger a organizaciones y usuarios contra amenazas cibernéticas. Ofrece productos y servicios como *firewalls*, soluciones para *endpoints*, sistemas de prevención de intrusiones y análisis avanzado de amenazas. Con tecnología de detección temprana y aprendizaje automático, abordan vulnerabilidades en tiempo real y brindan servicios de asesoramiento y monitoreo para fortalecer la protección digital de sus clientes.
Fortinet	Fortinet es una empresa multinacional estadounidense con sede en Sunnyvale, California. Su principal enfoque es el desarrollo y comercialización de *software*, dispositivos y servicios de ciberseguridad. Entre sus productos destacan *firewalls*, antivirus, prevención de intrusiones y seguridad en dispositivos de usuario. Fortinet es especialmente conocida por su línea de dispositivos de seguridad FortiGate, los cuales integran numerosas funciones de ciberseguridad en una sola solución. Su amplia gama de productos y servicios ayuda a empresas y organizaciones a protegerse eficazmente contra las crecientes amenazas cibernéticas en el entorno digital actual.
Mcafee	Empresa líder en ciberseguridad, con sede en California y enfocada en proteger tanto a individuos como a empresas de amenazas cibernéticas. Su amplia oferta de soluciones abarca desde antivirus y protección contra *malware* hasta *firewalls* y seguridad para *endpoints*. Con un enfoque en la innovación tecnológica y análisis de amenazas en tiempo real, Mcafee se dedica a proporcionar una sólida protección en el entorno digital actual, asistiendo a sus clientes para mantenerse seguros y resguardados contra las continuas y complejas vulnerabilidades cibernéticas.

Microsoft	La multinacional estadounidense Microsoft se dedica a ofrecer soluciones integrales de ciberseguridad para proteger a individuos y organizaciones contra las amenazas cibernéticas. Su enfoque incluye el desarrollo de *software* de seguridad, como Windows Defender Antivirus, y herramientas de detección y prevención de amenazas en tiempo real, como Microsoft Defender for Endpoint. Además, proporciona servicios de seguridad en la nube, como Microsoft Azure Security Center, para proteger los datos y aplicaciones en entornos en la nube. Microsoft se esfuerza por garantizar la seguridad y la confianza de sus clientes en el uso de sus productos y servicios digitales.
RSA	Con sede en Bedford, Massachusetts, Estados Unidos, es reconocida por desarrollar soluciones de seguridad y cifrado en el ámbito de la tecnología informática. Su enfoque se centra en proporcionar servicios y productos para proteger los sistemas y datos de empresas y organizaciones contra amenazas cibernéticas y ataques maliciosos. RSA también destaca por ofrecer soluciones de autenticación y gestión de identidad, ayudando a garantizar la integridad y confidencialidad de la información en el entorno digital actual.

Fuente: elaboración propia a partir de datos de las webs corporativas de las compañías.

Distribuidores

En el mercado chileno, los distribuidores de ciberseguridad desempeñan un papel esencial al conectar a proveedores de soluciones de seguridad cibernética con empresas que buscan resguardar sus activos digitales. Estos distribuidores ofrecen una gama diversa de productos, desde *firewalls* hasta sistemas de cifrado, y servicios que incluyen asesoramiento técnico, capacitación y soporte especializado. En un entorno de una constante y creciente adopción de tecnologías digitales, su figura es crucial para ayudar a las empresas a evaluar sus necesidades, elegir soluciones adecuadas y asegurar una implementación exitosa de las mismas. Su experiencia en las últimas tendencias de ciberamenazas y soluciones de seguridad resulta fundamental para proteger a los clientes en un entorno digital en evolución constante.

A continuación, se presenta una tabla con los distribuidores más relevantes del mercado de ciberseguridad chileno, los cuales se caracterizan por ser grandes empresas con presencia internacional:

PRINCIPALES DISTRIBUIDORES EN CHILE

Compañía	Descripción
Adistec	Fundada en 2002 en Miami, Adistec es una empresa líder en distribución tecnológica y ciberseguridad con un enfoque destacado en América Latina y el Caribe. Actuando como puente entre proveedores tecnológicos líderes y empresas, Adistec proporciona soluciones avanzadas en áreas como seguridad cibernética y redes. Su enfoque va más allá de la distribución convencional, ya que se destaca por ofrecer programas de capacitación y certificación para socios y clientes, impulsando un mayor conocimiento técnico.
CPNNet	Distribuidor especializado en soluciones de ciberseguridad, con más de 12 años de experiencia en el respaldo a sus *Partners*. Ofrece herramientas líderes e innovadoras en ciberseguridad para abordar las demandas cambiantes de los clientes, incluyendo Seguridad de aplicaciones, Pentesting, Gestión de Vulnerabilidades y más. CPNNet brinda apoyo en ventas, capacitaciones comerciales y potencia oportunidades mediante ofertas competitivas. Además, proporciona asesoría completa y soporte gracias a su equipo especializado en las soluciones que representa. Con su enfoque en la excelencia y la colaboración, CPNNet es un socio confiable para soluciones de ciberseguridad.

INGRAM MICRO	Ingram Micro es una renombrada empresa global de distribución y servicios de tecnología. Fundada en 1979, se destaca como un líder en conectar fabricantes de tecnología con revendedores y usuarios finales en todo el mundo. Ofreciendo una amplia gama de productos y servicios, incluyendo soluciones de ciberseguridad, *cloud* y logística, Ingram Micro facilita la entrega eficiente de tecnología a través de su red de socios. Con presencia en numerosos países, la empresa desempeña un papel crucial en la distribución y adopción de soluciones tecnológicas a nivel global.
Licencias *Online*	Empresa especializada en la distribución y gestión de *software* y servicios en línea. Fundada en 2001, ofrece soluciones tecnológicas a través de una red global de *partners* y clientes. Centrándose en la entrega eficiente de licencias de *software*, servicios en la nube y seguridad digital, Licencias *Online* simplifica la adquisición y administración de tecnología. Su enfoque en la innovación y la experiencia técnica la convierte en un actor clave en el mercado de soluciones digitales y en la facilitación de tecnología en múltiples sectores.
Nexsys	Nexsys es un líder en soluciones tecnológicas y distribución en América Latina, con un enfoque especial en ofrecer soluciones de *software*, *hardware* y servicios a través de su red de canales. Con una presencia establecida en varios países, Nexsys destaca por su capacidad para conectar fabricantes líderes con *reseller*s y revendedores en la región. Su oferta abarca una amplia gama de productos, desde *software* empresarial hasta soluciones de seguridad cibernética y dispositivos electrónicos. La compañía destaca por su compromiso en ofrecer valor agregado a sus *partners*, brindando soporte técnico, capacitación y herramientas para impulsar el éxito de sus clientes.
Micronet Chile	Distribuidor mayorista con más de 35 años de experiencia en soluciones de ciberseguridad y protección de datos, forma parte del Grupo Micronet. Conecta fabricantes líderes en seguridad, reconocidos en la industria, y ofrece atención personalizada y eficiente gracias a un equipo de más de 100 profesionales en áreas comerciales, técnicas y logísticas. Su enfoque se centra en aumentar la rentabilidad de los canales de *Partners* y establecer alianzas de colaboración, con presencia en múltiples países latinoamericanos, buscando la excelencia financiera y técnica.
ProWeb	Multinacional especializada en soluciones integrales de seguridad, networking y virtualización, operando mediante integradores y *reseller*s. La compañía, fundada en 1995 en Santiago, comenzó enfocada en seguridad y networking para Internet/Intranet. Representa y distribuye tecnología líder e innovadora en su región, brindando un apoyo integral desde la preventa hasta la postventa, proporcionando capacitación, equipamiento y herramientas para sus proyectos.
Westcon	Empresa global de distribución tecnológica, especializada en soluciones de networking, seguridad y comunicaciones. Fundada en 1985 en Estados Unidos, se conforma como un líder mundial en conectar a los principales fabricantes en tecnología con socios y revendedores en todo el mundo. Westcon se centra en brindar productos y servicios de calidad en áreas clave de tecnología, apoyando la implementación y adopción de soluciones innovadoras.

Fuente: elaboración propia a partir de datos de las webs corporativas de las compañías.

Servicios

Dentro del eslabón de servicios se pueden encontrar tres tipos de compañías en función del servicio que ofrecen. En primer lugar, se encuentran las **consultoras de ciberseguridad**, las cuales han destacado en Chile por su enfoque experto y su contribución en la protección de datos y sistemas críticos. Estas firmas no solo brindan soluciones de seguridad de vanguardia, sino que también desempeñan un papel crucial en la promoción de la conciencia y la preparación ante las crecientes amenazas cibernéticas.

A continuación, se presentan algunas de las consultoras de ciberseguridad más importantes en el mercado chileno, cuya experiencia y enfoque siguen siendo vitales en el sector.

PRINCIPALES CONSULTORAS DE CIBERSEGURIDAD EN CHILE

Compañía	Descripción
Accenture	Accenture, influyente firma global de consultoría y servicios, abarca diversas industrias. Con su profundo conocimiento en tecnología y transformación digital, también se destaca en ciberseguridad. Ofrece soluciones innovadoras para proteger activos digitales y datos sensibles, mientras guía a las organizaciones a navegar por desafíos cibernéticos y a aprovechar nuevas oportunidades en un entorno empresarial en constante evolución.
Base4 Security	Empresa chilena especializada en ciberseguridad que ofrece servicios de evaluación de riesgos y pruebas de penetración. Operando tanto a nivel nacional como internacional, su enfoque personalizado y experiencia diversa permiten a las organizaciones proteger sus activos digitales y mitigar amenazas cibernéticas
IT Sec	Fundada en 2010 y con sede en Santiago, IT SEC es un referente en ciberseguridad en Chile. Su especialización abarca pruebas de penetración, evaluación de riesgos y consultoría de seguridad. Operando en diversos sectores, IT SEC protege activos digitales y mitiga amenazas cibernéticas, brindando soluciones confiables en un entorno tecnológico en constante cambio.
Aiuken Cybersecurity	Firma internacional de ciberseguridad de origen español. La compañía está especializada en MDRS gestionados, integración de soluciones de seguridad y servicios Cloud de alto valor añadido, lo que le ha conducido a operar en 7 países.
DREAMLAB	Dreamlab Technologies, de origen suizo, es un referente en ciberseguridad y análisis de datos. Especializada en soluciones avanzadas para la protección de activos digitales y la optimización de datos, su enfoque innovador los distingue. Desde Suiza hasta el mundo, lideran en un entorno tecnológico en constante cambio, brindando seguridad y eficiencia a empresas y organizaciones.

Fuente: elaboración propia a partir de datos de las webs corporativas de las compañías.

En el dinámico panorama de la ciberseguridad en Chile, varios **integradores** han emergido como pilares fundamentales para proteger los activos digitales en un entorno cada vez más amenazante. A medida que las amenazas cibernéticas evolucionan, estos integradores juegan un papel crucial al diseñar y ejecutar estrategias que resguardan la integridad de la información en un mundo digital en constante cambio. A continuación, se presentan algunos de los principales integradores de ciberseguridad en el mercado chileno:

PRINCIPALES INTEGRADORES EN CHILE

Compañía	Descripción
Deloitte	Firma de consultoría global que ofrece servicios integrales de ciberseguridad, incluyendo evaluaciones de riesgos, pruebas de penetración, respuesta a incidentes y consultoría estratégica. Ayudan a las organizaciones a desarrollar y mejorar sus estrategias de seguridad cibernética.
EY	Empresa multinacional que brinda servicios de ciberseguridad que van desde la gestión de riesgos hasta la implementación de soluciones tecnológicas. Ayudan a las organizaciones a proteger sus activos digitales y cumplir con las regulaciones de seguridad aplicables.
PwC	Firma global de consultoría que abarca diversos sectores, incluyendo la ciberseguridad. Con experiencia en evaluaciones de riesgos, cumplimiento normativo y gestión de incidentes, PwC ofrece soluciones integrales para proteger activos digitales y datos sensibles, ayudando a las organizaciones a enfrentar los desafíos cibernéticos actuales.
KPMG	Firma de renombre mundial que se distingue por su enfoque en ciberseguridad. Proporciona servicios de evaluación de riesgos, estrategias y respuesta a incidentes, salvaguardando

	activos digitales y datos en el entorno cibernético actual. Su experiencia brinda a las organizaciones protección vital en un mundo interconectado y dinámico.
WatchGuard Technologies	WatchGuard Technologies es un destacado proveedor de soluciones de seguridad de red. Ofrecen *firewall*, VPN y protección de *endpoints*. Su enfoque abarca desde pequeñas empresas hasta grandes corporaciones, protegiendo infraestructuras digitales con tecnologías avanzadas y servicios de seguridad confiables.

Fuente: elaboración propia a partir de datos de las webs corporativas de las compañías.

En el complejo escenario de la ciberseguridad en Chile, la protección efectiva de los activos digitales requiere no solo tecnología avanzada, sino también una gestión constante y especializada. En este contexto, los **Proveedores de Servicios Gestionados de Seguridad (MSSP)** han surgido como figuras clave. Estas empresas no solo ofrecen soluciones de seguridad de primer nivel, sino que también se encargan de supervisar y gestionar proactivamente las amenazas cibernéticas. En este recorrido por el panorama de la ciberseguridad chilena, se identifican algunos de los principales MSSP que lideran el camino al brindar una protección integral y continua:

PRINCIPALES MSSP EN CHILE

Compañía	Descripción
Entel Ocean	Entel Ocean, la división de ciberseguridad de Grupo Entel en Chile, es un MSSP que brinda monitoreo y respuesta a amenazas cibernéticas. Especializados en telecomunicaciones, ofrecen soluciones personalizadas para detectar y mitigar actividades maliciosas, asegurando la protección de activos digitales. Su enfoque proactivo y experiencia los convierte en una opción confiable para la ciberseguridad empresarial.
Logicalis	Logicalis es una empresa global de tecnología y servicios que ofrece soluciones de ciberseguridad como Proveedor de Servicios Gestionados de Seguridad (MSSP). Su enfoque se centra en proporcionar a las organizaciones soluciones integrales para enfrentar los desafíos cibernéticos en constante evolución. Como MSSP, Logicalis ofrece servicios de monitoreo, detección y respuesta a amenazas cibernéticas, lo que ayuda a las empresas a proteger sus activos digitales y a mitigar riesgos.
GTD	GTD es una empresa chilena líder en telecomunicaciones y tecnología. Ofrecen soluciones integrales en servicios de comunicación, TI y ciberseguridad. Con su experiencia diversificada, GTD destaca como un proveedor confiable de servicios tecnológicos para empresas y organizaciones en Chile y la región.
Telsur	Telsur, destacada empresa de telecomunicaciones en Chile se especializa en brindar soluciones de ciberseguridad. Con su experiencia en el ámbito tecnológico, ofrece servicios y soluciones que van desde el monitoreo de amenazas hasta la implementación de estrategias de protección de datos, garantizando la seguridad de las operaciones digitales en un entorno desafiante.
Baufest	Baufest es una empresa global de consultoría y tecnología que se destaca por sus servicios de ciberseguridad. Ofrecen soluciones personalizadas, evaluaciones de riesgos y desarrollo de *software* seguro para proteger activos digitales.

Fuente: elaboración propia a partir de datos de las webs corporativas de las compañías.

4. Demanda

En los últimos años, la ciberseguridad se ha convertido en una de las principales preocupaciones en todos los estratos de la sociedad debido al continuo proceso de digitalización. Este fenómeno, que conlleva un aumento constante de riesgos y amenazas cibernéticas, ha motivado un crecimiento proyectado del 13,2 % en el gasto mundial en ciberseguridad para el año 2023, según el último informe *Global Cybersecurity Spending* de Canalys.

El panorama de amenazas evoluciona constantemente, y durante este año, las organizaciones se enfrentan a una presión adicional para fortalecer y expandir sus defensas de ciberseguridad. Aunque el *ransomware* persiste como la amenaza más destacada en términos operativos, financieros y de marca, la introducción y explotación de modelos generativos de IA, como ChatGPT, añaden una capa adicional de riesgo debido a la automatización en la creación de código malicioso.

El informe de *Tendencias en ciberataques de Check Point Research (CPR) 2022* subraya un aumento alarmante del 38 %, atribuido a bandas de *hackers* y *ransomware* más ágiles, enfocadas en aprovechar herramientas de colaboración en entornos de trabajo remoto. Esta expansión global de los ciberataques se ha visto impulsada por el interés de los hackers en organizaciones del sector sanitario y en instituciones educativas que migraron al aprendizaje en línea tras la pandemia.

4.1. Factores que afectan a la demanda

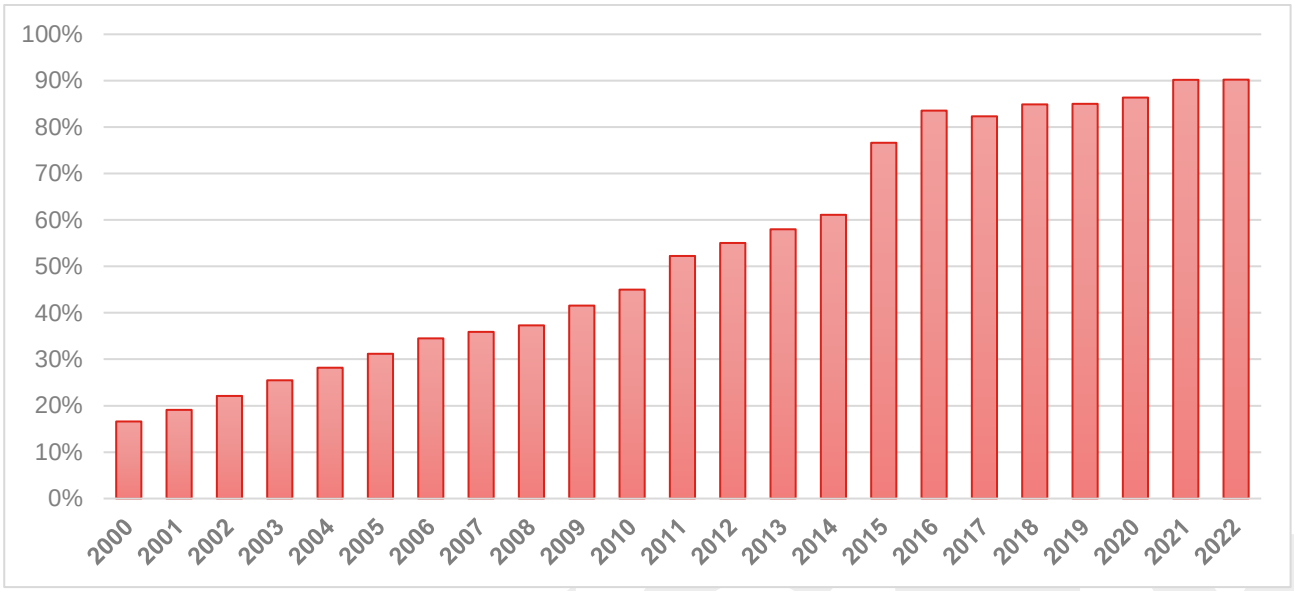
4.1.1. Uso de Internet

En la última década, Chile ha experimentado un significativo avance en el ámbito de la tecnología y las comunicaciones, siendo testigo de una rápida y constante penetración de Internet en todos los sectores de la sociedad. Este fenómeno ha transformado no solo la forma en que los chilenos se comunican, sino también la manera en que trabajan, estudian y acceden a la información.

Con un crecimiento sostenido en la infraestructura de telecomunicaciones, incluyendo la expansión de redes de banda ancha y la mejora de la conectividad móvil, Chile se ha posicionado como uno de los países líderes en América Latina en términos de acceso a Internet. Este avance tecnológico ha contribuido significativamente al desarrollo económico y social del país, facilitando la participación de la población en la era digital.

EVOLUCIÓN DE LA PENETRACIÓN DE INTERNET EN CHILE

Porcentaje de la población



Fuente: Statista.

En el gráfico anterior se puede observar cómo ha evolucionado la penetración de Internet entre la población chilena en las últimas décadas. En 2022 el grado de penetración fue del 90,2 %, situando a Chile como el país con el mayor índice en la región sudamericana.

4.1.2. Comercio electrónico

Chile, con más de 19 millones de habitantes, destaca como el quinto mercado de comercio electrónico más grande de Latinoamérica, liderando en ventas per cápita según un informe de Visa. Aunque el crecimiento previo se atribuyó a la pandemia y restricciones físicas, en 2022 el sector experimentó su primera caída histórica, con una disminución del 8 % en las ventas, alcanzando los 10,4 miles de millones de USD, según la Cámara de Comercio de Santiago.

Este descenso se atribuye a la disminución de ingresos, altos niveles inflacionarios, tasas de interés y la comparación con el excepcional 2021. La penetración del comercio electrónico en las ventas generales disminuyó del 16 % al 13 %, agravada por la reactivación completa del comercio físico. A pesar de la caída en las ventas de bienes en línea, los servicios turísticos, especialmente los viajes, experimentaron un sólido crecimiento del 91 %.

VENTAS DE COMERCIO ELECTRÓNICO B2C

Millones de USD

	2018	2019	2020	2021	2022	2023
Ventas B2C	5.200	6.079	9.423	11.967	10.453	10.976[8]

Fuente: Cámara de Comercio de Santiago (CCS).

Se espera que en 2023 el comercio electrónico se recupere, alcanzando cerca de 11.000 millones de USD, con un aumento del 5 % respecto al año anterior. Categorías como vestuario, calzado, alimentación y tecnología son las más populares entre los compradores chilenos en línea.

A pesar de los desafíos actuales, los expertos ven la actual coyuntura como un estímulo para que los emprendedores del sector impulsen la innovación y la cercanía con los consumidores, marcando pautas para el futuro de la economía digital en Chile.

4.1.3. Teletrabajo

En los últimos años, el teletrabajo en Chile ha experimentado una transformación notable, pasando de un crecimiento progresivo a una adopción masiva durante la pandemia de COVID-19 en 2020. La respuesta a las medidas de confinamiento llevó a muchas empresas a reconocer los beneficios del teletrabajo, lo que resultó en la consolidación de esta modalidad como una opción permanente en el paisaje laboral chileno. La pandemia no solo aceleró la adopción del teletrabajo, sino que también llevó a muchas empresas a repensar sus políticas laborales, promoviendo la flexibilidad y la combinación de trabajo presencial y remoto.

En 2022 se ha producido una disminución en los niveles de teletrabajo, marcando un retorno progresivo a los espacios laborales físicos. Según un estudio de la CCS basado en encuestas trimestrales a aproximadamente 950 personas, el formato exclusivamente presencial ha alcanzado su nivel más alto desde el inicio de la pandemia, llegando al 75 % en este último trimestre del año, en comparación con un 50 % en el segundo trimestre de 2021.

Aunque la presencialidad ha experimentado un aumento significativo, un porcentaje notable de trabajadores —alrededor del 26 %— sigue participando en alguna forma de teletrabajo (total o parcial), manteniendo cifras similares al trimestre anterior. Aquellos que trabajan totalmente de forma remota se estabilizan en torno al 10 %, mientras que la modalidad mixta retrocede levemente a un 15 %. Este cambio en la dinámica laboral plantea desafíos, ya que la persistencia de un porcentaje considerable de teletrabajadores podría aumentar la exposición a posibles problemas de ciberseguridad para las empresas en el futuro.

[8] Este dato es una proyección de la CCS.

4.1.4. Ciberdelincuencia

Según un informe de Sophos, el 65 % de las organizaciones chilenas experimentaron ataques de *ransomware* en el último año, con un aumento del 33 % respecto al período anterior, lo que conllevó coste de rescate superior a los 500.000 USD. Este fenómeno afectó no solo la seguridad de los datos, sino también a organizaciones críticas para la infraestructura del país.

El informe revela que las debilidades en las capacidades de "Operaciones de Ciberseguridad" son una causa importante del éxito de los ataques de *ransomware* en Chile. Numerosas empresas enfrentan problemas al revisar *logs*, correlacionar información de diferentes controles de ciberseguridad, integrar tecnologías, automatizar respuestas y comprender las tácticas utilizadas por los cibercriminales.

Este escenario evidencia una industria de cibercrimen avanzada y conectada que aprovecha las limitaciones de las empresas chilenas en ciberseguridad, resultando en un aumento en la cantidad y complejidad de los ataques. Este hecho afecta significativamente las operaciones y los ingresos de las víctimas, llevando a mayores costes de rescate y recuperación. Por tanto, es esencial mejorar la capacidad de las operaciones de ciberseguridad, centrándose en la rápida detección y respuesta, al tiempo que los cuerpos legislativos, judiciales y policiales colaboran de forma conjunta para eliminar este problema.

4.2. Principales demandantes de servicios

Los principales clientes de ciberseguridad del mercado chileno se pueden clasificar en:

- **Administración Pública:** demanda soluciones integrales de seguridad cibernética que abarquen aspectos clave como ciberinteligencia y ciberdefensa. Estas soluciones se requieren para proteger la integridad y confidencialidad de la información crítica. La adquisición de servicios en este sector generalmente se lleva a cabo mediante procesos transparentes y competitivos como licitaciones o contrataciones directas.

- **Empresas y operadores críticos:** requieren una gama diversa de soluciones en ciberseguridad, desde auditorías técnicas y gestión de incidentes hasta seguridad integral en la nube y soluciones industriales altamente especializadas. Este grupo abarca sectores cruciales como bancos, hospitales y clínicas privadas, empresas de servicios como aerolíneas y servicios públicos, bufetes de abogados y empresas multinacionales. La variedad de necesidades dentro de este segmento destaca la importancia de ofrecer soluciones adaptadas a industrias altamente especializadas y sensibles a la seguridad.

- **Mipymes y particulares:** buscan soluciones más simples en ciberseguridad, como herramientas especializadas o paquetes antivirus. La distribución y provisión de servicios para

este segmento generalmente se realiza a través de la concesión de licencias o la entrega de productos físicos, destacando la necesidad de enfoques accesibles y efectivos para protegerse contra amenazas cibernéticas.

Las necesidades de ciberseguridad en la **Administración Pública** chilena han alcanzado una urgencia crítica, evidenciada por eventos significativos durante el año 2022. El sector público sufrió una serie de ciberataques importantes, destacando el hackeo al Estado Mayor Conjunto, que resultó en la exposición de miles de documentos clasificados y secretos de la seguridad nacional chilena. Además, el Poder Judicial fue blanco de un ataque en septiembre, afectando a la Corte de Apelaciones de Santiago, y el Sernac se enfrentó a un episodio donde sus sistemas estuvieron secuestrados por *hackers* durante casi dos semanas.

Estos incidentes, revelados en el *Informe Anual 2022* de Nivel4[9], reflejan la vulnerabilidad crítica a la que se vieron expuestas diversas instituciones del Estado chileno. Según el informe, que clasifica las vulnerabilidades en las distintas industrias del país, el sector gubernamental se enfrenta a un panorama complejo. Entre las 12 entidades gubernamentales examinadas, el 6,18 % de las vulnerabilidades detectadas fueron catalogadas como críticas, subrayando la necesidad de medidas urgentes para abordar estas debilidades. Además, en el nivel de vulnerabilidad considerado como "alto", el Gobierno concentró un 13,48 % de las amenazas detectadas, posicionándose como el tercer sector con mayor exposición, después de la industria de seguros y de salud. Estos datos resaltan la necesidad de fortalecer las capacidades de ciberseguridad en la Administración Pública para salvaguardar la integridad de la información y proteger los sistemas vitales del Estado.

En el **sector privado** chileno, se ha evidenciado un notable aumento en la demanda de servicios de ciberseguridad debido al incremento de las amenazas cibernéticas. Entre las industrias afectadas, el **comercio minorista y mayorista** ha experimentado un cambio significativo al pasar de ser el segundo sector más atacado a convertirse en el más vulnerable en 2022 —representando el 28 % de los casos— según el informe *X-Force Threat Intelligence Index* 2022 de IBM Security. Este hecho subraya la urgente necesidad de implementar soluciones efectivas de ciberseguridad para proteger la integridad digital de estas industrias.

La identificación del sector minorista y mayorista como el blanco principal de ataques cibernéticos en Chile resalta la vulnerabilidad particular de estas áreas ante las crecientes amenazas. Este cambio se produjo en detrimento de otros sectores como **finanzas y seguros**, que ocuparon el segundo lugar con el 24 % de los casos, seguido de **energía y manufactura**, ambos con un 20 %. Ante este panorama, las empresas chilenas, independientemente de su sector, reconocen la necesidad de fortalecer sus medidas de ciberseguridad, adoptando enfoques proactivos para mitigar los riesgos y proteger la información vital.

[9] Consultora chilena de ciberseguridad especializada en el denominado *ethical hacking*, o hackeo ético, práctica que consiste en realizar testeos voluntarios de los sistemas de seguridad cibernética para detectar áreas de mejora.

Las **Micro, Pequeñas y Medianas Empresas** (mipymes) en Chile son fundamentales para la economía, representando el 98,6 % de las empresas, con un total de 235.569, y concentrando el 65,3 % de los empleos formales. Estas empresas se enfrentan a un riesgo significativo en el ámbito cibernético, ya que un tercio de los ataques globales se dirige a este tipo de compañías. Además, el 61 % de las organizaciones atacadas no logran sobrevivir a las consecuencias de estos ciberataques como consecuencia de su menor tamaño y recursos. Estos hechos subrayan la vulnerabilidad crítica de las pymes ante las amenazas cibernéticas y resaltan la necesidad de implementar medidas efectivas de ciberseguridad para proteger tanto la integridad de estas empresas como la estabilidad económica en su conjunto.

4.2.1. Sector público

En el contexto chileno, la contratación y acceso a proyectos de consultoría o ciberseguridad con entidades públicas se realiza mediante procesos de licitación. La plataforma central para acceder a oportunidades de licitación pública es www.mercadopublico.cl. De hecho, solo en el último año se han registrado 57 licitaciones públicas relacionadas con el sector de la ciberseguridad en este portal.

Actualmente, el Gobierno de Chile está compuesto por 24 ministerios, que podrían ser potenciales clientes de las diversas empresas de ciberseguridad.

- Ministerio del Interior y Seguridad Pública
- Ministerio de Relaciones Exteriores
- Ministerio de Defensa Nacional
- Ministerio de Hacienda
- Ministerio Secretaría General de la Presidencia
- Ministerio Secretaría General de Gobierno
- Ministerio de Economía, Fomento y Turismo
- Ministerio de Desarrollo Social y Familia
- Ministerio de Educación
- Ministerio de Justicia y Derechos Humanos
- Ministerio del Trabajo y Previsión Social
- Ministerio de Obras Públicas
- Ministerio de Salud
- Ministerio de Vivienda y Urbanismo
- Ministerio de Agricultura
- Ministerio de Minería
- Ministerio de Transportes y Telecomunicaciones
- Ministerio de Bienes Nacionales
- Ministerio de Energía
- Ministerio del Medio Ambiente
- Ministerio del Deporte

- Ministerio de la Mujer y la Equidad de Género
- Ministerio de las Culturas, las Artes y el Patrimonio
- Ministerio de Ciencia, Tecnología, Conocimiento e Innovación

La estructura de licitación pública abarca no solo a nivel nacional, sino también en las **16 regiones** con sus respectivas municipalidades, así como en las **168 instituciones** encargadas de ofrecer servicios públicos en el territorio. Esta extensa estructura pública conforma una amplia oportunidad para las empresas especializadas en ciberseguridad interesadas en participar en proyectos y consultorías con entidades gubernamentales en Chile.

El sector público chileno se enfrenta a desafíos sustanciales en ciberseguridad, con múltiples vulnerabilidades y hackeos en instituciones clave, como el Poder Judicial, el Servicio Nacional del Consumidor y el Estado Mayor de la Defensa Nacional. Estas brechas han expuesto al país a riesgos de extorsiones y filtraciones de información sensible, generando inquietudes en cuanto a la seguridad nacional.

Para hacer frente a estos problemas, se publicó en el Diario Oficial el 20 de junio de 2022 la Ley N.º 21459, que busca tipificar conductas y hechos como delitos informáticos. Además, en marzo de 2022, durante la administración del expresidente Sebastián Piñera, se presentó el proyecto de ley (*Boletín* N.º 14.847-06) con el propósito de establecer un marco regulatorio sobre ciberseguridad e infraestructura crítica de la información.

En el ámbito de la ciberseguridad en Chile, tanto diversas instituciones públicas como el país en su totalidad han sido evaluados en términos de madurez por la Organización de Estados Americanos (OEA) en los años 2016 y 2020. Según el Modelo de Madurez de Capacidades de Ciberseguridad de Naciones (CMM) de la Universidad de Oxford, Chile se sitúa entre los niveles 2 y 3 de los 5 niveles considerados. Esta evaluación indica que el país se encuentra en un nivel de madurez "intermedio" en ciberseguridad, a pesar de contar con una infraestructura digital considerable. Este desequilibrio respecto al nivel de digitalización del país subraya la urgencia de fortalecer las medidas de seguridad digital del país, no solo en el ámbito público, sino también en el privado.

4.2.2. Sector privado e infraestructuras críticas

En el contexto de economías en desarrollo, la expansión de las actividades industriales hacia la Industria 4.0 es esencial para el desarrollo. Sin embargo, este avance, acelerado por la pandemia, ha ampliado la exposición de las empresas a ciberataques, especialmente en sectores cruciales como energía, telecomunicaciones, agua, salud, servicios financieros, seguridad pública, transporte, administración pública, protección civil y defensa.

Es crucial salvaguardar estas infraestructuras críticas, como establece la Política Nacional de Ciberseguridad (PNCS), que no solo busca alinearlas con un enfoque de gestión de riesgos, sino también implementar medidas específicas para la ciberseguridad industrial. Entre estas medidas se

incluyen la creación de un Sistema de Gestión de Riesgos, un programa para fomentar una cultura de ciberseguridad, medidas de ciberprotección para instalaciones industriales y el establecimiento de objetivos para garantizar la resiliencia y continuidad de los sistemas operativos. Este enfoque integral no solo impulsa la transformación digital de la industria, sino que también mitiga los riesgos asociados a la creciente exposición cibernética de las infraestructuras críticas.

La Oficina del Centro de Ciberseguridad Industrial (CCI) en Chile señala un notable crecimiento en la conciencia sobre ciberseguridad en las organizaciones industriales. El país, respaldado por organismos gubernamentales como el Ministerio de Defensa, el Ministerio del Interior y el EMCO (Estado Mayor Conjunto), trabaja activamente para establecer un marco legal sólido, asegurando la integración progresiva de la ciberseguridad industrial, especialmente en infraestructuras críticas. Destacan leyes como el Decreto Supremo N.º 1299, que rige el manejo de la delincuencia cibernética, la Ley N.º 19.223, que incorpora delitos informáticos al Código Penal, y la Ley N.º 19.628, que aborda la privacidad y protección de datos.

En cuanto a las medidas implementadas por las organizaciones chilenas para proteger los sistemas de automatización industrial, los Coordinadores de CCI en Chile destacan la aplicación de consultoría y asesoría en ciberseguridad industrial, hacking ético, auditorías de seguridad internas y externas, *whitelisting* y antivirus. Este enfoque integral tiene como objetivo fortalecer la seguridad cibernética y resguardar las infraestructuras críticas en el contexto de la Industria 4.0.

Los Coordinadores del CCI en Chile describen la situación del país en cuanto a ciberseguridad industrial mediante el siguiente análisis DAFO:

DAFO CIBERSEGURIDAD INDUSTRIAL EN CHILE

Debilidades	Amenazas	Fortalezas	Oportunidades
Carencia de: - Certificaciones de tecnología OT, procesos y profesionales. - Normativa específica. - Promoción. - Soluciones y servicios a medida. - CERT específicos.	- Aplicación de medidas sin criterio. - Desarrollo industrial sin requisitos de seguridad. - Legislación lenta. - Escasez de profesionales y herramientas de gestión de riesgos específicos.	✓ Impulso desde el Estado. ✓ Existencia proyectos de innovación. ✓ Concienciación (especialmente en infra. críticas).	✓ Incremento demanda para Industria 4.0 el IoT. ✓ Conocimiento *Smart Grid.* ✓ Posicionamiento estratégico.

Fuente: CCI Chile.

4.2.3. Mipymes y particulares

En el contexto de la ciberseguridad en Chile, las mipymes[10] se enfrentan a desafíos significativos que han sido evidenciados por estudios y eventos específicos. Según una encuesta realizada por Microsoft en 2021, más del 50 % de las mipymes chilenas fueron víctimas de ataques cibernéticos. Este dato revela una vulnerabilidad notable en el tejido empresarial de menor tamaño, subrayando la necesidad urgente de medidas de protección.

Un hallazgo aún más preocupante es que el 62 % de estas admitieron carecer de las herramientas técnicas adecuadas para hacer frente a los problemas derivados de los ciberataques. Este déficit tecnológico evidencia una brecha en la infraestructura de seguridad digital, dejando a estas empresas expuestas a diversas amenazas cibernéticas.

La preferencia de los ciberdelincuentes por atacar a las pymes no se centra únicamente en motivaciones financieras. La facilidad para penetrar en los sistemas de estas empresas las convierte en blancos atractivos. Este riesgo, por ende, no solo se traduce en pérdidas económicas, sino también en posibles interrupciones operativas que pueden afectar la continuidad del negocio.

En respuesta a la vulnerabilidad de las pymes chilenas frente a amenazas cibernéticas, el Ministerio de Economía, en colaboración con Microsoft, reconoció la necesidad de fortalecer la seguridad digital de estas empresas. Durante la Semana de la pyme en 2022, se llevó a cabo una actividad específica centrada en ciberseguridad en el Centro de Negocios Sercotec Santiago. Se anunció la disponibilidad de 10.000 certificaciones gratuitas en ciberseguridad por parte de Microsoft, dirigidas a abordar la carencia de preparación técnica en las pymes y fortalecer sus defensas contra amenazas cibernéticas.

El compromiso conjunto del Ministerio de Economía y Microsoft subraya la importancia de la capacitación en ciberseguridad para emprendedores, destacando el vínculo entre grandes empresas y pymes en beneficio de la economía en general. Este enfoque reconoce que la seguridad cibernética es esencial para el desarrollo sostenible de las empresas más pequeñas. En última instancia, la iniciativa busca elevar la conciencia y capacidad de las pymes, abordando la problemática que afecta la seguridad de la información y la continuidad de los negocios en el entorno empresarial chileno.

[10] Micro, pequeñas y medianas empresas.

5. Precios

En el mercado de ciberseguridad en Chile, la diversidad de productos y servicios se traduce en variaciones de precios influenciadas por la naturaleza del producto y el perfil del comprador. En productos globalizados, como infraestructuras de *hardware* y soluciones de *software*, los precios tienden a ser homogéneos a nivel mundial, siendo particularmente evidente en soluciones básicas como antivirus o cortafuegos.

En servicios de consultoría de ciberseguridad, el componente de mano de obra es un factor crítico en el coste total, siendo más pronunciado en entornos con escasez de profesionales cualificados. La adaptabilidad de los precios según los requisitos técnicos específicos refleja la naturaleza personalizada de estas soluciones.

En lo que respecta al perfil de los clientes, se anticipa que aquellos que liderarán las inversiones en ciberseguridad en los próximos años serán:

- **Grandes empresas**
- **Administración Pública**
- **Ecosistema de las *startups***

En el contexto de las grandes empresas, sus necesidades específicas pueden conferirles un mayor poder de negociación al establecer los precios de las soluciones de ciberseguridad. Dado que ofrecer una solución integral para todas las amenazas es impracticable, la inversión de estas empresas dependerá del nivel de riesgo que estén dispuestas a asumir, así como de su propio análisis de coste/beneficio.

La posibilidad de sufrir filtraciones de datos que amenacen la seguridad nacional o revelen información sensible de gobiernos e instituciones públicas como consecuencia de ataques cibernéticos motiva a los organismos gubernamentales a incrementar su disposición para invertir recursos adicionales en ciberseguridad.

En lo que respecta a las micro, pequeñas y medianas empresas (mipymes) y a los usuarios particulares, se estima que su demanda se concentrará en soluciones de ciberseguridad básicas, como paquetes de antivirus o cortafuegos. Dado que la probabilidad de enfrentar amenazas significativas es relativamente baja, más allá de los habituales *softwares* espías y virus informáticos comunes, el precio se erigirá como uno de los factores más determinantes en sus decisiones de compra. En consecuencia, ofrecer un precio competitivo se convierte en un aspecto fundamental para este segmento de clientes.

6. Percepción del producto español

En el ámbito de la ciberseguridad, las empresas españolas destacan por su capacidad para abordar desafíos específicos en la región latinoamericana. Su liderazgo en Responsabilidad Social Corporativa no solo fortalece la productividad, sino que también impulsa la transferencia de capital intelectual, el acceso a tecnología avanzada y el continuo desarrollo de la capacitación laboral. La confidencialidad y criticidad inherentes a la ciberseguridad encuentran en las empresas españolas una ventaja significativa, respaldada por su reputación de credibilidad en el ámbito nacional.

Aunque España se posiciona en el cuarto lugar a nivel mundial en el Índice de Ciberseguridad Global (GCI) de la Unión Internacional de Telecomunicaciones (ITU), la nacionalidad española de las empresas no se presenta como un factor determinante al contratar servicios de ciberseguridad en Chile. A pesar de este reconocimiento global, la competencia en el sector chileno está marcada por actores provenientes principalmente de Estados Unidos e Israel.

La percepción general de los productos españoles en el ámbito de las Tecnologías de la Información y Comunicación es positiva, respaldada por la experiencia y prestigio de empresas como Telefónica, Everis e Indra. No obstante, en el sector de la ciberseguridad, las empresas españolas se enfrentan a un posicionamiento desafiante debido a la aún incipiente madurez del mercado.

El análisis del presente estudio de mercado revela que la procedencia del país de origen de las soluciones de ciberseguridad no influye significativamente en la decisión de contratación. El precio sigue siendo un factor crucial en servicios como auditorías y análisis de riesgos, aunque la calidad prevalece en servicios más especializados y a largo plazo, como los Centros de Operaciones de Seguridad Centralizada (SOC) y el desarrollo de *software*.

En el ámbito de la consultoría, las empresas españolas gozan de prestigio, especialmente gracias a pioneros como BBVA y Telefónica, que han replicado con éxito modelos exitosos en España.

En términos de formación, España destaca como referencia para empresas chilenas, siendo el Instituto Nacional de Ciberseguridad (INCIBE) popular entre los expertos, quienes buscan información sobre la formación proporcionada en España. Además, en materia normativa, España se erige como un referente, destacando la Ley de Protección de Datos Personales y la Ley de Infraestructuras Críticas.

La firma en julio de 2023 de un Memorándum de Entendimiento sobre Cooperación en Materia de Ciberseguridad entre España y Chile refuerza la posición de España como referente en este campo para Chile. Aunque la decisión final en la contratación de servicios de ciberseguridad está fuertemente influenciada por factores económicos, como el precio, y la experiencia de líderes

globales, la colaboración formal entre Chile y España subraya la relevancia de las empresas españolas en el sector chileno. Este acuerdo, enfocado en aspectos legislativos, policiales, estratégicos, técnicos y científicos de las Tecnologías de la Información y Comunicación (TIC), abre nuevas oportunidades para la colaboración y destaca la posición de España en el escenario de la ciberseguridad.

.

7. Canales de distribución

Los canales de distribución variarán en función de los clientes. Las empresas u organismos de ciberseguridad podrán prestar sus servicios a organismos públicos, empresas privadas o particulares, y para cada uno de ellos, será necesaria una estrategia de entrada distinta.

Cuando el cliente es un organismo o autoridad pública, el método utilizado es el proceso de licitación o adquisición pública, el cual se explica en el apartado 8.4.

En caso de que el cliente pertenezca al sector privado, se distinguen fundamentalmente dos canales de distribución:

- **Canal directo:** la práctica más frecuente se caracteriza por materializarse mediante un contrato entre el cliente final y el proveedor de ciberseguridad, donde se detallan las condiciones de prestación. Para captar este tipo de clientes, resulta esencial participar en ferias, eventos y conferencias especializadas. Este enfoque estratégico se revela especialmente beneficioso durante las fases iniciales de entrada en el mercado chileno. Dentro de este canal se incluyen a los fabricantes de *hardware* y *software y* a los proveedores de servicios (consultoras, integradores y MSSP)**.**

- **Canal indirecto:** el cliente elige a través de un distribuidor para la provisión de soluciones de ciberseguridad. Este método facilita la exportación de servicios al reducir la inversión inicial de la empresa y minimizar riesgos. Es un canal de distribución altamente beneficioso, especialmente durante las fases iniciales de internacionalización en el nuevo mercado. Se pueden considerar distintos tipos de distribuidores:

    - **Mayoristas.** Empresas que adquieren y venden productos de ciberseguridad a consultoras, integradores, proveedores de servicios de ciberseguridad o revendedores de valor añadido (VAR). Estas empresas pueden ser generalistas del sector TIC, telecomunicaciones o especializadas en ciberseguridad.
    - **Distribuidores**. empresas que realizan ventas directas al cliente final, a empresas de ciberseguridad o a revendedores de valor añadido (VAR).
    - **Minoristas**. Puntos de venta que abarcan desde tiendas físicas de informática y grandes superficies hasta pequeñas consultoras especializadas en satisfacer las necesidades de pymes y particulares.

En términos generales, las empresas asignarán recursos de sus presupuestos de TIC para cubrir sus necesidades de ciberseguridad. Las empresas más pequeñas suelen recurrir a distribuidores de confianza para obtener soluciones según sus necesidades. La recomendación del distribuidor juega un papel crucial en la toma de decisiones de contratación de este tipo de clientes.

Cuando el cliente es un particular, la adquisición de soluciones de ciberseguridad tiende a realizarse a través de minoristas, ya sea en grandes superficies o establecimientos locales. Además, durante los últimos años las tiendas *online* están ganando relevancia como canal de distribución emergente.

Como última opción, la empresa puede considerar establecerse en el país mediante una filial o un establecimiento permanente. ICEX ofrece Servicios Personalizados, como la Identificación de Socios Comerciales, que pueden ser valiosos a la hora de buscar agentes o socios comerciales locales.

8. Acceso al mercado – Barreras

8.1. Marco legislativo

8.1.1. Normativa

Es fundamental destacar que en los últimos años se ha fortalecido principalmente la legislación vigente en relación con la seguridad de la información en Chile. Las normativas correspondientes se reflejan en las siguientes disposiciones legales:

- **Ley N.º 21.459**: el 20 de junio de 2022 se aprobó esta ley, la cual establece la nueva normativa relacionada con los delitos informáticos.
- **Ley Marco Ciberseguridad e Infraestructura Crítica**: el 18 de octubre de 2022 se aprobó una ley que busca definir la institucionalidad, los principios y las normativas que tienen como objetivo organizar y coordinar la ciberseguridad en la Administración Pública, y regular la colaboración entre entidades estatales y privadas.
- **Ley N.º 21.398**: ley de protección al consumidor, la cual fue publicada el 24 de diciembre de 2021 y establece nuevos derechos para los consumidores en distintos ámbitos, entre ellos el digital.

Chile suscribió la Convención de Budapest en 2001, pero su adhesión no ocurrió hasta 2017, siendo aprobada por el Congreso Nacional según el oficio N.° 12.986 de la Cámara de Diputados, fechado el 17 de noviembre de 2016. El Instrumento de Adhesión fue depositado ante el Secretario General del Consejo de Europa el 20 de abril de 2017.

La Ley N.º 21.459 tipifica los siguientes delitos informáticos y sus sanciones:

MARCO JURÍDICO	CIBERDELITOS
Artículo 1º.	Ataque a la integridad de un sistema informático
Artículo 2º.	Acceso ilícito
Artículo 3º.	Interceptación ilícita
Artículo 4º.	Ataque a la integridad de los datos informáticos
Artículo 5º.	Falsificación informática
Artículo 6º.	Receptación de datos informáticos

Artículo 7º.	Fraude informático
Artículo 8º.	Abuso de los dispositivos

Fuente: Biblioteca del Congreso Nacional de Chile (BCN).

8.2. Barreras arancelarias y fiscales

8.2.1. Aranceles

Las importaciones de productos (*hardware*) están sujetas al pago del arancel general o derecho *ad valorem* sobre el valor CIF, que incluye el coste de la mercancía, la prima de seguro y el valor del flete, así como al pago del Impuesto sobre el Valor Añadido (IVA). El arancel general es del 6 % para mercancías originarias de países sin acuerdo comercial con Chile.

Desde 2003, está en vigor un Tratado de Libre Comercio entre Chile y la Unión Europea, cuya modernización se ha firmado a finales de 2023, lo que implica que la mayoría de los artículos importados desde Europa ingresan al país con un arancel de comercialización del 0 %, como es el caso del *hardware* en materia de ciberseguridad.

Hasta diciembre de 2003, el Servicio Nacional de Aduanas no tenía un criterio único para valorar los programas informáticos importados en soporte físico. Sin embargo, desde enero de 2004, el valor aduanero de estos soportes informáticos considera únicamente el valor del soporte físico, que incluye el *software* básico necesario para su funcionamiento. Por tanto, los pagos por derechos aduaneros son poco significativos en el caso de *software* que no constituye el programa base del equipo informático.

8.2.2. IVA e impuesto adicional

Hasta el año 2012, el artículo 59 de la Ley del Impuesto sobre la Renta (LIR) establecía un impuesto adicional del 15 % (10 % para el caso de España debido al Convenio para Evitar la Doble Imposición) sobre las cantidades pagadas desde Chile al extranjero por la utilización, disfrute o aprovechamiento de programas informáticos estándares, lo que incluía las licencias de *software*.

Sin embargo, desde enero de 2013 se exime de este impuesto a las cantidades pagadas por el uso de programas estándar. Se entiende como *software* estándar todo aquel que no ha sido sometido a un desarrollo específico para un cliente concreto. Por lo tanto, el impuesto adicional sería del 0 % si el programa vendido es de carácter estándar. Para el *software* a medida, se aplicaría el tipo del 15 % —10 % para España en virtud del acuerdo para evitar la doble imposición entre ambos países—, no siendo de aplicación en ningún caso el tipo general del Impuesto Adicional (35 %) ni el IVA (19 %). De esta manera, se reducen los costes de entrada en beneficio de los usuarios.

En cuanto al IVA, se distingue el tratamiento aplicable al soporte físico y al soporte intelectual e informático. El soporte físico siempre quedará gravado al entrar en el país por la Aduana (con un arancel del 0 % si proviene de la Unión Europea, en virtud del Acuerdo de Asociación) y con el 19 % de IVA aplicado sobre el valor CIF sumado al derecho *ad valorem*. La parte intelectual, que es la de mayor coste (*software*), en el caso de programas estandarizados, quedará exenta de dicho impuesto. En cambio, en el caso de programas especializados o a medida, pagará el impuesto adicional, pero no pagará IVA, debido a la exención establecida en el art. 12 de la Ley de IVA para todos aquellos productos a los que se les aplica el impuesto adicional.

8.3. Barreras no arancelarias

Algunos de los obstáculos al comercio internacional que no están relacionados con aranceles dentro del sector de ciberseguridad en Chile son los siguientes:

1. Regulación y Cumplimiento

Las normativas en el ámbito de la ciberseguridad en Chile pueden ser complejas y cambiantes, planteando desafíos para las empresas que buscan adaptarse a los estándares requeridos. Este entorno normativo complejo no solo dificulta la implementación efectiva de medidas de seguridad cibernética, sino que también puede generar barreras para el cumplimiento obligatorio. Las empresas se enfrentan a la necesidad de ajustarse a estándares específicos de seguridad, lo que, a su vez, puede aumentar los costes operativos y administrativos.

Chile ha demostrado una tendencia activa en la actualización normativa en ciberseguridad. En los últimos años, el país ha trabajado en fortalecer sus leyes y regulaciones para abordar cuestiones clave, como la protección de datos personales. Estas medidas reflejan la voluntad de mantenerse al día con los desafíos emergentes en el ámbito digital y podrían influir en los requisitos de ciberseguridad que las empresas deben cumplir.

2. Protección de la Propiedad Intelectual

La alta prevalencia de *software* pirata y la falta de respeto a los derechos de autor representan desafíos significativos para las empresas de ciberseguridad que buscan salvaguardar sus productos y tecnologías en Chile. Estas altas tasas de piratería no solo amenazan la integridad de la propiedad intelectual, sino que también plantean obstáculos para el desarrollo y la innovación en el sector.

La inclusión de Chile en la "lista de observación prioritaria" de la USTR[11] debido a presuntas violaciones de propiedad intelectual subraya la importancia crítica de abordar la piratería y fortalecer el respeto a los derechos de autor en el país. Este hecho destaca la necesidad de medidas más efectivas para garantizar la protección de la propiedad intelectual en el ámbito de la ciberseguridad

[11] Oficina del Representante Comercial de los Estados Unidos.

y resalta la relevancia de acciones gubernamentales y empresariales para abordar esta problemática.

3. Conciencia Limitada sobre Ciberseguridad

A pesar de los esfuerzos realizados en los últimos años para concienciar sobre ciberseguridad, persiste una limitada comprensión sobre este tema en el país. La adopción de medidas de ciberseguridad por parte de diversas empresas se ve obstaculizada por una conciencia limitada sobre la relevancia de estas acciones en determinados sectores.

4. Escasez de Talento

Aunque la inversión en programas educativos y de formación en ciberseguridad podría estar generando un impacto positivo en la disponibilidad de profesionales especializados, persiste una brecha entre la demanda y la oferta de talento en este campo. La escasez de profesionales capacitados en ciberseguridad no solo limita la capacidad de las empresas para implementar medidas efectivas, sino que también presenta desafíos adicionales, especialmente para empresas extranjeras que encuentran dificultades al intentar contratar personal local. La necesidad de abordar esta brecha y fomentar el desarrollo continuo de talento especializado en ciberseguridad sigue siendo una prioridad para garantizar la seguridad digital en el mercado laboral chileno.

5. Relaciones con el Gobierno

Las relaciones con el gobierno en el ámbito de la ciberseguridad se ven afectadas por la presencia de burocracia gubernamental, que puede ser un obstáculo para la implementación eficiente de medidas de seguridad, especialmente cuando se requieren aprobaciones y autorizaciones. No obstante, se han observado cambios recientes en los procesos gubernamentales, como la digitalización de trámites, lo que podría haber impactado positivamente en la eficiencia de la implementación de medidas de ciberseguridad. Estas actualizaciones en trámites ofrecen una oportunidad para agilizar procesos y mejorar la colaboración entre el sector privado y el gobierno en la protección cibernética.

6. Coordinación Interinstitucional

Aunque se observan esfuerzos gubernamentales para mejorar la coordinación entre diversas entidades responsables de la ciberseguridad, la falta de alineación entre estas entidades sigue siendo un desafío. Esta falta de coordinación puede generar lagunas en la implementación y aplicación efectiva de políticas de ciberseguridad. Es esencial abordar esta brecha y fortalecer los mecanismos de coordinación interinstitucional para garantizar una respuesta coherente y eficiente ante las amenazas cibernéticas en Chile.

8.4. Reglamentación de compras públicas y licitaciones

8.4.1. Ley N.º 19.886 de Compras públicas y su Reglamento

Establece las directrices para la adjudicación de contratos gubernamentales mediante licitaciones públicas, privadas o contratación directa. Existe una obligatoriedad de licitación pública para contrataciones que superen las 1.000 UTM (aproximadamente 64.200 euros), con excepciones, a través de un proceso transparente y competitivo.

- **Licitación pública o propuesta pública:** procedimiento concursal donde la Administración realiza un llamado público a través de ChileCompra y otros medios para que interesados presenten propuestas, seleccionando la más conveniente.

- **Licitación privada o propuesta privada:** procedimiento concursal donde, mediante resolución fundada, la Administración invita a personas específicas a presentar propuestas, eligiendo la más conveniente.

- **Trato o contratación directa**: Procedimiento de contratación sin concurrencia de requisitos para licitación, aplicable en casos fundamentados como falta de interesados, emergencias o contratos confidenciales.

El marco legal prohíbe fragmentar contrataciones con el fin de variar el procedimiento. En ciberseguridad, este marco normativo garantiza la transparencia y competitividad en la adquisición de soluciones digitales gubernamentales.

El Reglamento de Compras públicas establecido mediante el Decreto N.º 250 de 2004 completa la Ley 19.886 con disposiciones específicas. En el contexto de la ciberseguridad, este reglamento establece criterios técnicos y de seguridad que las soluciones digitales deben cumplir para ser consideradas en procesos de licitación. Estos requisitos contribuyen a garantizar la calidad y efectividad de las adquisiciones en el ámbito de la seguridad cibernética.

8.4.2. ChileCompra

Desde su implementación en 2003, ChileCompra ha desempeñado un papel fundamental en la modernización de las compras públicas y licitaciones en Chile. Esta plataforma centralizada ha logrado digitalizar y simplificar de manera integral todas las fases del proceso de adquisición, proporcionando un espacio único para una gestión eficiente.

La distinción principal de ChileCompra reside en su enfoque en la competencia justa, facilitando el acceso de proveedores de diversos tamaños a oportunidades gubernamentales. Este enfoque promueve una competencia equitativa que no solo beneficia la calidad de las adquisiciones del sector público, sino que también estimula la innovación.

La transparencia se erige como otro pilar clave en la operación de la plataforma. ChileCompra asegura el acceso público a información detallada sobre licitaciones y contratos, fortaleciendo la rendición de cuentas y generando confianza en la gestión gubernamental. Su eficiencia operativa adicional se traduce en la simplificación de procesos y la reducción de tiempos y costes para entidades gubernamentales y proveedores.

La eficiencia operativa de ChileCompra no solo ha transformado las compras públicas, sino que también ha facilitado la adopción ágil de soluciones avanzadas de ciberseguridad. En este sentido, la plataforma no solo representa una herramienta integral para las adquisiciones gubernamentales, sino también un impulsor efectivo del fortalecimiento de la ciberseguridad en el sector público chileno.

9. Perspectivas del sector

El sector de ciberseguridad en Chile se encuentra en un momento de crecimiento y consolidación. La creciente digitalización de la economía y la sociedad, junto con el aumento de las amenazas cibernéticas, están impulsando la demanda de soluciones y servicios de ciberseguridad.

El crecimiento continuado del mercado tiene su justificación en una serie de factores:

- **La creciente digitalización**: Chile es un país altamente digitalizado, con una penetración de Internet superior al 90 %. Este hecho está impulsando la demanda de soluciones y servicios de ciberseguridad para proteger los sistemas y datos digitales.
- **El aumento de las amenazas cibernéticas**: Los ciberataques se están volviendo cada vez más sofisticados y frecuentes. Esto está obligando a las empresas y organizaciones a invertir en ciberseguridad para protegerse de estos ataques.
- **La creciente concienciación**: Las empresas y organizaciones son cada vez más conscientes de la importancia de la ciberseguridad para proteger sus activos digitales. Esto está impulsando la demanda de soluciones y servicios de ciberseguridad.

En este contexto, se espera que el sector de ciberseguridad no solo crezca debido a factores externos, sino también a la consolidación de las principales tendencias que impulsarán el mercado.

9.1. Evolución hacia la nube segura

La creciente adopción de servicios en la nube está transformando radicalmente la gestión de datos empresariales en Chile. Esta tendencia no solo refleja un cambio en la infraestructura tecnológica, sino que también genera una demanda creciente de soluciones de ciberseguridad más robustas. La necesidad de proteger datos en tránsito y almacenados en entornos *cloud* ha impulsado el desarrollo de tecnologías específicas. La implementación de medidas como cifrado avanzado, control de acceso detallado y monitoreo continuo se vuelve esencial. Además, la migración hacia la nube segura exige estrategias adaptativas que garanticen la integridad y confidencialidad de los datos en un entorno dinámico y distribuido.

9.2. Expansión del Internet de las Cosas

El crecimiento exponencial del IoT está generando una conectividad sin precedentes entre una diversidad de dispositivos. A medida que esta interconexión se profundiza, la superficie de ataque se expande, presentando desafíos únicos en ciberseguridad. La necesidad imperante es el

desarrollo de estrategias especializadas para abordar estas complejidades. Esto implica la implementación de protocolos de seguridad sólidos, la autenticación robusta de dispositivos y la monitorización constante para detectar posibles vulnerabilidades. Enfrentar eficazmente estos desafíos permitirá a las empresas aprovechar las oportunidades del IoT de manera segura y sostenible.

9.3. Inteligencia Artificial (IA) para la defensa cibernética

La integración de la IA en soluciones de ciberseguridad marca un avance crucial. Los sistemas autónomos y las capacidades predictivas permiten una detección y respuesta a amenazas cibernéticas de manera más eficaz y proactiva. La IA no solo mejora la eficiencia operativa al automatizar tareas repetitivas, sino que también es capaz de aprender y adaptarse dinámicamente a patrones cambiantes de ataques. Esto significa que las organizaciones pueden anticipar y contrarrestar amenazas de manera más rápida y precisa. Sin embargo, la implementación exitosa de la IA en ciberseguridad también conlleva la necesidad de una supervisión constante y la actualización continua de algoritmos para mantenerse al tanto de las tácticas de ataque en constante evolución.

A pesar del crecimiento, el sector de ciberseguridad en Chile se ve confrontado por desafíos cruciales. La primera problemática radica en la escasez de talento especializado. La creciente demanda de profesionales en ciberseguridad resalta la urgencia de implementar programas educativos y de capacitación especializados para abordar la brecha de habilidades existente en este ámbito. El segundo desafío es la evolución constante de las tácticas de ciberataque, lo que implica que las empresas deben adoptar un enfoque proactivo y mantenerse a la vanguardia de las últimas tecnologías y prácticas de seguridad para hacer frente a amenazas persistentes avanzadas.

En conclusión, el sector de ciberseguridad en Chile, aunque experimenta un crecimiento significativo, no está exento de desafíos evolutivos. La combinación de una escasez de talento especializado y la necesidad de enfrentar amenazas cada vez más sofisticadas destaca la importancia de una respuesta proactiva. Sin embargo, la presencia de factores de crecimiento sólidos, la adopción de tendencias tecnológicas emergentes y los esfuerzos colaborativos posicionan a Chile favorablemente para abordar los desafíos y capitalizar las oportunidades en este dinámico paisaje de la ciberseguridad.

10. Oportunidades

10.1. Fortalecimiento de políticas de ciberseguridad

Chile fue clasificado en 2020 como el tercer país con mejor desempeño en políticas de ciberseguridad en la región latinoamericana, según los informes de la Organización de los Estados Americanos (OEA) y el Banco Interamericano de Desarrollo (BID). Este liderazgo proporciona un entorno propicio para establecer alianzas estratégicas y colaboraciones con actores clave en el ámbito de la ciberseguridad, lo que supone una oportunidad única para las empresas españolas.

En mayo de 2023, Chile presentó una nueva propuesta de la Política Nacional de Ciberseguridad, la cual incluye un eje de gobernanza público-privada. Esta iniciativa demuestra el compromiso continuo del país en fortalecer sus capacidades cibernéticas mediante la colaboración entre el sector público y privado, un enfoque estratégico que, respaldado por la nueva política integral, crea un mercado receptivo para las empresas españolas que ofrecen soluciones y servicios en ciberseguridad. Exportar tecnologías, asesoramiento y servicios especializados puede ser una vía estratégica para capitalizar las oportunidades que surgen en este entorno dinámico.

La nueva propuesta de la Política Nacional de Ciberseguridad en Chile, con su énfasis en la gobernanza público-privada, presenta oportunidades significativas para las empresas españolas. Participar en proyectos conjuntos con el sector público chileno no solo fortalecerá las relaciones comerciales, sino que también permitirá compartir conocimientos y tecnologías avanzadas en ciberseguridad, e incluso podría conducir a participar en proyectos con instituciones públicas de otros países sudamericanos.

La colaboración en la implementación de la nueva política nacional, respaldada por el enfoque proactivo de Chile en ciberseguridad, abre la puerta a la creación conjunta de proyectos innovadores en este ámbito. Las empresas españolas tienen la oportunidad de liderar iniciativas pioneras, consolidando su posición como referentes en el desarrollo de tecnologías avanzadas y eficaces contra amenazas cibernéticas. Este enfoque integral y proactivo crea un entorno propicio para la inversión y la expansión de las empresas españolas en el mercado chileno, permitiéndoles participar activamente en un ecosistema que no solo fortalecerá su posición en Chile, sino que también les brindará acceso a oportunidades emergentes en la región latinoamericana.

En resumen, el liderazgo de Chile en ciberseguridad y su compromiso con la colaboración público-privada, evidenciado por la nueva propuesta de política, ofrecen a las empresas españolas una plataforma única para expandir su presencia, liderar proyectos innovadores y contribuir al desarrollo sostenible de soluciones efectivas en el ámbito de la ciberseguridad en Latinoamérica.

10.2. Cooperación internacional

La cooperación internacional desempeña un papel crucial ante los desafíos compartidos, como los ataques cibernéticos transfronterizos que afectan a todos los países. Chile, al demostrar un compromiso sólido con la ciberseguridad, se posiciona de manera única no solo para fortalecer la colaboración internacional en esta área, sino también para liderar iniciativas con impacto a nivel regional. Su participación en acuerdos y colaboraciones a nivel regional e internacional consolida su posición en el ámbito cibernético, facilitando el intercambio de buenas prácticas, conocimientos y tecnologías avanzadas.

Ejemplos tangibles de esta colaboración incluyen acuerdos previos, como el firmado con Israel en 2018, donde ambos gobiernos colaboraron en ciberseguridad aplicada a las telecomunicaciones. De manera similar, en 2019, se estableció un acuerdo de cooperación entre los Gobiernos de Chile y el Reino Unido, destinado a fortalecer sus capacidades cibernéticas mediante la cooperación en el ámbito de la ciberseguridad.

Un hito destacado es el acuerdo sobre Cooperación en Materia de Ciberseguridad entre Chile y España, firmado en 2018. Este acuerdo busca no solo extender la cooperación bilateral en ciberseguridad, sino también promover el intercambio de buenas prácticas en la aplicación de estrategias nacionales de seguridad cibernética y agendas digitales respectivas. Además, se centra en el conocimiento de la situación, la alerta y la respuesta ante incidentes cibernéticos, evidenciando el compromiso de Chile con la cooperación internacional en ciberseguridad. En 2023, los Gobiernos de España y Chile firmaron un Memorando de Entendimiento sobre Cooperación en Ciberseguridad.

A esta dinámica se suma el acuerdo de cooperación entre la OEA y el Gobierno de Chile, firmado en 2018 para fortalecer su trabajo conjunto en ciberseguridad. Este acuerdo, en respuesta a los riesgos y desafíos en la globalización tecnológica, amplía aún más las oportunidades para los actores de ciberseguridad españoles. Les permite participar en proyectos de relevancia regional y global, contribuyendo a su destacada posición en el ámbito de la ciberseguridad a nivel internacional.

10.3. Otras oportunidades

- **Educación y formación**

  En Chile, el ámbito de la educación y la formación en ciberseguridad ofrece oportunidades significativas, con un énfasis especial en el crecimiento de empresas dedicadas a la educación a distancia. La creciente conciencia sobre la importancia de la ciberseguridad impulsa la demanda de programas educativos especializados, creando un terreno propicio para el desarrollo y la expansión.

- **Ley de Protección de Datos Personales (PDP)**

  Promulgada en 1999, tiene como objetivo salvaguardar el derecho a la privacidad y resguardar los datos personales de individuos, aplicándose a todos los contribuyentes, particulares, empresas y organizaciones. Esta legislación impone a las empresas diversas obligaciones, como obtener el consentimiento para el tratamiento de datos, informar a los titulares sobre el propósito del tratamiento y proteger la información contra accesos no autorizados, pérdidas, destrucciones o alteraciones.

  La PDP se presenta como una oportunidad para las empresas españolas de ciberseguridad en Chile, ya que estas pueden colaborar con otras compañías para asegurar su cumplimiento de la ley. Ofreciendo soluciones de seguridad, como sistemas de gestión de identidades y acceso (IAM), encriptación para proteger datos en reposo y en tránsito y herramientas de detección y respuesta a incidentes (DFIR), las empresas de ciberseguridad no solo ayudan a cumplir con la PDP, sino que también mejoran la seguridad general de la información. Esta contribución a la seguridad informática general puede reducir el riesgo de violaciones de datos, mitigando posibles impactos negativos en la reputación, finanzas y operaciones de las empresas.

  En definitiva, la PDP representa una oportunidad significativa para las empresas de ciberseguridad en Chile. Aquellas capaces de ofrecer soluciones efectivas para cumplir con esta ley estarán bien posicionadas para crecer en el mercado chileno, brindando no solo cumplimiento normativo, sino también una mejora integral en la seguridad de la información para sus clientes.

- ***Hacking* Ético y Análisis de Código**

  El *Hacking* Ético ha experimentado un crecimiento destacado en Chile, donde la creciente conciencia sobre las amenazas cibernéticas impulsa la demanda de evaluaciones de seguridad robustas. Las empresas de ciberseguridad españolas pueden capitalizar esta tendencia al ofrecer servicios especializados de pruebas de penetración, ayudando a las organizaciones chilenas a identificar y corregir vulnerabilidades en sus sistemas y redes.

  Asimismo, el pronóstico de un aumento en la demanda de servicios de Análisis de Código destaca la importancia de garantizar la seguridad desde las etapas iniciales del desarrollo de *software* y aplicaciones. Las empresas españolas pueden aprovechar esta oportunidad ofreciendo servicios especializados de revisión de código fuente, contribuyendo así a la creación de aplicaciones más seguras y resistentes a las amenazas cibernéticas. Al satisfacer la creciente demanda de servicios de seguridad en el desarrollo de *software*, las empresas de ciberseguridad españolas pueden desempeñar un papel crucial en el fortalecimiento de la infraestructura digital en Chile.

- **Ciberseguridad Industrial y TSCM**

  En el ámbito de la ciberseguridad industrial en Chile, se anticipa un aumento sustancial en la demanda de procesos de *Technical Surveillance Counter Measures* (TSCM) para contrarrestar el espionaje industrial. La protección de infraestructuras críticas se posiciona como una oportunidad estratégica en un entorno empresarial cada vez más interconectado. Las empresas de ciberseguridad españolas están bien posicionadas para aprovechar esta oportunidad, dada su experiencia en la implementación de medidas de seguridad en entornos industriales.

  La creciente interconexión de infraestructuras críticas expone a las empresas a amenazas cibernéticas más sofisticadas, generando una necesidad urgente de proteger los sistemas industriales contra posibles intrusiones. Las soluciones integrales de TSCM ofrecidas por las empresas españolas pueden abordar tanto amenazas cibernéticas como físicas, proporcionando un enfoque completo para salvaguardar los activos industriales. La colaboración estratégica con empresas locales puede ser clave para adaptar las soluciones a los requisitos específicos del sector industrial en Chile y establecer relaciones sólidas en este mercado en crecimiento. Por tanto, la ciberseguridad industrial y los procesos de TSCM representan una oportunidad estratégica para las empresas de ciberseguridad españolas, que pueden desempeñar un papel esencial en el fortalecimiento de la seguridad en el sector industrial chileno.

11. Información práctica

11.1. Organizaciones relacionadas

Las organizaciones relacionadas con el sector de la ciberseguridad en Chile y el mundo digital son las siguientes:

- **Fundación País Digital** (http://www.paisdigital.org/)
- **Cámara de Comercio de Santiago** (http://www.ccs.cl/)
- **Club Chile Digital** (http://www.club.chile-digital.com/)
- **Cámara Chilena de Comercio Electrónico** (http://www.camaradecomercioelectronico.cl/)
- **Asociación Chilena de Empresas de Tecnología de la Información** (http://www.acti.cl/)
- **Asociación de Empresas Chilenas de Tecnologías** (http://www.chiletec.org/)
- **Servicio Nacional del Consumidor** (http://www.sernac.cl/)
- **Asociación de Bancos e Instituciones Financieras** (https://www.abif.cl/)
- **Asociación de Emprendedores de Chile** (http://www.asech.cl)
- **CETIUC** (http://www.cetiuc.com/)
- **Centro de Ciberseguridad (CSIRT)** (https://www.ciberseguridad.gob.cl/)
- **Alianza Chilena de Ciberseguridad (**https://alianzaciberseguridad.cl/**)**
- **Centro de Ciberseguridad Industrial en Chile** (https://www.cci-es.org/maps/chile/)
- **CDTI (**https://www.cdti.es/)

11.2. Ferias y eventos del sector

Uno de los principales puntos de encuentro en el sector de la ciberseguridad en Chile reside en las ferias y eventos que se organizan en el país. Algunos de los más destacados son:

- SeguridadExpo: feria comercial líder integral de seguridad convergente en Chile para Latinoamérica. Se realiza anualmente en Santiago y reúne a expositores de todo el mundo, ofreciendo soluciones en los siguientes ámbitos: seguridad pública y privada, seguridad industrial y salud ocupacional, ciberseguridad y seguridad contra incendios y desastres naturales.
- Cybersecurity Bank & Government: evento de organizado por Infosec que reúne a innovadores, tecnólogos y líderes empresariales de la ciberseguridad de bancos y gobiernos en América

Latina, Centro América y Caribe para ayudarlos a proteger sus redes y activos en un entorno digital cada vez más complejo y hostil.

- Cyber iCON Chile: encuentro organizado por Deloitte, tiene por objetivo presentar los desafíos que enfrenta la ciberseguridad en Chile en el contexto actual, considerando los retos de una industria que avanza y evoluciona de manera constante.
- Summit País Digital: evento anual que se realiza en Chile y reúne a representantes de la sociedad civil, el sector público y el sector privado para discutir sobre el desarrollo de la cultura digital en el país. El evento se centra en temas como la economía digital, la innovación, la educación digital y la ciberseguridad.
- 8.8 Computer Security Conference: evento anual que se realiza en Chile y reúne a profesionales de la ciberseguridad de todo el mundo. El evento se centra en temas como la seguridad de la información, la seguridad de las redes, la seguridad de los dispositivos y la respuesta a incidentes de ciberseguridad.
- Foro Nacional de Ciberseguridad: evento anual, organizado por el Senado de Chile y la Fundación País Digital, que reúne a expertos de la ciberseguridad, representantes del sector público y privado y miembros de la sociedad civil para discutir sobre los desafíos y oportunidades de la ciberseguridad en el país. El Foro Nacional de Ciberseguridad fue lanzado en 2023 por el Senado de Chile con el objetivo de promover el diálogo y la cooperación entre los actores públicos y privados en materia de ciberseguridad.
- Bsides Chile: conferencia de ciberseguridad sin ánimo de lucro que se celebra anualmente en Santiago de Chile. El evento reúne a profesionales de la seguridad de la información de todo el mundo para compartir conocimientos y experiencias sobre las últimas tendencias y amenazas en el campo.

11.3. Publicaciones del sector

- *Panorama de Amenazas en América Latina*, de Kaspersky.
  https://latam.kaspersky.com/
- Reportes del Observatorio de Ciberseguridad de América Latina y el Caribe.
  https://observatoriociberseguridad.org/#/final-report
- Reporte Cuarta Edición Índice Global de Ciberseguridad
  https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E
- *Chile Cybersecurity Market Size & Share Analysis*
  https://www.mordorintelligence.com/industry-reports/chile-cybersecurity-market

- *El Avance de la Economía Digital en Chile*, por Accenture y Oxford Economics https://dokumen.tips/documents/el-avance-de-la-accenture-6-el-avance-de-la-economa-digital-en-chile-figura.html?page=1
- *Global Cybersecurity Spending* de Canalys https://www.canalys.com/analysis/cybersecurity
- Informe *X-Force Threat Intelligence Index 2022* de IBM Security https://www.ibm.com/downloads/cas/ADLMYLAZ
- *Reporte de Ciberseguridad 2022 y Tendencias 2023 en Chile y Latinoamérica* https://landing.enteldigital.cl/reporte-ciberseguridad-2022-y-tendencias-2023?utm_campaign=Reporte %20ciberseguridad %202023&utm_source=email&utm_medium=mail&utm_term=organic&utm_content=reporte_ciberseguridad_2023_CCI
- Informe Global del Panorama de Amenazas 2022 de Fortinet https://www.fortinet.com/lat/demand/gated/threat-report-2h-2022

Si desea conocer todos los servicios que ofrece ICEX España Exportación e Inversiones para impulsar la internacionalización de su empresa contacte con:

Ventana Global
913 497 100 (L-J 9 a 17 h; V 9 a 15 h)
informacion@icex.es

Para buscar más información sobre mercados exteriores siga el enlace

www.icex.es

GOBIERNO DE ESPAÑA
MINISTERIO DE INDUSTRIA, COMERCIO Y TURISMO
ICEX España Exportación e Inversiones