
digital
REPORTE
CIBERSEGURIDAD
2024
Desarrollado por el
Centro de Ciberinteligencia
4ta edición

INDICE

Introducción

En el año 2023, Latinoamérica se sumó a la tendencia mundial de aumento en los ciberataques, y Chile, lamentablemente, tampoco fue la excepción. Las amenazas por Ransomware y los ciberincidentes marcaron la actualidad noticiosa semanal de nuestro país durante los últimos meses del año, dejando a su paso un octubre negro para los registros. Si bien este contexto fue previsto en nuestro reporte previo, ¿Qué hay realmente de nuevo?

Tal vez lo primero sea señalar que, a diferencia de años anteriores, durante 2023 todo tipo de organizaciones, sin importar su tamaño o sector productivo, se vieron afectadas por ciberamenazas que dejaron al descubierto trascendentales brechas de seguridad.

Asimismo, la sofisticación de los ataques no ha disminuido, muy por el contrario, la ingeniería social, el robo de información y los ataques a usuarios y administradores de sistemas se han convertido prácticamente en commodities. ¿Estaremos hablando entonces de su "industrialización"?

En parte sí. El uso de nuevas herramientas de Inteligencia Artificial (IA) y Cloud ha generado una ola de innovación en el mundo, impactando los procesos de negocios basados en datos, propulsando la creatividad y la productividad. Sin embargo, a modo de contracara, 1000% de los ataques automatizados se ejecutaron siguiendo inmediatamente el lanzamiento de nuevas versiones de IA generativa: ataques transnacionales en búsqueda de brechas y vulnerabilidades en los sistemas publicados.

>1000%
Ataques tras lanzamiento IA generativa

Por otra parte, 2023 fue un año récord de ciberataques a las infraestructuras Cloud, lo que provocó que miles de configuraciones fueran filtradas y aprovechadas enseguida por la ciberdelincuencia. Aunque la respuesta de las empresas de tecnologías de ciberseguridad ha sido efectiva en sus entornos productivos, los actores de ambos campos se enfrentan hoy a una escala de desarrollo nunca antes vista.

Desde nuestro lado, como "defensores" de los activos de las organizaciones y en especial de nuestros clientes, **proyectamos un volumen en expansión de los ataques de complejidad aguda, los que sólo podrán ser resueltos con el uso de IA y tecnologías de anticipación e inteligencia.**

La gestión de incidentes es clave y la realidad país da cuenta de que muchas empresas aún no logran anticipar y menos orquestar estos incidentes, ya sea por falta de madurez interna, manejo de crisis, expertise o presupuesto. Es evidente que, ante este contexto, la colaboración se vuelve una necesidad estratégica.

Es aquí donde nuestro propósito de compartir experiencias y conocimiento con la comunidad cobra sentido y se fortalece. Como Entel Digital, nos enorgullece ser parte de **Forum of Incident Response and Security Teams** (FIRST), organización de equipos expertos a nivel mundial que apuesta por la colaboración para responder a incidentes de seguridad que afecten a una organización en cualquier lugar del planeta.

+200
Alertas de amenazas

Como parte de esta visión, en Entel Digital nos hemos comprometido con la vigilancia, a través de nuestro equipo experto de Ciberinteligencia. Así, hemos asumido un rol activo en la generación de información a la comunidad, reportando más de 200 alertas e innumerables informes de ciberamenazas en Chile y fuera de sus fronteras para aumentar capacidades de respuesta.

Felicitamos por este enorme esfuerzo a nuestros equipos, cerrando un año exigente, apoyando a numerosas empresas en mejorar su postura, conciencia y elección de servicios y tecnologías, siempre poniendo en el centro la Ciberinteligencia.

Esperamos que este reporte sea un referente para los desafíos en este ámbito para cada lector.

Cyril Delaere
Gerente de la unidad
de Ciberseguridad

CAPÍTULO 1

Entel Digital se suma a FIRST

La principal red global de especialistas en Inteligencia Cibernética

Entel Digital ya es miembro de FIRST

La efectividad en la gestión de ataques cibernéticos es un desafío mundial al que **Entel Digital contribuye desde 2023, a través de su división de Inteligencia Cibernética (CCI), ahora integrada a la red global FIRST**.

FIRST es una entidad de profesionales de renombre que colabora, siguiendo estrictos protocolos de confidencialidad, para mitigar el impacto de los ciberataques en cualquier lugar del mundo. **Opera bajo un esquema de gobernanza colaborativa, integrando equipos especializados en la respuesta a incidentes de ciberseguridad**, productos de seguridad y analistas independientes.

La red FIRST:

Involucra a más de 700 equipos de respuesta

Está presente en más de 100 países

Permite intercambiar información valiosa

Entrega acceso a conferencias y reuniones anuales

* Fuente: https://www.first.org/

“Integrar estos equipos de trabajo valida los servicios de Entel Digital a nivel global, posibilitando una colaboración estrecha con colegas del sector para mantenerse actualizados”

Eduardo Bouillet, Director del CCI de Entel Digital, señaló la importancia de ser parte de esta organización, ya que se trata de una vasta red que promueve la confianza entre sus integrantes, quienes **comparten conocimientos sobre la gestión de una variedad de ciberataques que impactan a diversas industrias**. Con una conexión constante entre todos los miembros, el equipo intercambia información, procedimientos y estudios para estar en la vanguardia de la seguridad digital y ofrecer respuestas más rápidas y seguras a sus clientes.

El Director del CCI también mencionó que integrar estos equipos de trabajo valida los servicios de Entel Digital a nivel global, posibilitando una colaboración estrecha con colegas del sector para mantenerse actualizados sobre las dinámicas cambiantes de ciberataques, mejorando así los servicios que Entel Digital brinda a sus clientes.

En 2023, el equipo de seguridad de Entel Digital participó en la Conferencia Anual de FIRST “Empowering Communities” realizada en Canadá con más de 800 asistentes, **que demostró el valor de la colaboración en el fortalecimiento de la oferta de servicios frente a ciberamenazas**. Ya se anticipa con entusiasmo la próxima conferencia que tendrá lugar en Japón en 2024.

* Fuentes: https://www.first.org/conference/2023/
https://www.first.org/conference/2024/

Actividades Clave y Logros de FIRST

Conferencias y talleres

Organiza conferencias anuales y talleres que sirven como foro para el intercambio de experiencias, ideas y estrategias en la gestión de incidentes de seguridad.

Estándares y prácticas

La organización ha sido instrumental en el desarrollo y la promoción de estándares y buenas prácticas para la respuesta a incidentes de seguridad informática.

Colaboración global

Ha fomentado la colaboración global entre equipos de respuesta a incidentes, proporcionando una red crítica para compartir información y recursos.

Formación y capacitación

Ofrece programas de formación y capacitación para mejorar las habilidades y conocimientos de los profesionales en la gestión de incidentes de seguridad.

Impacto Actual y Futuro

› Relevancia en la era digital

En la actualidad, FIRST sigue siendo una entidad clave en el ámbito de la ciberseguridad, adaptándose continuamente a las cambiantes dinámicas y desafíos del espacio digital.

› Enfoque en Nuevas Amenazas

La organización sigue evolucionando para abordar nuevas amenazas, como la seguridad en la nube, la ciberseguridad en sistemas críticos y la creciente complejidad de los ataques informáticos.

En resumen, juega un papel crucial en el **fortalecimiento de la respuesta global a incidentes de ciberseguridad**, promoviendo la colaboración, el intercambio de conocimientos y el desarrollo de prácticas efectivas en un mundo cada vez más interconectado y digitalizado.

* Fuente: https://www.first.org/

Integración MISP ENTEL con MISP FIRST

Durante el transcurso de 2023, Entel ha dado un paso significativo hacia las mejoras en ciberseguridad mediante la **integración exitosa de nuestra plataforma MISP con la plataforma MISP de FIRST**.

Esta estrategia no solo refleja nuestro compromiso con la seguridad digital, sino que también demuestra nuestra capacidad para colaborar y compartir información crítica de amenazas en tiempo real.

La colaboración ha permitido a Entel aprovechar las fortalezas de FIRST en la detección y análisis de amenazas, optimizando así nuestras operaciones de respuesta a incidentes.

› Mejor tiempo de respuesta

Desde el punto de vista tecnológico, **la interoperabilidad entre las plataformas MISP se ha mejorado** gracias a la implementación de herramientas analíticas avanzadas y la automatización de procesos, mejoras que han permitido un análisis más profundo y una respuesta más rápida a las amenazas emergentes.

* Fuente: https://www.first.org/global/sigs/information-sharing/misp

› Menos incidencias

Los datos recopilados desde el comienzo de esta alianza, muestran una disminución en la frecuencia de incidentes, así como una reducción en el tiempo de respuesta a las amenazas detectadas. Estas métricas son testimonio del valor tangible que **la integración de MISP aporta a nuestras capacidades de Threat Intelligence**.

› Mirando hacia el futuro

Nos estamos preparando para expandir esta integración. Entendemos que el panorama de amenazas es dinámico y que solo a través de la adaptabilidad y la innovación continua podemos esperar mantenernos a la vanguardia de la seguridad cibernética.

Nuestros planes incluyen el **desarrollo de nuevas funcionalidades y la profundización de la colaboración con FIRST** y otros socios estratégicos.

* Fuente: https://www.first.org/global/sigs/information-sharing/misp

Este capítulo no solo sirve como registro de nuestro progreso, sino también como un compromiso con la excelencia continua y la colaboración dentro de la comunidad global de ciberseguridad.

Alianza
Desde el **24 de febrero de 2023**, somos parte de FIRST.

1363
Organizaciones componen actualmente FIRST.

Conexión 24/7
Permite ofrecer servicios seguros y **acotar los tiempos de respuesta a incidentes**.

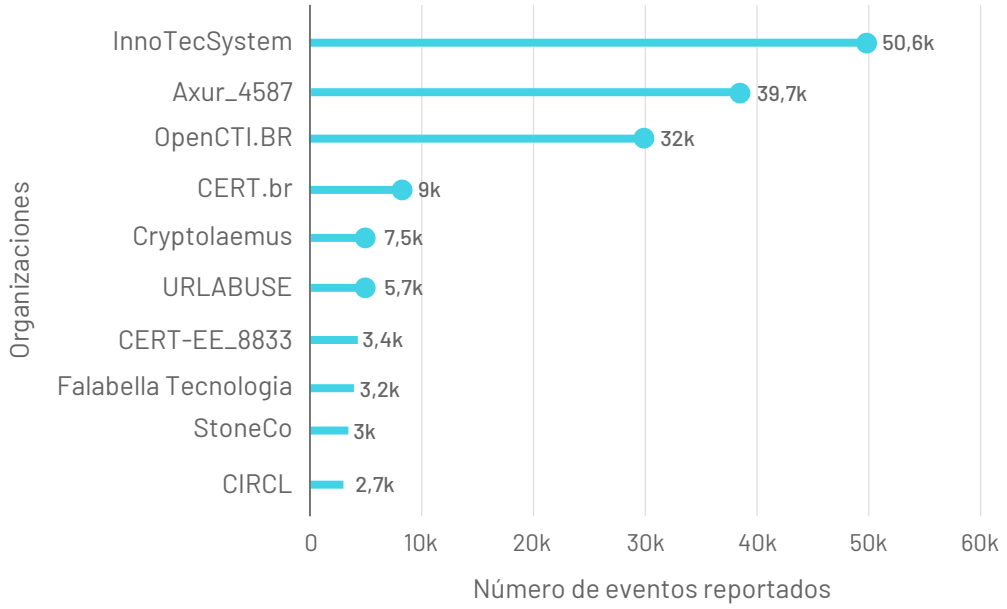
+ de 190.000
Eventos han sido reportados desde la creación de FIRST.

Cooperación Global
Brinda la **visión de incidentes** en otros continentes para mitigar ciertas amenazas.

+ de 35.000
Eventos han sido **reportados en lo que va del 2023**.

El siguiente gráfico detalla el Top 10 de la cantidad de eventos reportados por las primeras 10 organizaciones, **abarcando el periodo desde el lanzamiento FIRST en el año 2015 hasta diciembre de 2023**.

Top 10 organizaciones que más eventos han reportado en Misp de FIRST



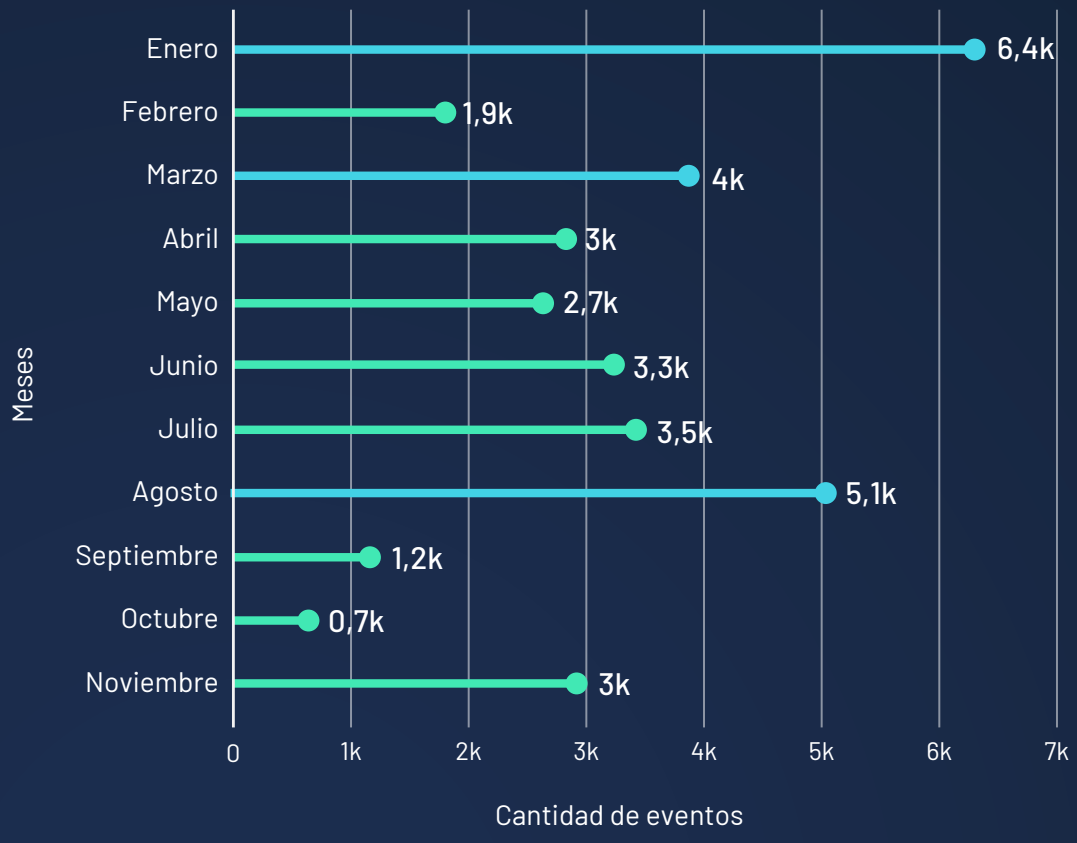
* Fuente: https://misp.cci-entel.cl/

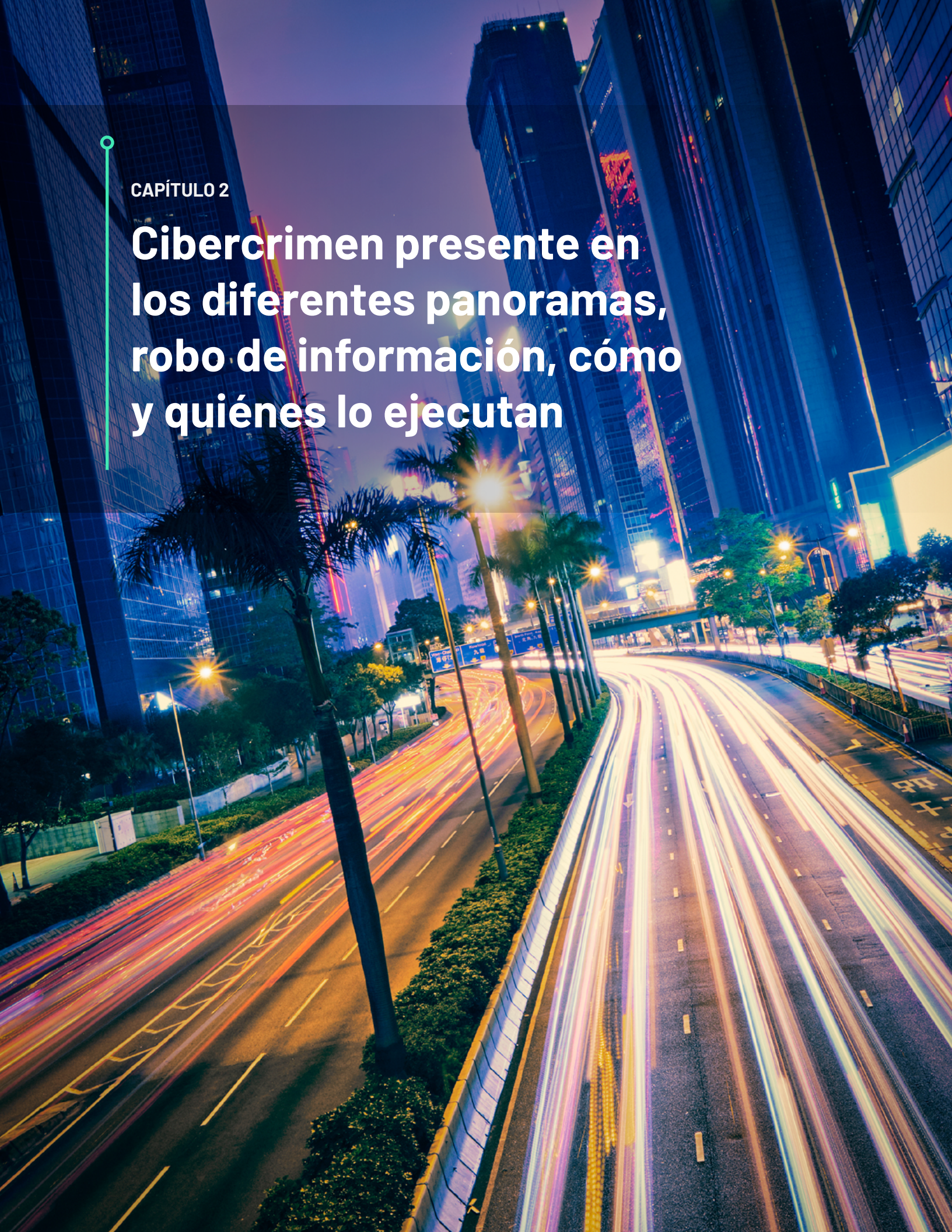
El siguiente gráfico muestra los eventos reportados por meses en la plataforma MISP de FIRST durante el año 2023. Cabe destacar que la gran mayoría de los eventos reportados corresponden a **ataques de Phishing y Malware (incluido Ransomware)**.

Estos eventos fueron aproximadamente 35.000, lo cual equivale a un **18,4% del total de eventos desde que se implementó la plataforma en el año 2015**.

* Fuente: https://misp.cci-entel.cl/

Eventos por meses en Misp de First (2023)





CAPÍTULO 2

Cibercrimen presente en los diferentes panoramas, robo de información, cómo y quiénes lo ejecutan

La tecnología ha transformado radicalmente la forma en que interactuamos, trabajamos y nos comunicamos a diario, dando lugar a un fenómeno preocupante: el cibercrimen, una modalidad utilizada por actores que **se valen de la tecnología informática y las redes de comunicación como medio para cometer actos ilegales en el ciberespacio**.

Estos delitos **pueden abarcar una amplia variedad de actividades maliciosas**, que van desde fraudes en línea y robo de identidad personal hasta ataques cibernéticos más sofisticados, como la infiltración de sistemas informáticos, ejecución de Malware, el secuestro y robo de información confidencial, extorsión, entre otros.

› Análisis del robo de información

Hoy en día, tanto empresas como organizaciones utilizan grandes cantidades de datos para llevar a cabo sus operaciones y así cumplir con sus objetivos estratégicos.

El problema es que gran parte de los ciberataques tienen como objetivo principal **robar información clasificada, para obtener un beneficio económico a cambio**. Por lo mismo, independientemente de dónde almacene sus datos cada empresa (nubes compartidas, centros locales, etc.) es fundamental que se cumplan ciertos estándares de seguridad que garanticen la integridad, confidencialidad y disponibilidad de la información.

Uno de los **ataques más frecuentes y que mayor impacto provocan en las víctimas es el Ransomware.** Este tipo de ataque ha desarrollado una modalidad de doble extorsión, en donde **no solo cifran la información de la organización, sino que también extorsionan con publicarla** días después en caso de no pagarse el rescate. Dependiendo de la víctima, esto puede causar graves daños, como la interrupción en las operaciones comerciales, costos financieros adicionales, impacto en la continuidad del negocio, daño reputacional en sus clientes, pérdida de confianza y prestigio.

2.1 Panorama de Amenazas (Malware y Ransomware)

› Malware

El panorama de Malware suele estar liderado por los mismos actores año tras año, debido al perfeccionamiento continuo de sus procesos y a su larga trayectoria.

Si bien existen diversos tipos de Malware, no suele haber mucha variedad en sus métodos de acceso inicial a los equipos, pues **la mayoría se ejecutan por medio de mecanismos de ingeniería social**, logrando que sea el usuario quien voluntariamente ejecute o active el Malware.

Entre los **diversos métodos** se pueden encontrar:

- **Acceso mediante troyanos**
- **Acceso mediante phishing**

› Troyanos

Existen diversos tipos de troyanos, y **gran parte de ellos tienen su origen en Brasil**, un importante generador de varias familias de Malware que han plagado a los clientes bancarios latinoamericanos durante años. Algunas variantes como Amavaldo, Mekotio, Grandoreiro y Cabaneiro, según una investigación de ESET, comparten varias similitudes atribuibles a un probable esfuerzo de colaboración entre múltiples actores de amenazas.

Troyanos	Funcionamiento	Características
Amadey Pertenece a una **red botnet**. Fue detectado por primera vez en **2018**.	Extrae información confidencial de los sistemas comprometidos. Actúa como puente para la descarga de las etapas subsiguientes de un ataque.	Se ha visto estrechamente vinculado con Smoke Loader, un Malware que presenta características similares.
Mekotio Malware brasileño.	Usualmente, aprovecha temáticas contingentes de phishing en cada país donde se distribuye.	Se ha observado principalmente en países hispanohablantes como Perú, Uruguay, Paraguay, Bolivia, México, Chile, España, Argentina, Ecuador, Brasil y Colombia.

* Fuentes: https://www.eset.com/py/acerca-de-eset/sala-de-prensa/comunicados-de-prensa/articulos-de-prensa/eset-advierte-sobre-notificaciones-judiciales-falsas-que-distribuyen-un-troyano-bancario/
https://www.welivesecurity.com/la-es/2020/04/28/grandoreiro-troyano-bancario-dirigido-brasil-espana-mexico-peru/
https://www.welivesecurity.com/la-es/2021/12/15/analisis-12-troyanos-bancarios-america-latina/

Troyanos	Funcionamiento	Características
TrickBot **(También conocido como Trickster, TheTrick o TrickLoader).** Botnet activa desde finales de 2016.	Con el tiempo se ha convertido en un Malware multipropósito, disponible como Malware-as-a-Service (MaaS).	En sus inicios contenía exclusivamente características de troyano para robar credenciales de acceso a cuentas bancarias en línea. Ha llegado a ser una de las botnets más prolíficas.
Grandoneiro Malware brasileño.	Tiene como objetivo principal a entidades bancarias y servicios de criptomonedas.	Comparte características con otros de su mismo país de origen.

› Infostealer

Durante los últimos años, ha existido un constante crecimiento en el uso de **Infostealers que se ofrecen como Malware as a Service (MaaS)**. Su función principal es robar la mayor cantidad de información posible de un usuario, para luego venderla en mercados negros o generar ataques de Ransomware, tanto por la información que capturan como por los accesos iniciales que entregan.

Si bien, cada Malware tiene sus propias características, existen algunas comunes como la sustracción de credenciales guardadas en navegadores, sistemas o servicios del equipo. La última tendencia es la sustracción de billeteras de criptomonedas, un tipo de ataque que ha demostrado ser bastante lucrativo y escasamente regulado.

* Fuentes: https://www.eset.com/py/acerca-de-eset/sala-de-prensa/comunicados-de-prensa/articulos-de-prensa/eset-advierte-sobre-notificaciones-judiciales-falsas-que-distribuyen-un-troyano-bancario/ https://www.welivesecurity.com/la-es/2020/04/28/grandoreiro-troyano-bancario-dirigido-brasil-espana-mexico-peru/ https://www.welivesecurity.com/la-es/2021/12/15/analisis-12-troyanos-bancarios-america-latina/

Entre los **infostealer más visualizados durante los últimos años** se encuentran:

Infostealer	Funcionamiento	Características
Redline Es administrado directamente por sus propios operadores.	Se encuentra distribuido principalmente mediante softwares troyanizados, ofrecidos de forma gratuita para prestar servicios que originalmente son de pago.	Es el Malware as a Service (MaaS) con mayor presencia en Chile.
Vidar Se evidenció originalmente a finales de 2018.	Se observa como un canal para permitir la implementación de Ransomware.	Es capaz de filtrar una variedad de datos de un equipo infectado.
MetaStealer Fue identificado por primera vez en marzo de 2022.	Se autodenomina como una versión mejorada del conocido Redline. Además de la sustracción de credenciales, es capaz de obtener acceso a billeteras de criptomonedas instaladas en equipos o navegadores.	En mayo de 2022 se registraron las primeras afectaciones en Chile.

Crypto Minero XMRig

Es un software de minería de código abierto que, a diferencia de otras amenazas, es completamente legítimo para facilitar el acceso a la criptominería de Monero (criptomoneda difícil de rastrear). Su uso mal intencionado otorga mayor anonimato para los ciberdelincuentes y, por tanto, no se considera un Malware por sí solo, más bien es una herramienta.

Ha sido adoptada por los cibercriminales para **añadir funcionalidades de cripto minería a su Malware**, y es completamente adaptable a las necesidades de los actores maliciosos, aspecto que lo ha hecho popular y lo mantiene vigente hasta el día de hoy. Fue visto por primera vez en mayo de 2017.

Ransomware

Es un tipo de Malware que presenta uno de los mayores índices de ataques en LATAM y se caracteriza por tener un gran impacto sobre las víctimas.

A modo general, su operación se basa en el secuestro de información por parte de ciberdelincuentes, para luego solicitar un rescate económico.

Este tipo de amenazas continúa siendo un dolor de cabeza para los afectados, ya que **implica arduas negociaciones que pueden definir el futuro de la organización,** sobre todo si no se cuenta con adecuados respaldos de información.

Negociaciones

En estas negociaciones, se debe decidir si asumir pérdidas y posibles filtraciones de datos o pagar un rescate. Las víctimas suelen ser publicadas en portales en línea, lo que daña su reputación y las expone a ser fijadas como objetivo de otros actores, que pasan a considerar la organización como una posible fuente de dinero.

Cabe destacar que las publicaciones de víctimas en portales de actores de amenaza también puede darse en pleno proceso de negociación, ya que esta es una medida de extorsión utilizada por los ciberactores.

Doble extorsión

También se usa la modalidad de doble extorsión, en donde **los actores de amenaza no solo cifran la información de la organización, sino que también presionan con publicarla días después en caso de no pagar por el rescate**, lo que puede causar graves daños como:

- Interrupción de las operaciones comerciales.
- Costos financieros adicionales.
- Impacto en la continuidad del negocio.
- Daño reputacional que lleve a los clientes a perder la confianza.

Un constante riesgo

Aquellas organizaciones que aún no se han visto afectadas por este tipo de amenazas corren un riesgo constante, ya que **los ciberdelincuentes ponen a prueba diferentes pilares organizacionales de manera continua, afectando su adecuada protección:**

- Existen organizaciones que han logrado perfilar sus vulnerabilidades, pero por el desinterés de los tomadores de decisiones o la falta de agilidad organizativa, **no se destinan los recursos adecuadamente o a tiempo, abriendo la posibilidad de ser atacados en cualquier momento.**

- Aquellos que están conscientes de los riesgos y las amenazas en internet, toman decisiones para adelantarse a estas eventualidades. Sin embargo, debido a la velocidad, capacidades y sofisticación de los actores, pueden existir vulnerabilidades Zero-Day o de alta criticidad que **abren brechas de ataques hasta en las organizaciones más preparadas**.

En este punto, **es importante contar con claros protocolos** y mecanismos de respuesta para anticiparse, detectar, contener y mitigar amenazas sin mayores daños.

Ransomware en LATAM

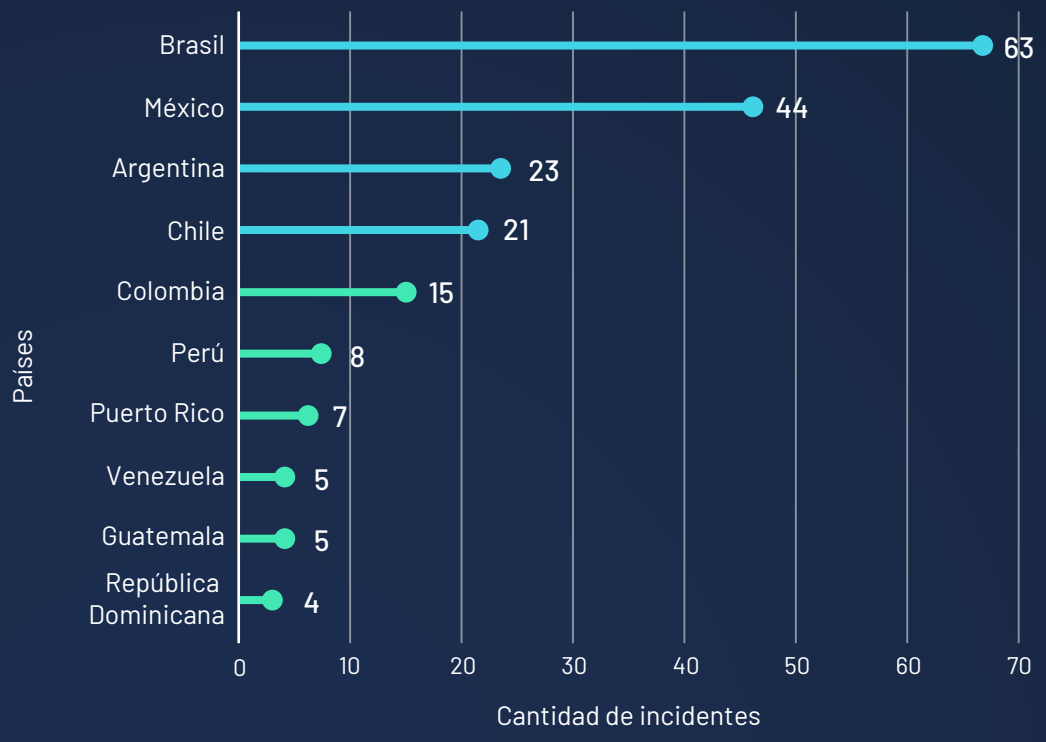
› Países más afectados durante 2023

Durante 2023, se mantiene un registro de **22 países afectados dentro de LATAM**, incluido Chile, el cual se encuentra en la cuarta posición, detrás de Brasil, México y Argentina, siendo este último quien en el Q1 de 2023 se encontraba en igualdad de víctimas con Chile.

El Top 5 concentra el 74,8% de los ataques en todo el territorio Latinoamericano, siendo Brasil el más afectado con un 29% del total, mientras que Chile presenta el 9,7% de los casos.

* Fuentes: Registros internos CCI Entel Digital
RR. SS.
https://www.stealthmole.com/

TOP 10 países más afectados con ransomware en Chile y LATAM



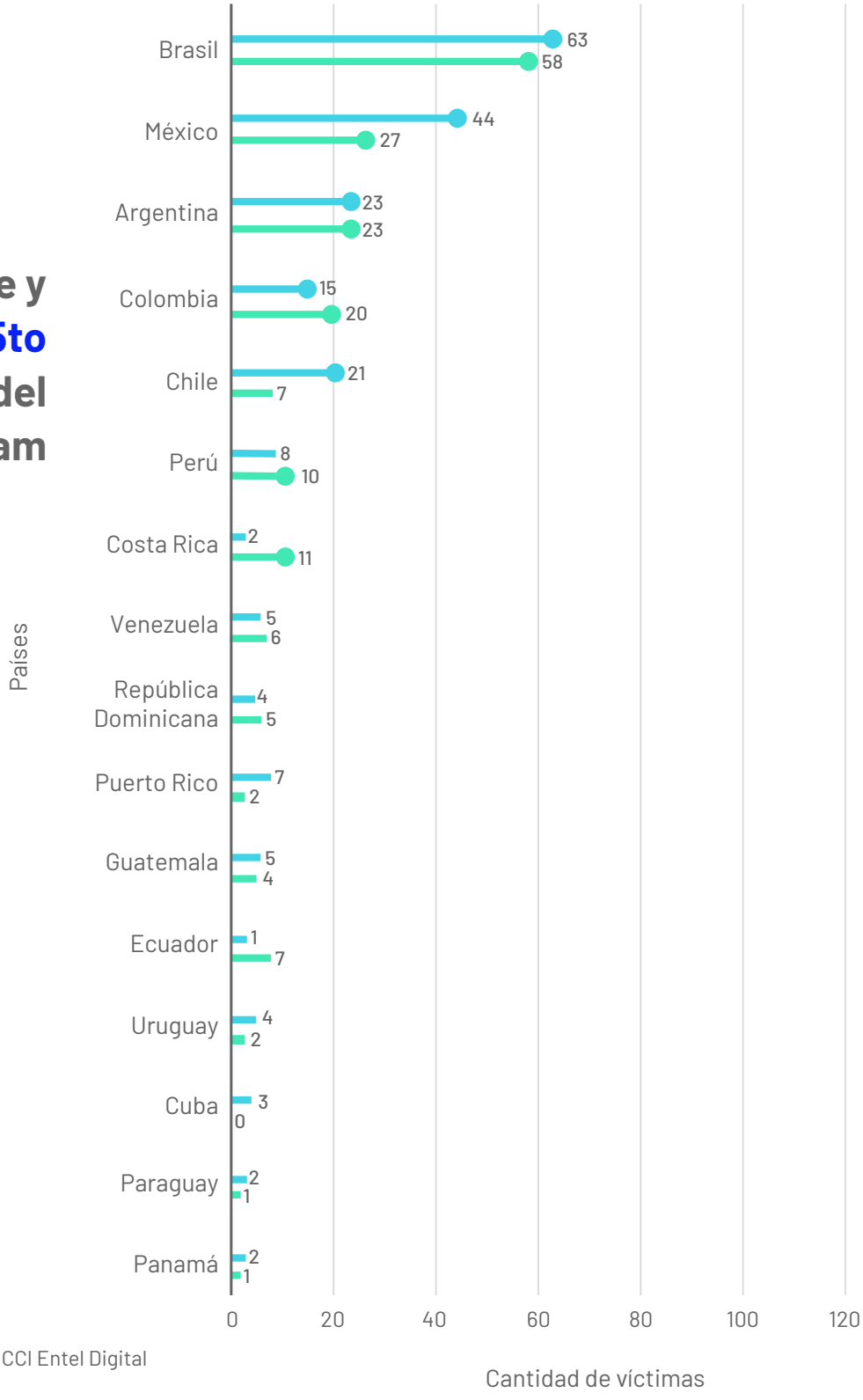
Al visualizar esta misma información en el mapa, se puede apreciar que la mayor parte del territorio continental cuenta con víctimas de Ransomware, restando principalmente a países como Guyana francesa, Surinam y algunas islas, lo cual da luces de cómo los actores distribuyen sus objetivos dentro del territorio.

Mapa víctimas de ransomware en Chile y LATAM 2023

* Fuentes: Registros internos CCI Entel Digital
RR. SS.
https://www.stealthmole.com/

Comparativa de víctimas de ransomware en Chile y LATAM 2022 v/s 2023

Chile sube y llega al 5to puesto del ranking Latam



* Fuentes: Registros internos CCI Entel Digital
RR. SS.
https://www.stealthmole.com/

Comparativa países 2022 - 2023

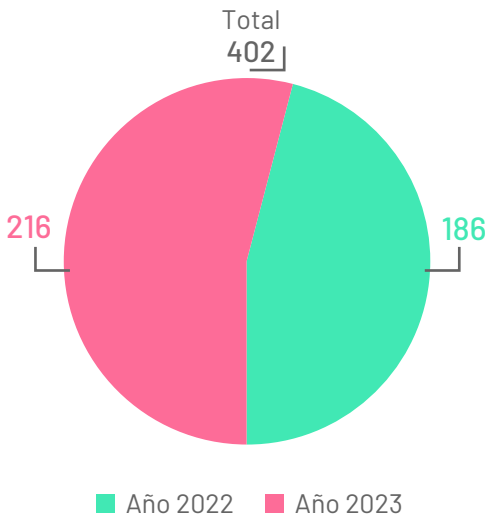
Al analizar el grado de incidencia de 2023, es posible identificar que la tendencia se mantiene similar a los datos presentados en 2022, con la diferencia de que ahora **Chile ha escalado al último lugar del Top 5.**

Por su parte, **Brasil se mantiene indiscutiblemente a la cabeza con un 30%** de las víctimas totales en LATAM, presentando una holgada diferencia respecto de México que se encuentra en la segunda posición.

Comparativa histórica

En septiembre de 2023 ya se superó la cantidad de víctimas de Ransomware en LATAM de todo el año 2022, generando un total de 402 incidentes totales, considerando ambos años. Se espera que este número continúe en constante aumento, debido a las grandes retribuciones económicas que obtienen los ciberdelincuentes mediante este tipo de ataques.

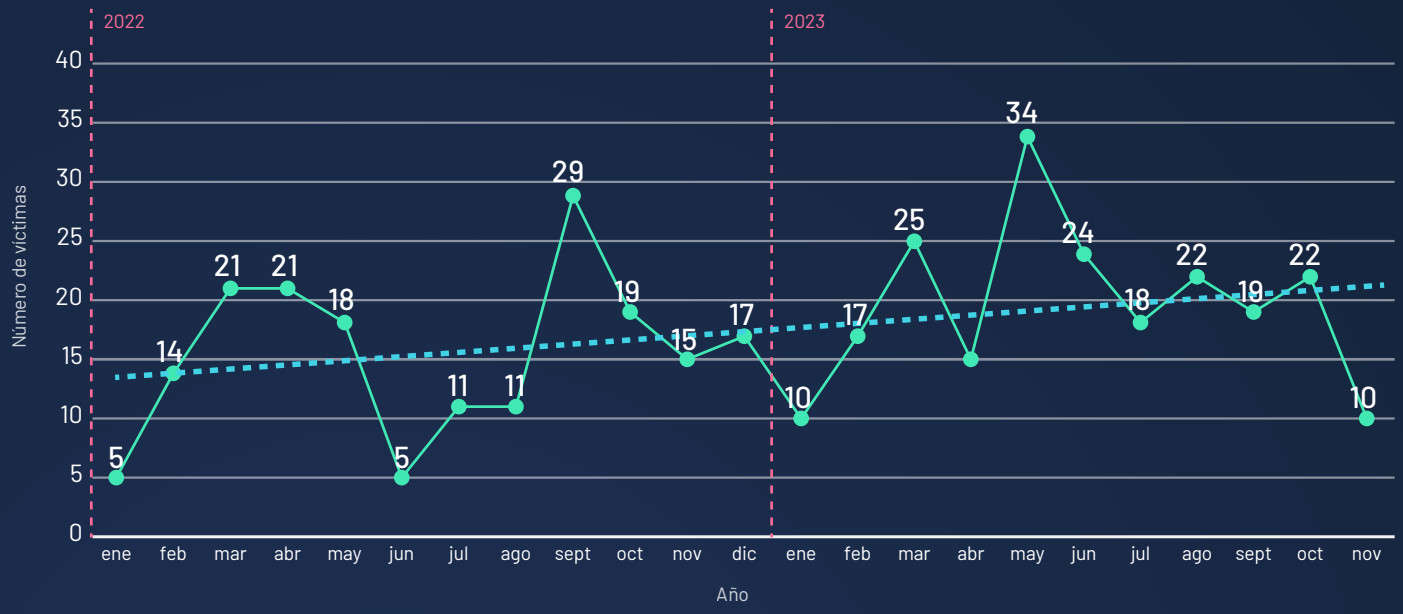
Total incidentes de ransomware años 2022 y 2023



Al segregar los datos por meses, es posible visualizar que tuvo un mayor alza durante mayo de 2023 y que la tendencia va en constante aumento hacia 2024.

* Fuentes: Registros internos CCI Entel Digital
RR. SS.
https://www.stealthmole.com/

Cantidad de víctimas de ransomware por mes entre 2022 y 2023



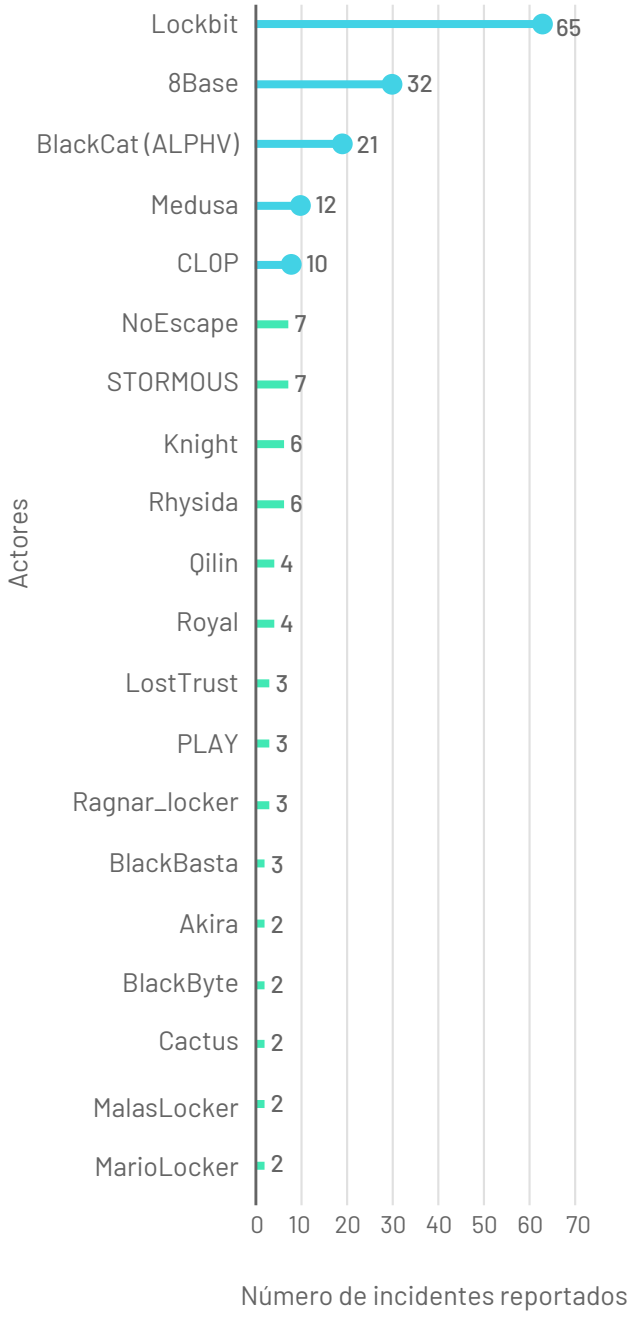
Grupos más activos durante 2023

Durante 2023, los grupos con altos índices de incidencias han mantenido posiciones similares a años anteriores. **8Base es el único que ha registrado un aumento significativo**, pues ha realizado una serie de ataques de forma ininterrumpida a una gran variedad de industrias y rubros de la región.

Un total de 39 grupos de Ransomware diferentes han afectado a 216 organizaciones diferentes en LATAM. **El Top 20 de actores abarca el 90,2% de los casos**, siendo **LockBit quien encabeza la lista con un 30,6% de las incidencias** anuales en LATAM.

* Fuentes: Registros internos CCI Entel Digital
RR. SS.
https://www.stealthmole.com/

Top 20 actores de ransomware en Chile y LATAM 2023



* Fuentes: Registros internos CCI Entel Digital
RR. SS.
https://www.stealthmole.com/

En general, los Top 5 de perfiles de Ransomware presenta el mayor riesgo y la mayor probabilidad de realizar un ataque. Sin embargo, siempre existe la posibilidad de registrar incidentes provocados por grupos emergentes o que se activan, única y exclusivamente, para campañas de corta duración, que tras cumplir sus objetivos no vuelven a actuar, al menos bajo el mismo nombre y TTP's.

Este último caso sin embargo, está mostrando una mayor recurrencia que se encuentra dado principalmente por una serie de filtraciones de códigos fuentes de Ransomware, como Babuk y Lockbit, entre otros. Esto ha permitido a usuarios menos experimentados adquirir herramientas con un alto nivel de desarrollo para modificarlas y utilizarlas a su favor.

Entre los perfiles que más destacan en LATAM se encuentran:

Top 5

Perfiles	Descripción	Motivación e industria
1 LockBit 113 víctimas históricas LATAM. Actividad: Septiembre de 2019 - actualidad.	Ocupa el primer lugar entre los ciberactores y es de los más peligrosos y sofisticados en su forma de ataque. Utiliza el modelo de RaaS para distribuir su código malicioso en la DDW (Deep y Dark Web).	Posicionamiento y beneficio económico. Variedad de industrias y rubros.
2 BlackCat (Alphv) 36 víctimas históricas LATAM. Actividad: Diciembre de 2021 - actualidad.	Ofrece servicios de RaaS y no se dedican a hacer ataques de manera aleatoria. Operan mediante asociados que unen esfuerzos para realizar ataques a objetivos ya perfilados.	Beneficio económico. Construcción, energía, finanzas, logística.
3 8Base 32 víctimas históricas LATAM Actividad: Mayo de 2023 - actualidad.	Son pentesters con foco en la extorsión de información a través de ataques de ransomware. Atacan a organizaciones desprevenidas. Se cree que el grupo posee un alto grado de madurez.	Posicionamiento y beneficio económico. Variedad de industrias y rubros.
4 Medusa 12 víctimas históricas LATAM. Actividad: Septiembre de 2019 - actualidad.	Se dio a conocer en 2023 por la publicación de su sitio de filtraciones en la red: Onion, donde publica los nombres de sus víctimas para extorsionarlos y amenazarlos.	Beneficio económico. Variedad de industrias y rubros.
5 ClOp 12 víctimas históricas LATAM Actividad: Febrero de 2019 - actualidad.	Está asociado con el grupo de amenazas TA505. Se enfocan en ataques de alto perfil dirigiendo sus agresivas campañas contra las grandes empresas.	Beneficio económico. Sector financiero, sanitario, manufacturero, comunicaciones y pequeñas y medianas empresas.

Comparativa de grupos 2022 - 2023

Al realizar un gráfico comparativo de las incidencias de Ransomware en LATAM entre 2022 y 2023, es posible identificar la clara dominancia de LockBit, seguido por BlackCat y 8Base que, pese a su reciente surgimiento, se ha posicionado rápidamente como uno de los Ransomware con mayor actividad histórica en LATAM.

De igual forma, hay otros actores que, aunque han detenido sus operaciones, siguen manteniendo un volumen importante de víctimas en la región, como es el caso de Conti.

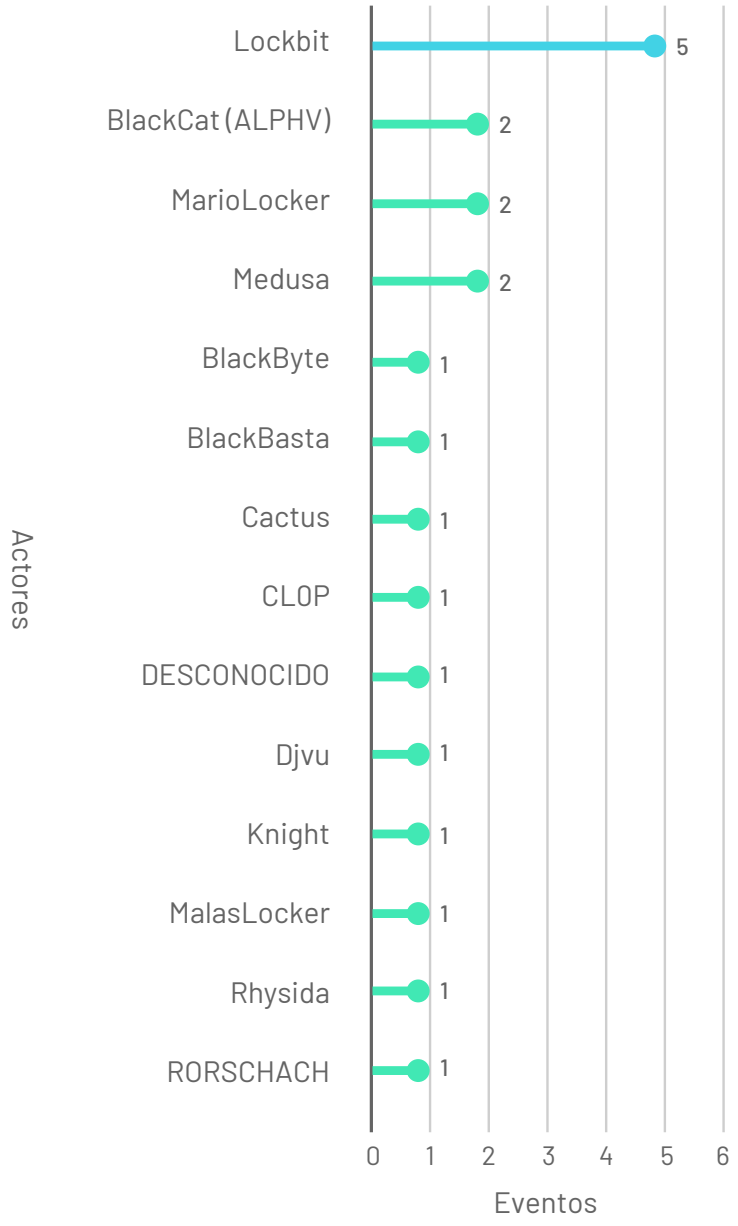
Este análisis pone en evidencia las serias falencias de seguridad de las organizaciones de la región, incluyendo a gigantes tecnológicos que previamente se encontraban posicionados como referentes de la industria. El impacto ha sido tan grande que ha afectado indirectamente a miles de clientes, generando así una ola disruptiva que los atacantes conocen y aprovechan para extorsionar con mayor tasa de éxito a sus víctimas.

Ransomware CHILE

› Grupos 2023

Al igual que el escenario en LATAM, en los registros de actividad de Ransomware en Chile, LockBit se mantiene como el operador con mayor incidencia en 2023, mientras que BlackCat y Medusa no se quedan atrás y se continúan posicionando dentro del top 5 de mayor actividad.

Actores de ransomware con mayor incidencia en Chile durante 2023



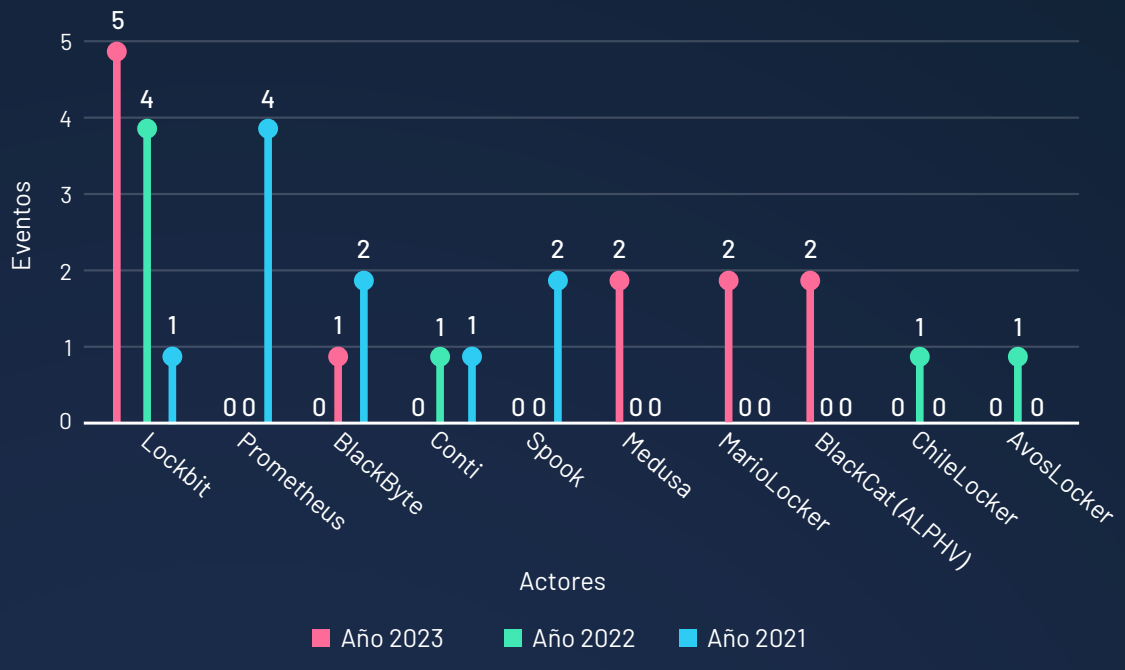
* Fuentes: Registros internos CCI Entel Digital
RR. SS.
https://www.stealthmole.com/

Comparativa de grupos 2021 - 2023

Entre 2021 y 2023, **se mantiene liderando el ranking de mayor presencia en Chile el grupo Lockbit.** El cuarto lugar se comparte entre múltiples actores, con algunos de ellos sin operaciones activas o actualmente desarticulados, como por ejemplo:

- Prometheus.
- Conti.
- Spook.

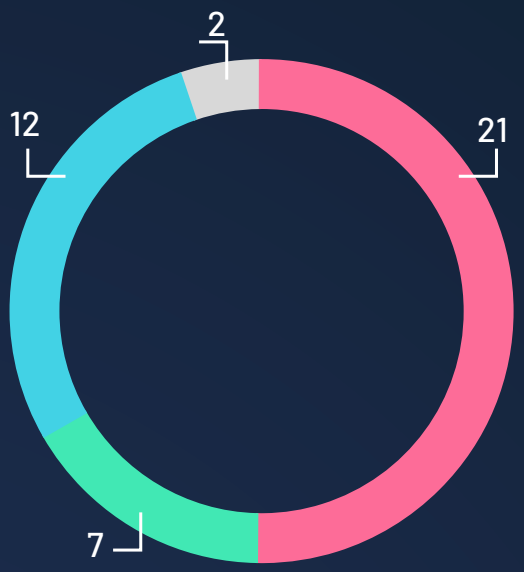
Cantidad de víctimas de ransomware en Chile entre 2021 y 2023



* Fuentes: Registros internos CCI Entel Digital
RR. SS.
https://www.stealthmole.com/

En relación con años anteriores, se observan incidentes de manera intermitente, pero a grandes rasgos se puede ver un aumento de los casos. **El año 2023 destaca sobre años anteriores con un promedio de 1,9 incidentes por mes**, casi duplicando la cantidad de incidentes de 2021, lo que coincide además con el constante aumento a nivel global.

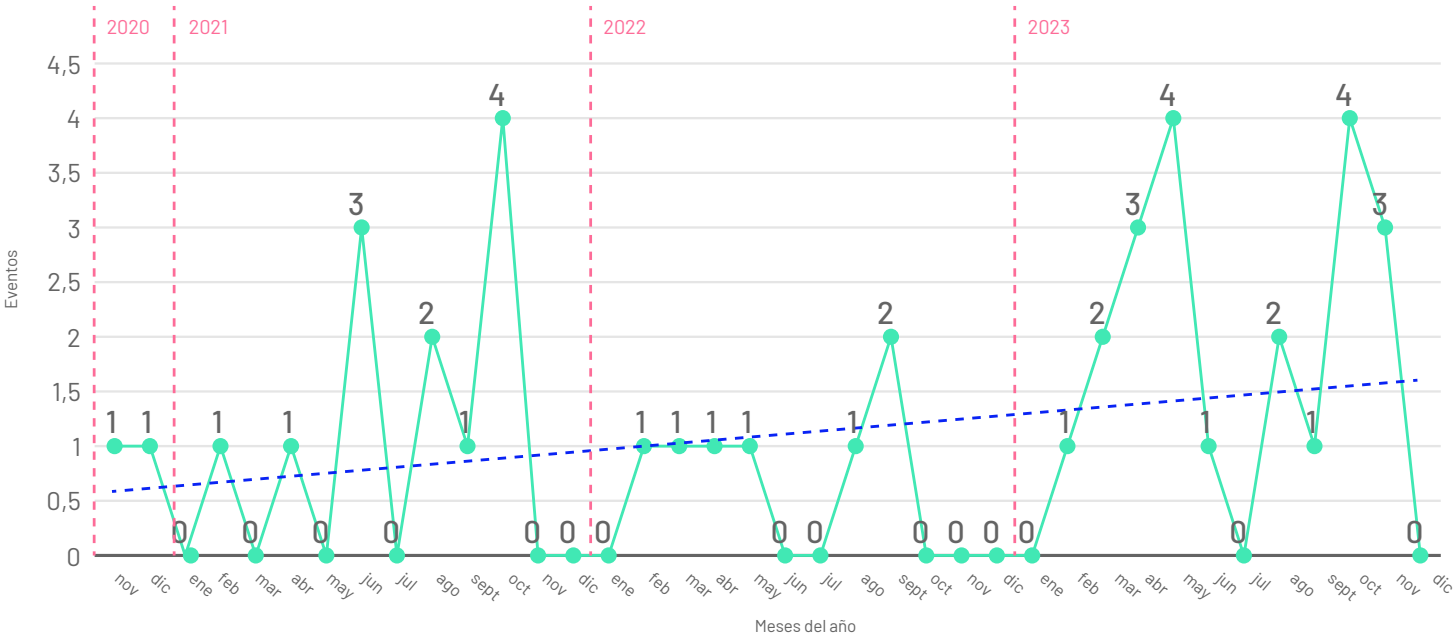
Víctimas de ransomware en Chile entre 2020 y 2023



>300%

* Fuentes: Registros internos CCI Entel Digital
RR. SS.
https://www.stealthmole.com/

Cantidad de víctimas de ransomware en Chile entre 2020 y 2023



Ante estos datos y entendiendo que cada día los grupos de Ransomware logran afectar más organizaciones de relevancia e interés nacional de forma crítica, **resulta necesario plantearnos la pregunta de qué tan preparados estamos para afrontar el futuro.**

Las grandes retribuciones monetarias que los ciberactores obtienen de cada víctima les permite capitalizar sus campañas de tal forma que ya funcionan como verdaderas empresas de hacking. Así, adquieren y mantienen grandes infraestructuras para lograr coordinar y almacenar la información secuestrada de todos sus ataques de forma segura y anónima.

Esto, sumado a las capacidades técnicas de sus miembros, da como resultado una combinación peligrosa para quienes se encuentren entre sus objetivos.

* Fuentes: Registros internos CCI Entel Digital
RR. SS.
https://www.stealthmole.com/

2.2 Panorama de Phishing

El Phishing involucra un conjunto de técnicas a través de las cuales se busca engañar a una víctima para que entregue sus datos personales. La mayoría de los ataques de este tipo comienzan con la recepción de un correo electrónico o un mensaje directo en el que el remitente se hace pasar por una entidad bancaria, una empresa u otra organización real.

+90%
de los ciberataques exitosos comienzan con un correo electrónico fraudulento

El mensaje, generalmente, busca alertar o persuadir al receptor bajo una supuesta urgencia (por ejemplo, el posible cierre de su cuenta bancaria) e incluye enlaces a un sitio web preparado por los criminales, que imita al de la empresa legítima. Una vez que la víctima entra al sitio falso, con la intención de solucionar el problema, la plataforma le pide que ingrese sus datos.

Existe una vinculación entre el Spam y el Phishing, ya que los mensajes fraudulentos suelen enviarse de forma masiva para multiplicar el número de víctimas. Actualmente, el Phishing es una de las ciberamenazas más frecuentes en el mundo. Según la CISA, **más del 90% de los ciberataques exitosos comienzan con un correo electrónico de Phishing.**

* Fuentes: https://www.cisa.gov/sites/default/files/2023-02/phishing-infographic-508c.pdf
https://www.cisa.gov/resources-tools/resources/phishing-guidance-stopping-attack-cycle-phase-one

Los objetivos que persigue una campaña de Phishing

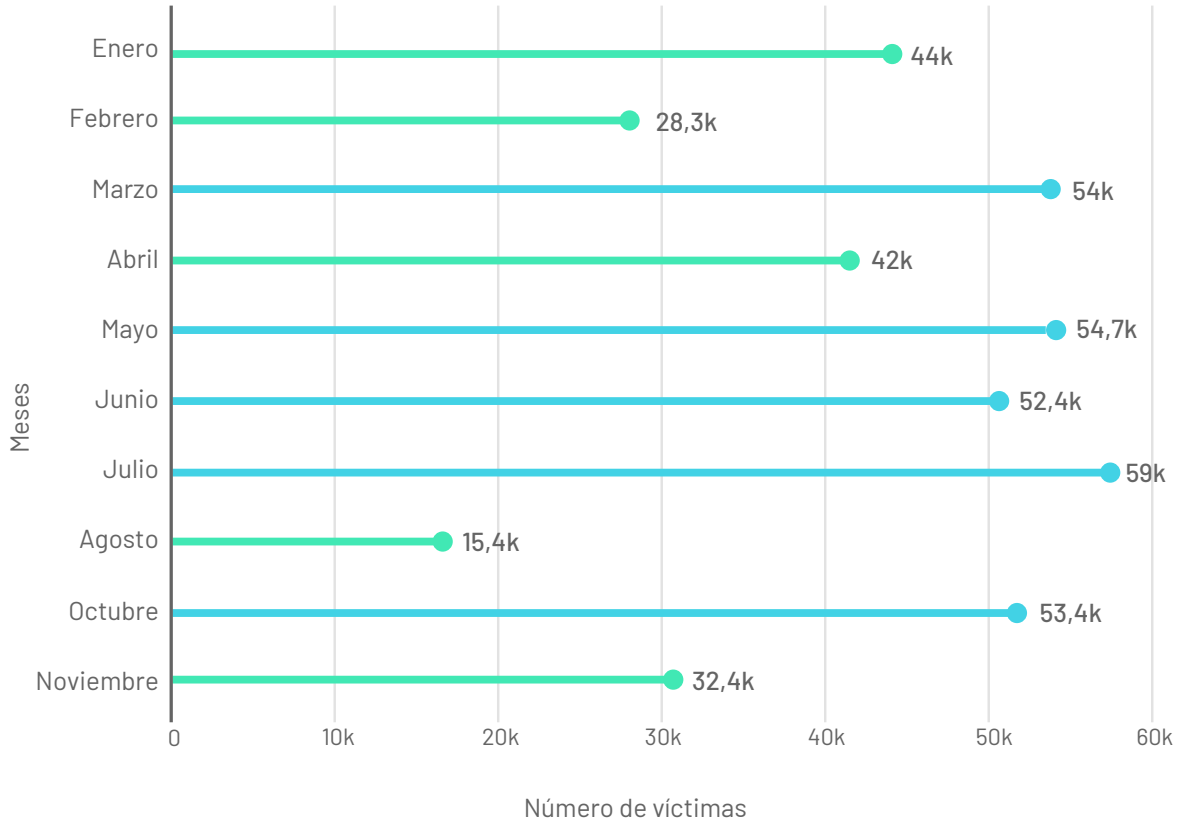
El Phishing se vale de la suplantación de identidad para conseguir:

- Robo de contraseñas.
- Tarjetas de crédito.
- Datos financieros.
- Usurpación de identidad en redes sociales.

El Phishing a nivel global

Según el portal **phishstats.info**, a noviembre de 2023 se han registrado **más de 700 mil sitios categorizados como Phishing,** lo que implica una **disminución del 37% con respecto al año anterior.** Sin embargo, sigue siendo una amenaza altamente frecuente.

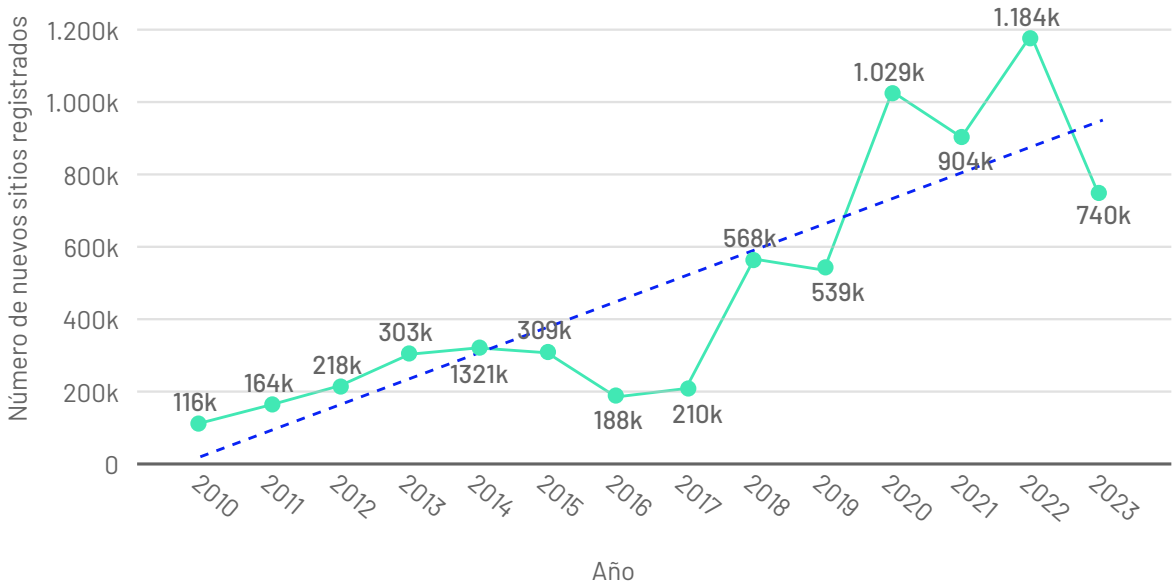
Phishing registrados a nivel Global durante 2023



* Fuentes: Registros internos CCI Entel Digital
https://phishstats.info/

El 2022 representó un récord histórico en cuanto a cantidad de sitios registrados de Phishing en los últimos 10 años.

Sitios de Phishing registrados en los últimos 10 años



* Fuentes: Registros internos CCI Entel Digital
https://phishstats.info/

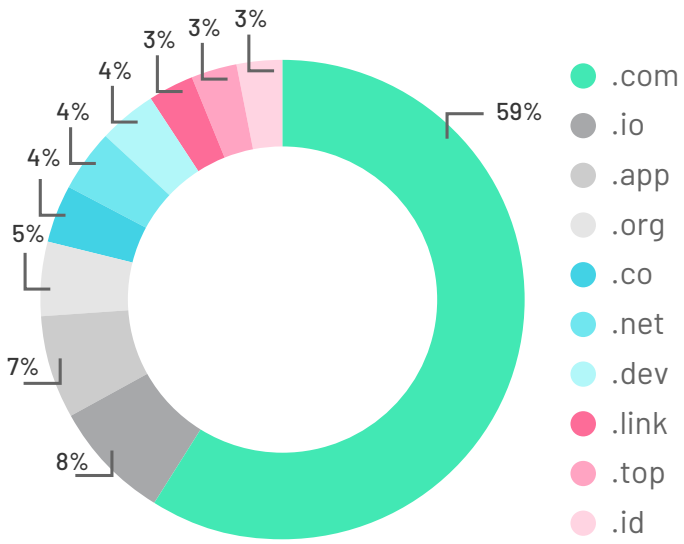
TOP TLD's (Top Level Domain)

Entre los Top Level Domain más utilizados para campañas de Phishing, destaca el **dominio .com, que abarca aproximadamente un 59% de los hallazgos.** A este lo siguen **.io con un 10% y .org con un 8%.** También resulta significativo destacar que el dominio .co, atribuido a Colombia, figura en el Top 10 del año 2023.

Considerando que la obtención de un dominio .com implica un proceso de compra que entrega una trazabilidad clara con los operadores, resulta llamativo que sean tan utilizados para este tipo de crímenes. En estos casos, para evitar ser identificados, los ciberactores recurren a diferentes mecanismos, como:

- La implantación de Phishing en sitios vulnerables legítimos que ya cuentan con un TLD conocido.
- La adquisición de los dominios deseados sin entregar datos personales reales, gracias a la alta presencia de mercado negro de tarjeras bancarias.
- La utilización de web hosting gratuito con dominios conocidos.

Top 10 TLD



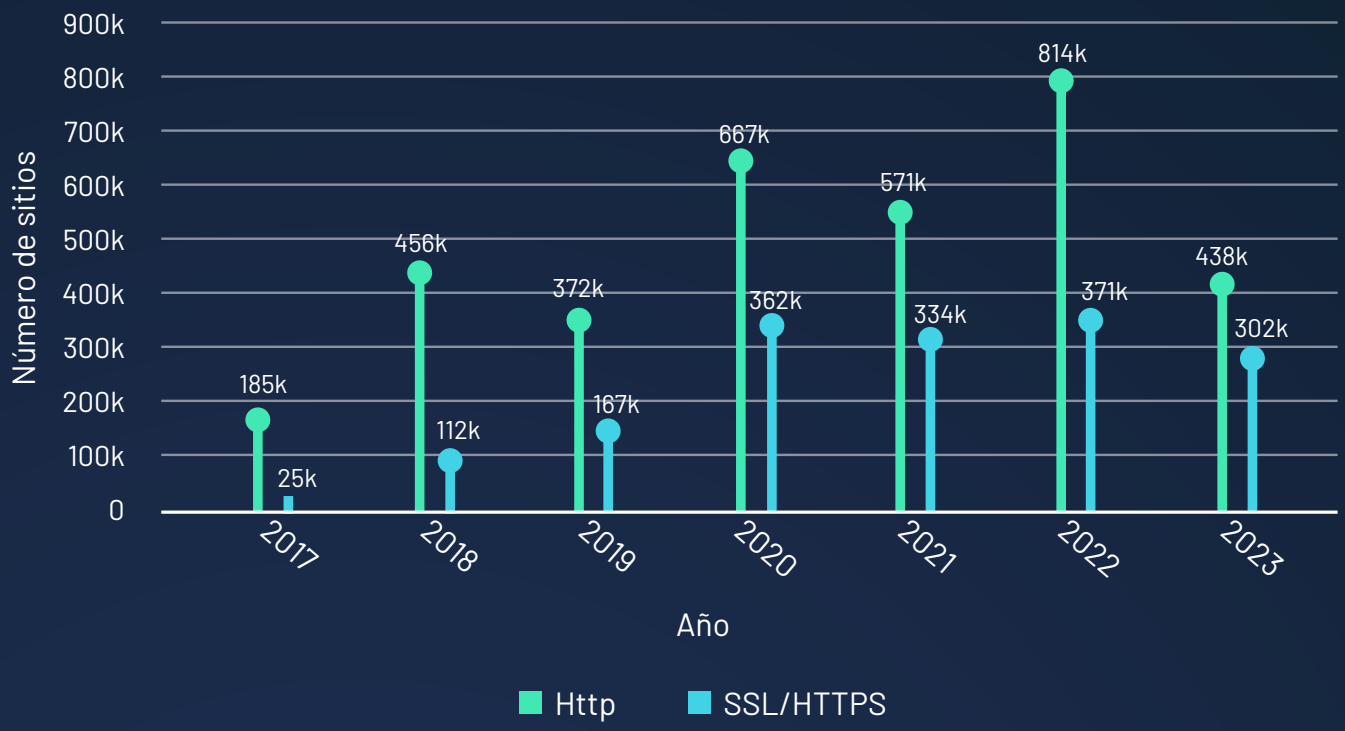
* Fuentes: Registros internos CCI Entel Digital
https://phishstats.info/

HTTP V/S HTTPS

El desarrollo constante de nuevos procesos de seguridad en internet ha obligado a los atacantes a reinventar y adaptar sus campañas, para hacerlas cada vez más convincentes. En ese sentido, el porcentaje de los ciberactores que utilizan sitios HTTPS para sus campañas de Phishing es cada vez mayor.

En 2023, el 40% del total de los atacantes de Phishing utilizó el protocolo HTTPS, lo que implica un aumento del 10% respecto a 2022.

Sitios web phishing



* Fuentes: Registros internos CCI Entel Digital
https://phishstats.info/

Para conseguir estos certificados de seguridad en sus sitios, los ciberactores han adoptado nuevos mecanismos:

- Utilización de web hosting gratuitos que cuentan con certificados.
- Implantación de sitios fraudulentos en sitios vulnerables que cuentan con certificados.
- Suplantación de tarjetas bancarias para la adquisición de certificados.
- Ataques a entidades certificadoras (CA).

2.3 Panorama de Data Leak

La filtración de datos, también conocida como Data Leak, se ha convertido en una amenaza creciente en los últimos años, ya que existe una gran variedad de ciberactores que impulsan campañas de filtración de datos, impulsados por diferentes objetivos.

› Objetivos del Data Leak

Se pueden identificar 3 principales motivaciones detrás de los ataques de Data Leak:

1. Motivación financiera

La venta de información sensible en internet puede entregar altas retribuciones monetarias. En este caso, algunos se mantienen ligados a un usuario reconocible a través de múltiples canales de venta, para aumentar su reputación y la confianza entre sus clientes.

2. Hacktivistas

Estos activistas digitales liberan información de forma gratuita, principalmente movilizados por ideales políticos o religiosos. En estos casos, el actor suele crear alias específicos para estas campañas, con el fin de evitar su seguimiento y/o rastreo.

2. Oportunismo

También existen casos en que ciertos actores aprovechan alguna vulnerabilidad por gusto y/o hobbie, sin alguna motivación mayor identificada. Estos casos suelen estar ligados a actores que atacan vulnerabilidades críticas recientes de fácil explotación o actores que, tras mantenerse por grandes cantidades de tiempo en internet, identifican vulnerabilidades en algún sitio y no dudan en explotarlas.

La evolución constante de los Alias en los Ciberactores

En los últimos años, podemos observar una renovación constante en los nombres de los actores que han realizado ataques de Data Leak. Esta renovación no implica necesariamente la aparición de nuevos actores, sino que puede responder a una de las siguientes causas:

- Actores que se crean nuevos usuarios tras las caídas, renovaciones o surgimiento de nuevos foros de mercados underground en Deep y Dark Web.
- Usuarios creados únicamente para una serie de campañas específicas.
- Cambio de alias, no vinculable al perfil anterior para evitar seguimiento.

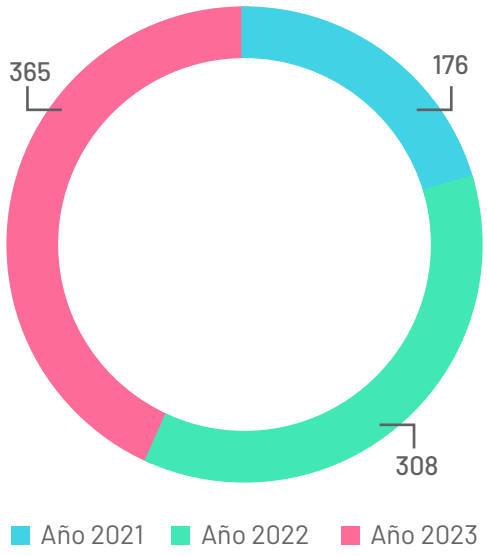
Por otra parte, existe un número de actores de renombre que persisten y se encuentran constante o esporádicamente activos bajo su mismo alias en diferentes fuentes, para ser reconocidos y aumentar progresivamente su estatus y credibilidad.

Data Leak en LATAM

El avance continuo de este tipo de amenazas se ha convertido en un fenómeno global y nuestra región no ha quedado indiferente. De hecho, entre 2021 y 2023 se observa un total de 849 incidentes de Data Leak en LATAM. Lo que es peor, únicamente en el mes de septiembre de 2023 se superó la cantidad total de víctimas de todo el año 2022.

En esa misma fecha, también se registró un aumento histórico en cantidad de grupos de Ransomware activos, lo que sugiere una correlación entre las actividades e intereses de actores maliciosos en LATAM. Todo indica que su avance no se detendrá en el futuro cercano.

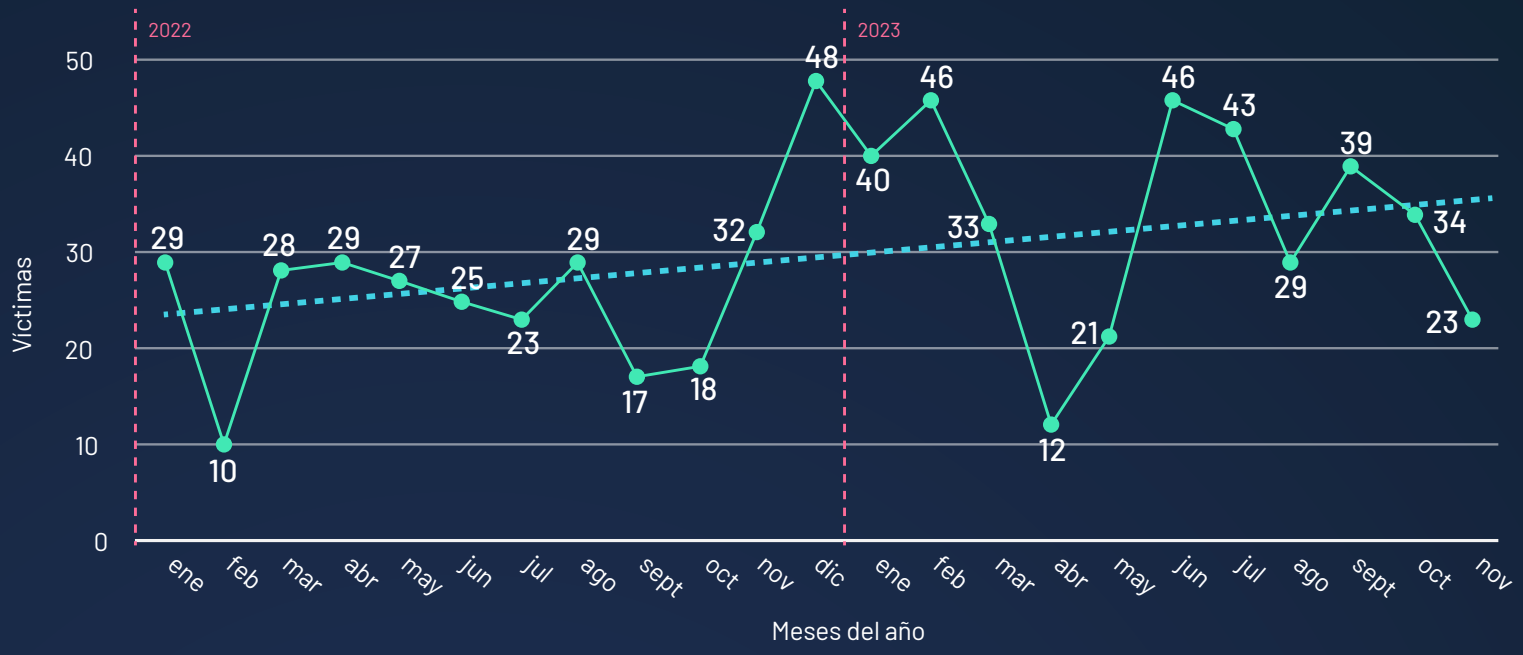
Cantidad de víctimas de Data Leak por año en LATAM entre 2021 y 2023



Más aún, al observar los datos específicos para cada mes en estos últimos años, es posible observar una tendencia en constante aumento, que tuvo su mayor alza durante diciembre de 2022 y febrero de 2023.

* Fuentes: Registros internos CCI Entel Digital
Monitoreo de DDW
RR. SS.

Cantidad de Data Leak en Chile y LATAM por mes entre 2022 y 2023



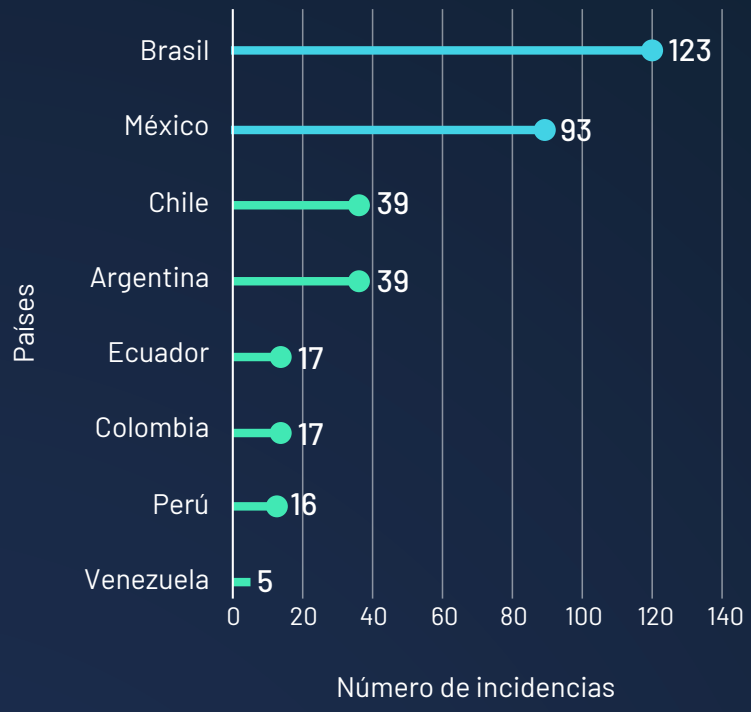
Países más afectados en 2023

Durante 2023, se mantiene un registro de 23 países afectados dentro de LATAM. Entre los países con mayor número de incidencias, destaca en primer lugar Brasil, en segundo México, en tercero Chile, en cuarto Argentina y en quinto Ecuador.

Estos 5 países abarcan el 84,9% de las víctimas en todo el territorio latinoamericano. Liderando Brasil, que por sí solo se queda con un 33,7% del total.

* Fuentes: Registros internos CCI Entel Digital
Monitoreo de DDW
RR. SS.

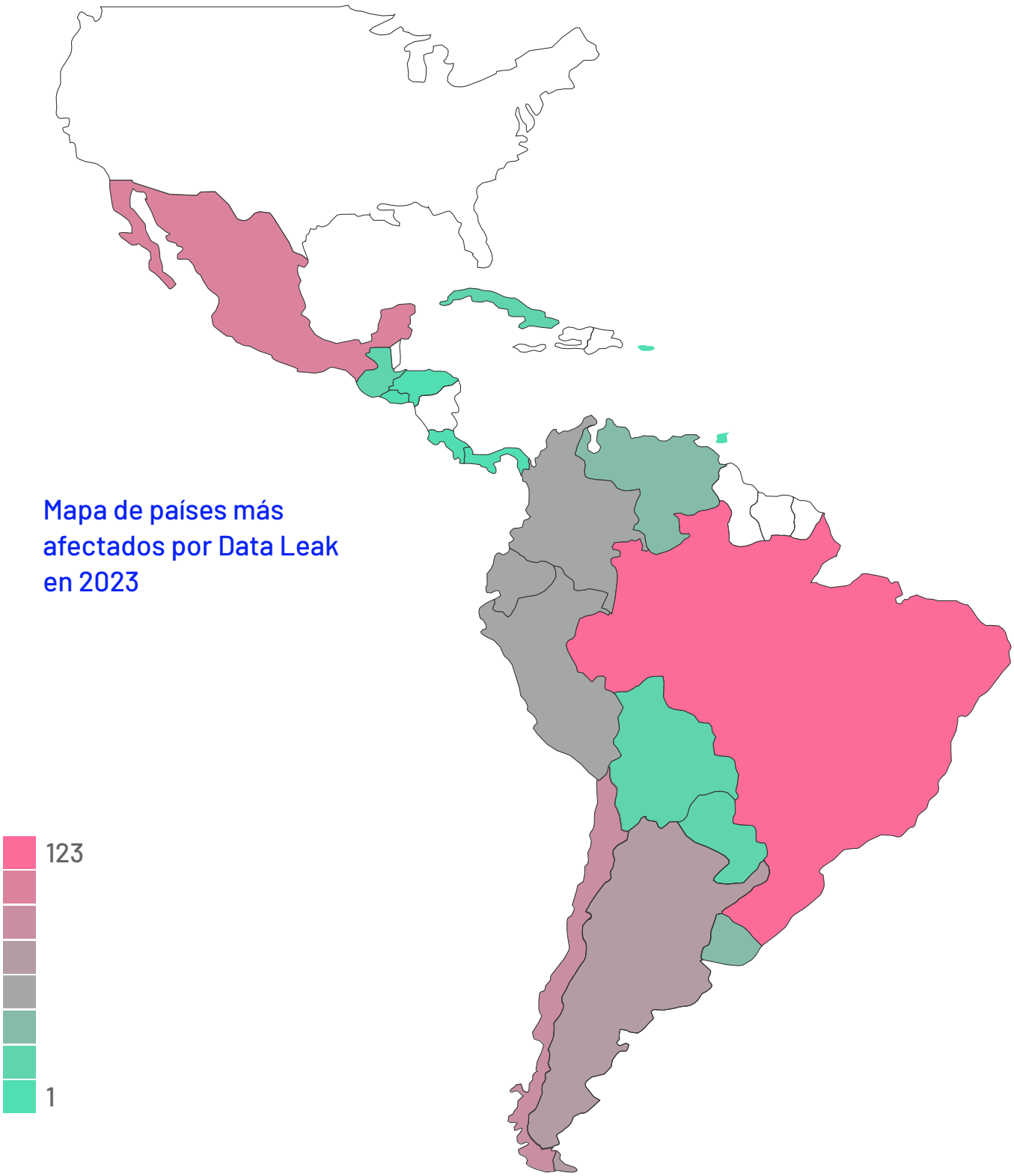
Incidencia de Data Leak en Chile y LATAM durante 2023



De cualquier manera, 22 de los 33 países que conforman nuestra región han sido afectados por este tipo de incidentes, exceptuándose países como Guyana Francesa, Surinam y algunas islas. Es importante destacar que esta distribución geográfica es muy similar a la de las amenazas de Ransomware, lo que permite comprender que factores como la densidad de población resultan atractivos para ciberactores maliciosos.

* Fuentes: Registros internos CCI Entel Digital
Monitoreo de DDW
RR. SS.

Mapa de países más afectados por Data Leak en 2023



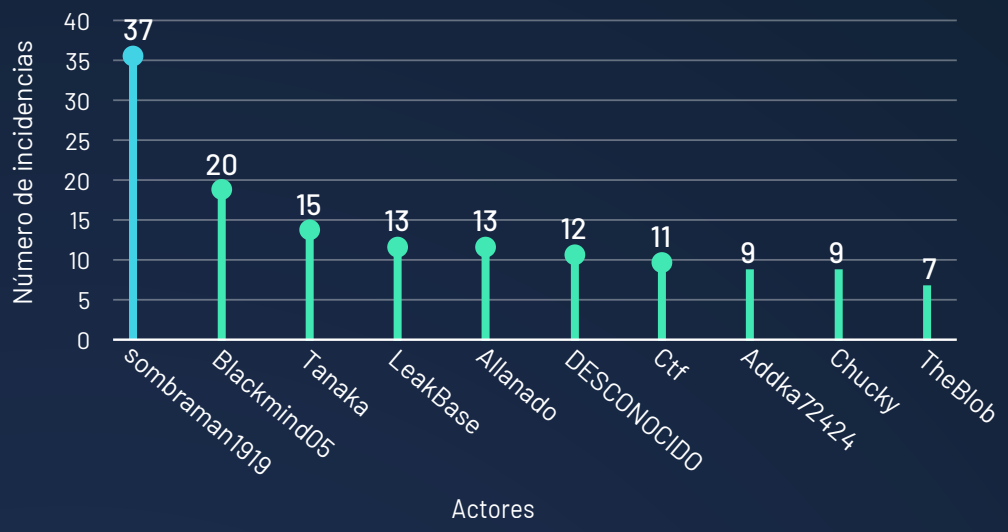
* Fuentes: Registros internos CCI Entel Digital
Monitoreo de DDW
RR. SS.

Actores de Amenaza más activos en 2023

Los actores con mayor presencia en incidentes de Data Leak en LATAM durante el año 2022 han mantenido posiciones similares durante 2023, y acumulan un largo historial de incidencias.

En total, han sido 148 alias diferentes los que han afectado a 366 organizaciones en la región. **Entre ellos destaca Sombraman1919**, quien encabeza la lista con un 51,5% de los casos anuales en Chile y LATAM.

Top 10 actores con mayor incidencia en LATAM durante 2023



A continuación destacamos los top 5 actores de Data Leak que representan mayor riesgo en la región y a los que es necesario poner atención:

* Fuentes: Registros internos CCI Entel Digital
Monitoreo de DDW
RR. SS.

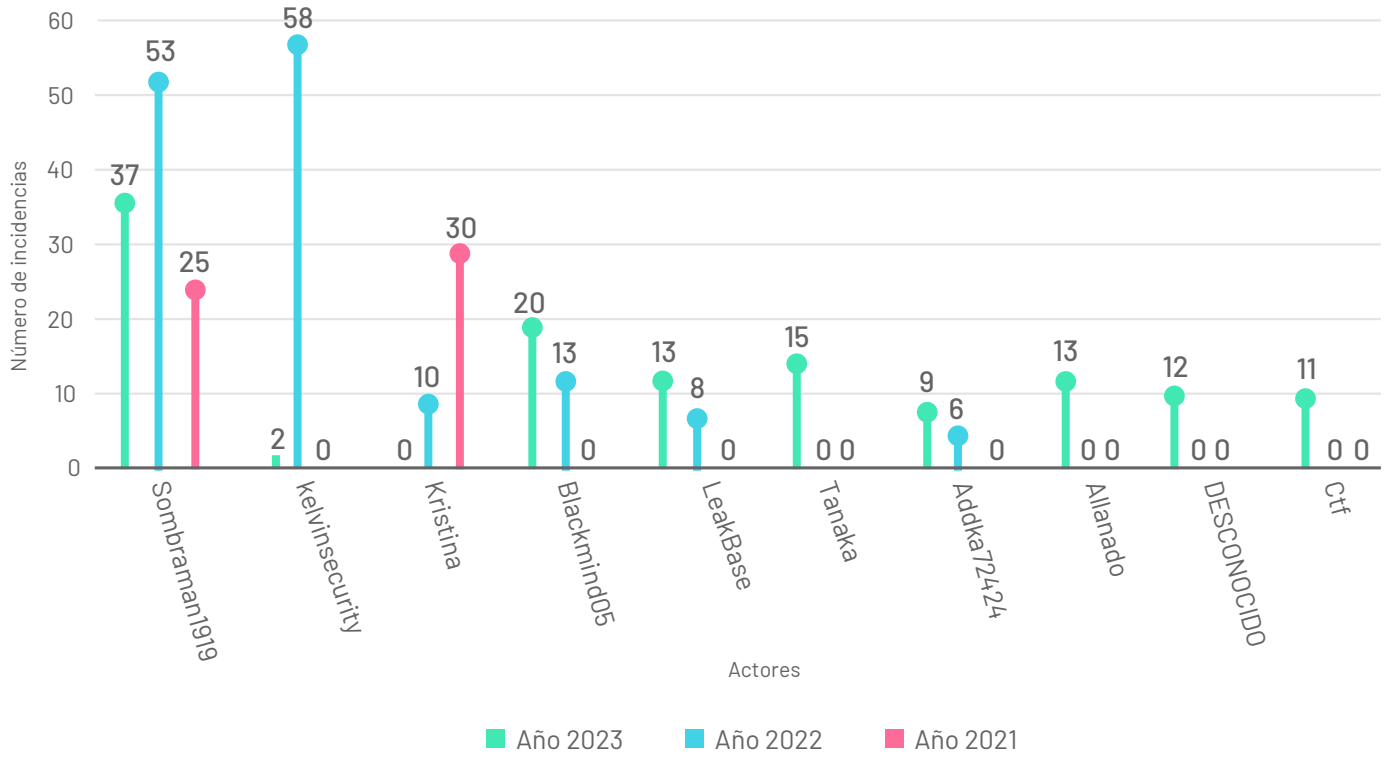
Top 5

Perfiles	Descripción	Motivación e industria
1 Sombraman1919 115 víctimas históricas LATAM. Actividad: 2012 - actualidad.	Suele publicar muestras de sus bases de datos, que posteriormente vende mediante su canal de Telegram.	Financiera. Telecomunicaciones y banca.
2 BlackMind05 33 víctimas históricas LATAM. Actividad: 2021-actualidad.	Suele publicar muestras de sus bases de datos, que posteriormente vende mediante su canal de Telegram. Similar a Sombraman1919.	Financiera. Telecomunicaciones y banca.
3 LeakBase 21 víctimas históricas LATAM Actividad: 2012-actualidad.	Grupo activo hace gran cantidad de años, altamente reconocido en foros DDW. Comparte información por su propio canal de Telegram e incluso mantiene su propio foro donde otros usuarios pueden compartir información. Uno de los principales operadores es Chucky, quien también mantiene sus propios canales de difusión y una alta reputación. Sus filtraciones se componen principalmente de SQL dumps.	Demostración de capacidades y financiera. Gobierno y retail.
4 Tanaka 15 víctimas históricas LATAM. Actividad: Desconocido-actualidad.	Mantiene objetivos alrededor de todo el mundo, presentando una gran actividad mensual, lo que da indicios de dedicación a tiempo completo en la materia, mientras que gran parte de sus publicaciones indican su origen mediante SQL dumps.	Hacktivismo y oportunismo. Gobierno y retail.
5 Allanado 13 víctimas históricas LATAM Actividad: 2023-actualidad.	Este actor presenta gran actividad desde su creación hasta la fecha, sin embargo, se desconoce si cuenta con actividad previa bajo otro alias o si corresponde a un alias desechable para una campaña temporal, mientras que sus principales objetivos se encuentran centrados en argentina, lo que podría dar referencias sobre su ubicación.	Hacktivismo y demostración de capacidades. Gobierno y educación.

* Fuentes: Registros internos CCI Entel Digital
Monitoreo de DDW
RR. SS.

En comparación con el pasado año 2022, llama la atención la baja en la actividad de nombres como KelvinSecurity y Kristina. De cualquier manera, el panorama general se mantiene similar y todo indica que estos ciberactores seguirán presentes y activos dentro de LATAM este año.

Comparativa Top 10 actores con mayor incidencia en Chile y LATAM entre 2021 y 2023

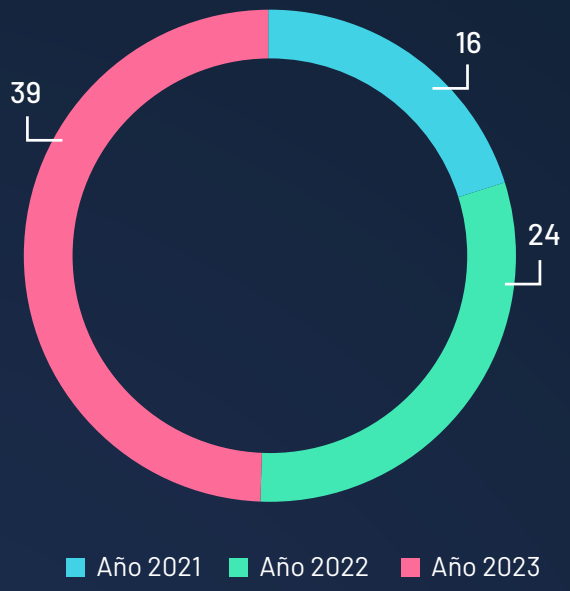


› Data Leak en Chile

Chile ha experimentado un aumento constante en el número de filtraciones de datos anuales. Así, el año 2023 ha alcanzado un promedio aproximado de 3,5 incidentes por mes, lo que implica más del doble de lo observado en el año 2021.

* Fuentes: Registros internos CCI Entel Digital
Monitoreo de DDW
RR. SS.

Víctimas de Data Leak en Chile por año



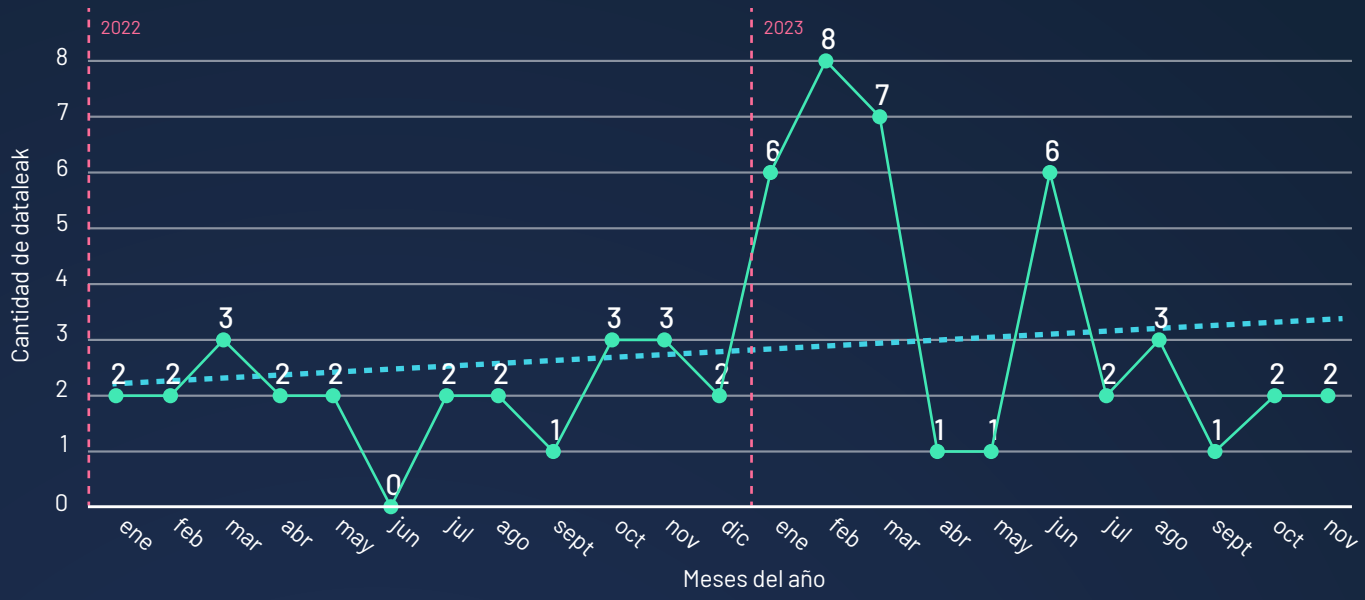
+60%
crecieron los ataques en Chile

Al revisar el detalle mensual de incidentes registrados entre enero de 2022 y noviembre de 2023, es posible observar que el punto más alto se concentra en el verano de 2022 y 2023, seguido por otro aumento en los meses de junio y julio 2023.

Considerando que estos meses representan períodos de vacaciones en el país, es posible deducir que una parte importante de los ciberactores involucrados mantienen trabajos estables durante el año y otros, posiblemente, son estudiantes.

* Fuentes: Registros internos CCI Entel Digital
Monitoreo de DDW
RR. SS.

Cantidad de Data Leak en Chile por mes entre 2022 y 2023



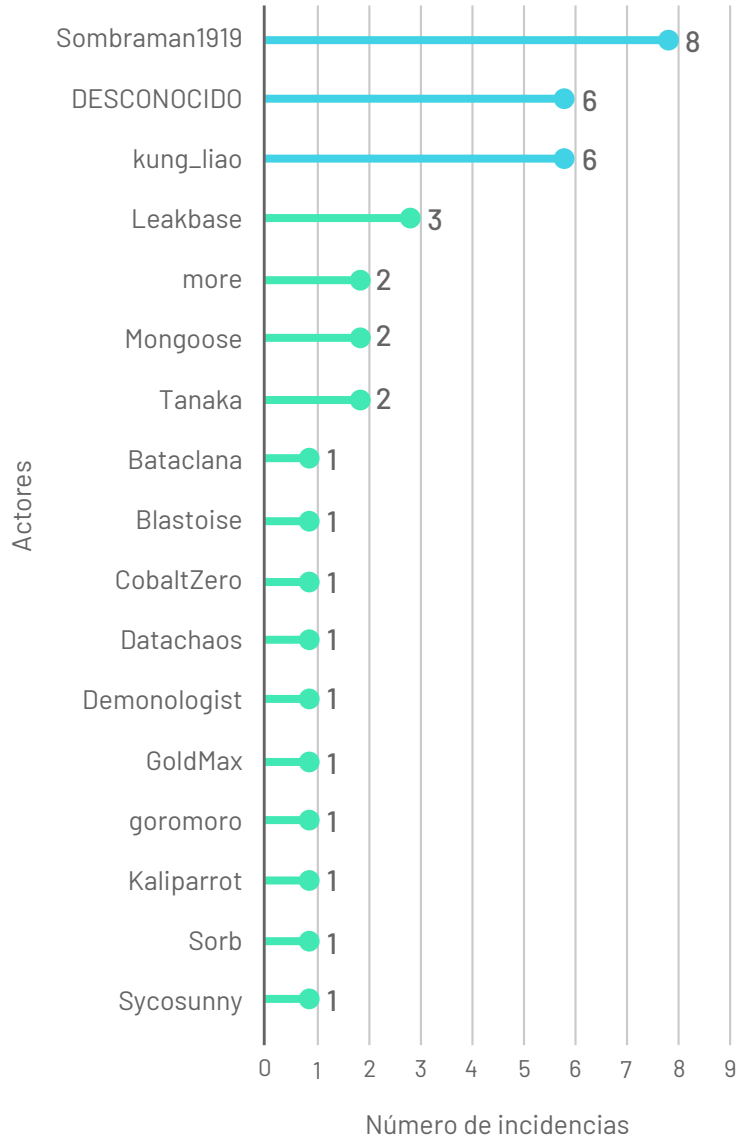
Otro aspecto a considerar es que existen claras correlaciones entre los periodos de mayor actividad de Data Leak y los de Ransomware. Este estrecho vínculo entre ambas actividades revela que, probablemente, una parte de los actores independientes que publican sus propios trabajos pueden ser también colaboradores de grupos organizados de mayor escala.

› Actores de Amenaza más activos

Tal como sucede en el resto de la región, Sombraman1919 se mantiene como el actor con mayor actividad en Chile durante este año 2023.

* Fuentes: Registros internos CCI Entel Digital
Monitoreo de DDW
RR. SS.

Actores de Data Leak en Chile durante 2023



Igualmente, existen otros ciberactores que aparecen de forma emergente o que se activan única y exclusivamente para campañas de corta duración y luego desaparecen, como es el caso del alias Kung_liao que, durante inicios de 2023, mantuvo en alerta a diferentes instituciones públicas.

Este es el Top 5 de perfiles de actores de Data Leak que representan mayor riesgo en Chile y a los que más vale la pena poner atención:

* Fuentes: Registros internos CCI Entel Digital
Monitoreo de DDW
RR. SS.

Top 5

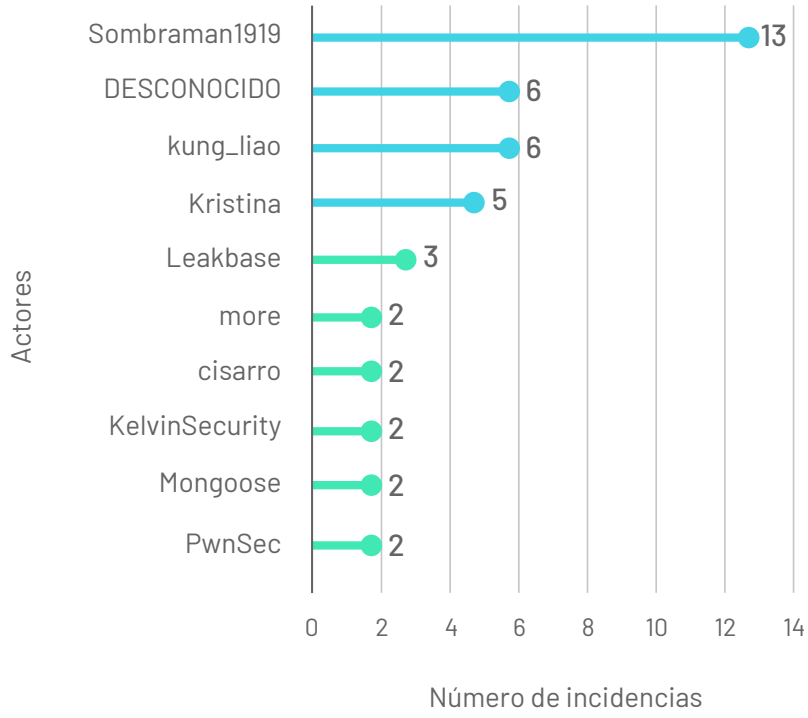
Perfiles	Descripción	Motivación e industria
1 Sombraman1919 115 víctimas históricas LATAM. Actividad: 2012 - actualidad.	Suele publicar muestras de sus bases de datos que posteriormente vende mediante su canal de Telegram, enfocado principalmente en compañías de telefonía móvil de LATAM.	Telecomunicaciones y banca. Financiera.
2 LeakBase 21 víctimas históricas LATAM. Actividad: 2012-actualidad.	Grupo activo hace gran cantidad de años, altamente reconocido en foros DDW. Comparte información por su propio canal de Telegram e incluso mantiene su propio foro donde otros usuarios pueden compartir información. Uno de los principales operadores es Chucky, quien también mantiene sus propios canales de difusión y una alta reputación. Sus filtraciones se componen principalmente de SQL dumps.	Demostración de capacidades y financiera. Retail y Gobierno.
3 Kung_Liao 6 víctimas históricas LATAM Actividad: Enero 2023-Marzo 2023.	Utilizado para campañas de corta duración. Marcó tendencia a comienzo de año debido al ataque directo a instituciones nacionales de gobierno. Su actividad fue breve, pero resultó ser de relevancia nacional.	Hacktivismo y financiera. Gobierno y TI.
4 More 2 víctimas históricas LATAM. Actividad: Junio 2023 - Actualidad.	Presenta una baja actividad, pero completamente dirigida a Chile. Dado que aún se mantiene activo, es esperable que continúe con sus ataques a otras instituciones nacionales, por lo que su interés da luces sobre su posible ubicación geográfica.	Hacktivismo. Gobierno.
5 Desconocido N/A N/A	Corresponde a aquellos Data Leaks que han sido identificados de una u otra manera, pero a los que no se les ha logrado asignar un alias responsable.	N/A N/A

* Fuentes: Registros internos CCI Entel Digital
Monitoreo de DDW
RR. SS.

Este Top 5 de actores con mayor presencia en Chile mantiene nombres similares a los que se han destacado en años anteriores. Sin embargo, no todos ellos se encuentran centrados específicamente en el país. Por ejemplo, Chucky del grupo LeakBase se encuentra en los últimos lugares en el listado, pero participa de un grupo con gran actividad a nivel latinoamericano.

Por otra parte, el tipo de instituciones afectadas permite reconocer la existencia de otras motivaciones, más que solo financieras. En ese sentido, considerando que los hacktivistas o actores motivados por ideales políticos suelen ser usuarios que se sienten identificados con problemáticas del país, sus ataques entregan referencias sobre su posible ubicación geográfica.

Actores de Data Leak en Chile entre 2021 y 2023



* Fuentes: Registros internos CCI Entel Digital
Monitoreo de DDW
RR. SS.

CAPÍTULO 3

Panorama Vulnerabilidades

Cada año, la tecnología avanza a pasos agigantados, entregando nuevos productos y servicios que facilitan el trabajo de numerosas empresas. Sin embargo, estos software y aplicativos a menudo presentan fallas que, en manos equivocadas, son aprovechadas para causar violaciones de seguridad e impactar negativamente a las organizaciones que los utilizan.

Estas fallas son identificadas por los proveedores correspondientes mediante un CVE (Common Vulnerabilities and Exposures) y luego son notificadas a sus clientes para que tomen medidas y realicen las actualizaciones proporcionadas.

Sin embargo, a pesar de estas notificaciones, muchas veces las empresas y administradores de estos servicios no actualizan sus aplicativos a tiempo. En ocasiones, esto se debe a que priorizan la operación antes que la seguridad, ya que una pausa en las actividades diarias puede resultar en grandes pérdidas económicas.

Los ciberactores comprenden claramente este escenario y aprovechan las fallas como una puerta de entrada y vector de ataque para intrusiones a gran escala, razón por la cual logran monetizar sus operaciones.

Instituciones y organismos mundiales

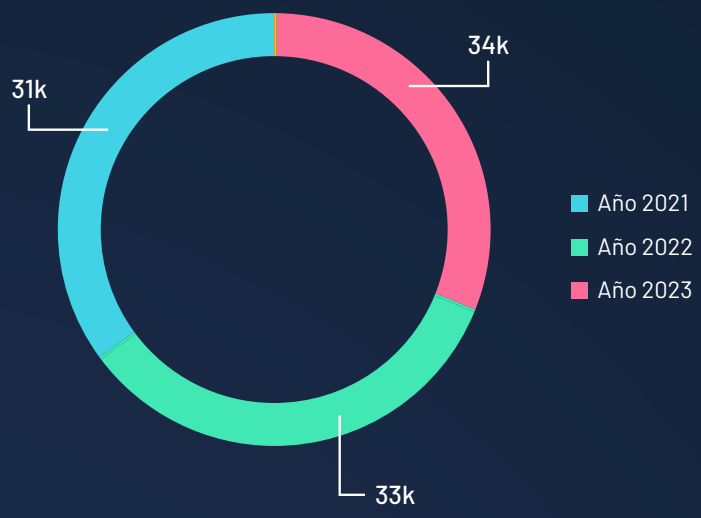
Actualmente, diversas instituciones mundiales velan por la ciberseguridad. Entre ellas, destaca el trabajo de la Agencia de Seguridad Cibernética y de la Infraestructura (CISA) y el del Instituto Nacional de Estándares y Tecnología (NIST), que informan sobre nuevas vulnerabilidades a la comunidad para que se tomen las acciones correspondientes.

El Instituto Nacional de Estándares y Tecnología (NIST):

Es el repositorio de datos de gestión de vulnerabilidades del gobierno de EE.UU. Cuenta con una base de datos nacionales de vulnerabilidades (NVD), que están basados en estándares representados por el protocolo de automatización de contenido de seguridad.

De este repositorio, podemos analizar los datos desde 2021 hasta el 11 de noviembre de 2023, los cuales reflejan un aumento del 12% en la cantidad de CVE en 2023 en comparación con 2021, y un aumento del 2% respecto a 2022.

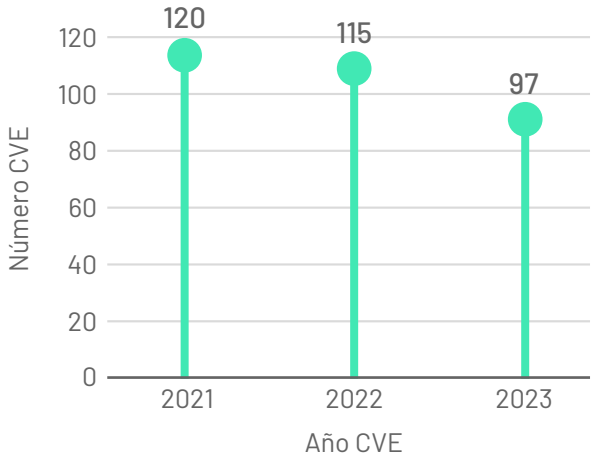
Total de CVE publicados por el NIST NVD



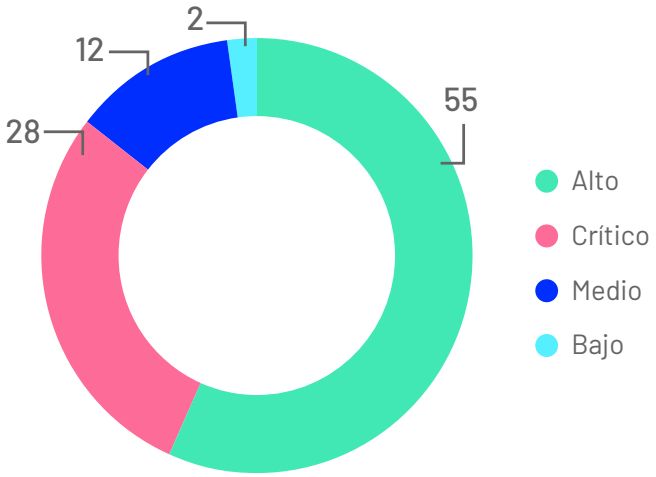
* Fuentes: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
https://nvd.nist.gov/vuln

Si cruzamos la información entregada por la base de datos nacional de vulnerabilidades (NVD) con el catálogo de vulnerabilidades más explotadas (KEV), con datos desde 2021 hasta el 8 de noviembre de 2023 que proporciona la CISA, podemos ver que, de los 97 CVE catalogados como más explotados del 2023, 28 son de severidad Crítica, 55 de severidad Alta, 12 de severidad Media y 2 de severidad Baja.

Total de CVE por año del catálogo KEV



Criticidad de los CVE más explotados del 2023

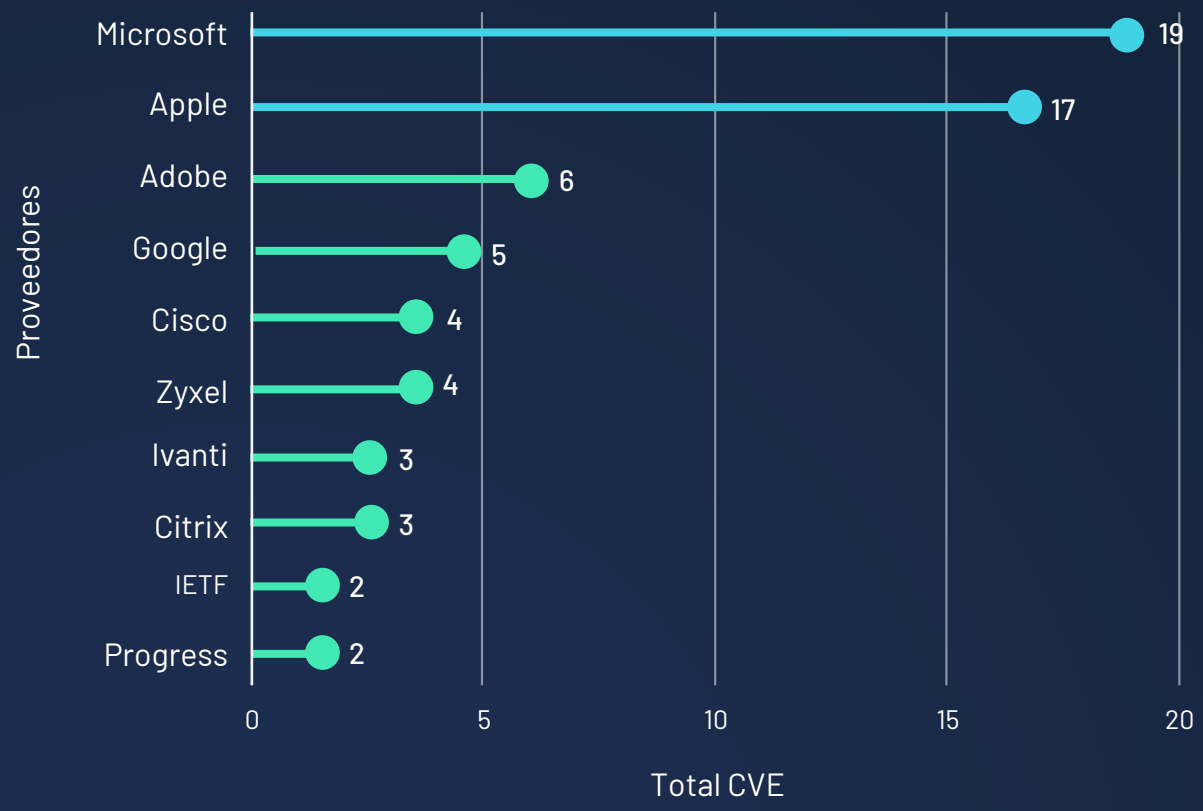


* Fuentes: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
https://nvd.nist.gov/vuln

Ahora, de las 97 vulnerabilidades identificadas, se extraen los siguientes proveedores de tecnologías.

Microsoft lidera con 19 vulnerabilidades dentro del catálogo KEV, seguido por Apple (17) y Adobe (6).

Top 10 de CVE por proveedores de tecnología



* Fuentes: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
https://nvd.nist.gov/vuln

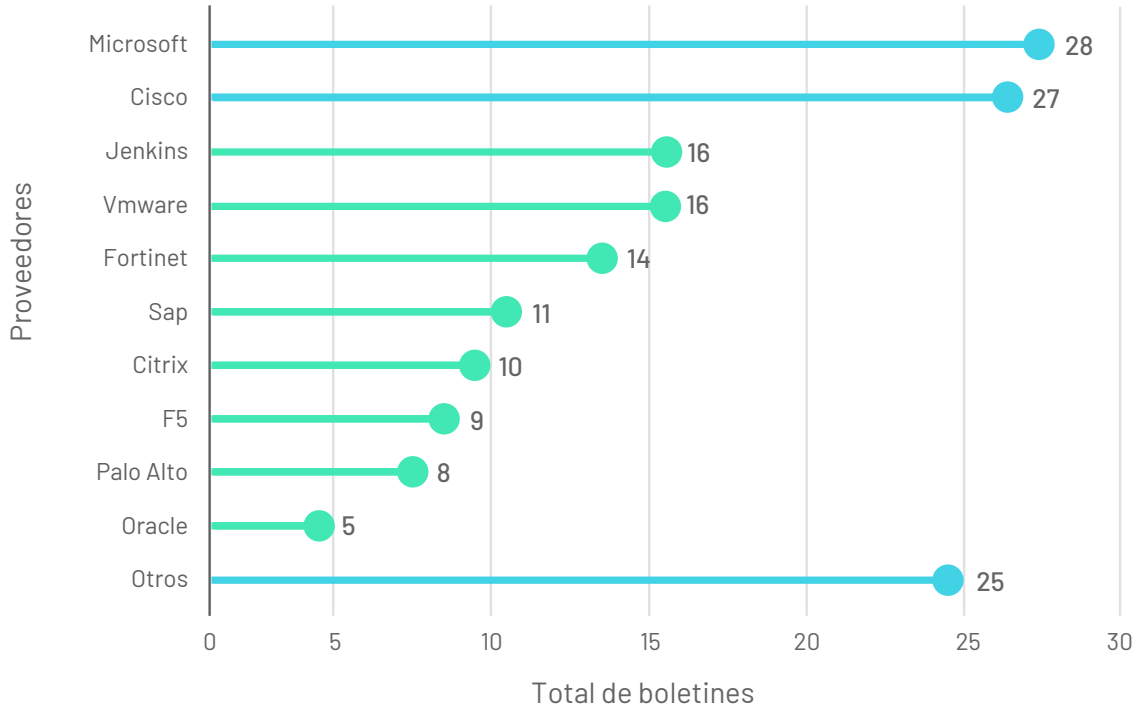
Entel

Como Centro de Ciberinteligencia de Entel, también llevamos un registro de las vulnerabilidades identificadas, las cuales informamos a nuestros clientes a través de los boletines de amenazas que confeccionamos a diario.

Hasta el día 16 de noviembre del 2023, contabilizamos la publicación de 2,347 vulnerabilidades registradas durante este mismo año, las cuales fueron distribuidas en 169 boletines.

Estas vulnerabilidades corresponden a los principales proveedores de tecnología como Microsoft, Cisco, VMware, Palo Alto, F5, Fortinet, SAP, entre otros.

Total de boletines por proveedores de tecnología



* Fuentes: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
https://nvd.nist.gov/vuln

Los datos revelan un aumento constante en la cantidad de CVE registrados anualmente, evidenciando la necesidad de una gestión de riesgos enfocada y la participación activa de los proveedores tecnológicos y centros de ciberinteligencia, como el Centro de Ciberinteligencia de Entel, que resulta esencial para abordar y mitigar eficazmente estas amenazas en constante evolución.

Al igual que en el catálogo de las vulnerabilidades más explotadas, Microsoft lidera con 28 boletines asociados a parches de CVE, seguido por Cisco (27), Jenkins (16) y VMware (16).

La presencia de vulnerabilidades en software y aplicativos representa una amenaza constante, exacerbada por la falta de actualizaciones oportunas por parte de las organizaciones, muchas veces debido a la priorización de la operación sobre la seguridad.

Los datos revelan un aumento constante en la cantidad de CVE registrados anualmente, evidenciando la necesidad de una gestión de riesgos enfocada y la participación activa de los proveedores tecnológicos y centros de ciberinteligencia, como el Centro de Ciberinteligencia de Entel, que resulta esencial para abordar y mitigar eficazmente estas amenazas en constante evolución.

* Fuentes: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
https://nvd.nist.gov/vuln

CAPÍTULO 4

Panorama de Infraestructura Crítica

En la medida que diferentes áreas de la industria, la administración política y la economía en general se apoyan en innovaciones tecnológicas para desarrollarse, **la ciberseguridad se vuelve esencial para proteger sectores vitales como energía, telecomunicaciones y otros servicios básicos.**

Así, resulta necesario comprender las tácticas de los ciberdelincuentes y establecer un marco sólido de protección a escala mundial. Esto permite desarrollar soluciones basadas en mejores prácticas de ciberseguridad y colaboración público-privada, para aumentar la resiliencia en el entorno digital en todas las regiones.

A la vez, resulta importantísimo considerar leyes y regulaciones específicas, **como la Ley chilena N° 21.542, que define a las infraestructuras críticas en nuestro país,** considerando la creciente dependencia de tecnologías de la información en todo el mundo.

Infraestructura crítica

No es necesario ir muy lejos para observar cómo la infraestructura crítica de nuestro país ha sido impactada en diversas ocasiones, como en el emblemático caso que sacudió a una entidad bancaria en el año 2018. En este incidente, un grupo de ciber actores de origen norcoreanos consiguió (según comunicados oficiales) sustraer alrededor de US$10 millones a través de transacciones autorizadas.

Asimismo, en 2020 el Ransomware REvil (también conocido como Sodinokibi) afectó a otra entidad bancaria nacional, que tuvo que mantener la mayoría de sus sucursales cerradas durante al menos cuatro días, provocando una indisponibilidad generalizada en sus sistemas y servicios al cliente.

A raíz de estos incidentes, la Comisión de Economía acordó solicitar al ejecutivo la aplicación de la máxima urgencia al mensaje en segundo trámite que establece normas sobre delitos informáticos, derogando la ley N° 19.223 y modificando otros cuerpos legales con el objetivo de adaptarlos al convenio de Budapest.

Más tarde, el 19 de septiembre del año 2022, el grupo de hackers conocido como Guacamaya filtró cerca de 400.000 correos electrónicos de organizaciones de las FF. AA. en Chile.

Del mismo modo, en el transcurso de este año 2023, tres organizaciones de nuestro país han sufrido las acciones de un presunto ciberactor chileno, de alias “Kung_Liao”:

* Fuentes: Registros internos CCI Entel Digital
https://www.stealthmole.com/
https://portal.cci-entel.cl/Threat_Intelligence/Boletines/1693/

Los ataques de “Kung_Liao” en 2023

Sector de la organización	Descripción
Financiero	Impactó sus sistemas mediante una vulnerabilidad de inyección SQL.
Financiero	Publicó una supuesta shell obtenida a través de SQLMap y compartió el presunto endpoint vulnerable.
Tecnología y ciberseguridad	Publicó un acceso a la infraestructura de Microsoft de la organización afectada y expuso información de usuarios corporativos.

Por otra parte, en la última semana de mayo de 2023, se reveló que una organización de las FF. AA. de Chile fue objetivo del grupo de Ransomware Rhysida. Los ciberatacantes publicaron en su sitio de filtraciones aproximadamente 360.000 documentos, afirmando que esta cantidad solo representa el 30% de la información sustraída.

En ese sentido, son cada vez más las organizaciones estatales y nacionales cuyo funcionamiento se ve amenazado por ciberataques.

* Fuentes: Registros internos CCI Entel Digital
https://www.stealthmole.com/
https://portal.cci-entel.cl/Threat_Intelligence/Boletines/1693/

Ataques a Infraestructura Crítica por Área

Petróleo y Gas

Desde enero de 2022 hasta noviembre de 2023, se ha identificado un total de 88 ataques de Ransomware dirigidos a la industria del petróleo a nivel global. Estos incidentes son un recordatorio de la vulnerabilidad que poseen las infraestructuras críticas frente a las amenazas cibernéticas.

En 2022, se registraron 40 de estos ataques, que dan cuenta del interés de los ciberdelincuentes a apuntar a sectores vitales para la economía y el funcionamiento de las sociedades.

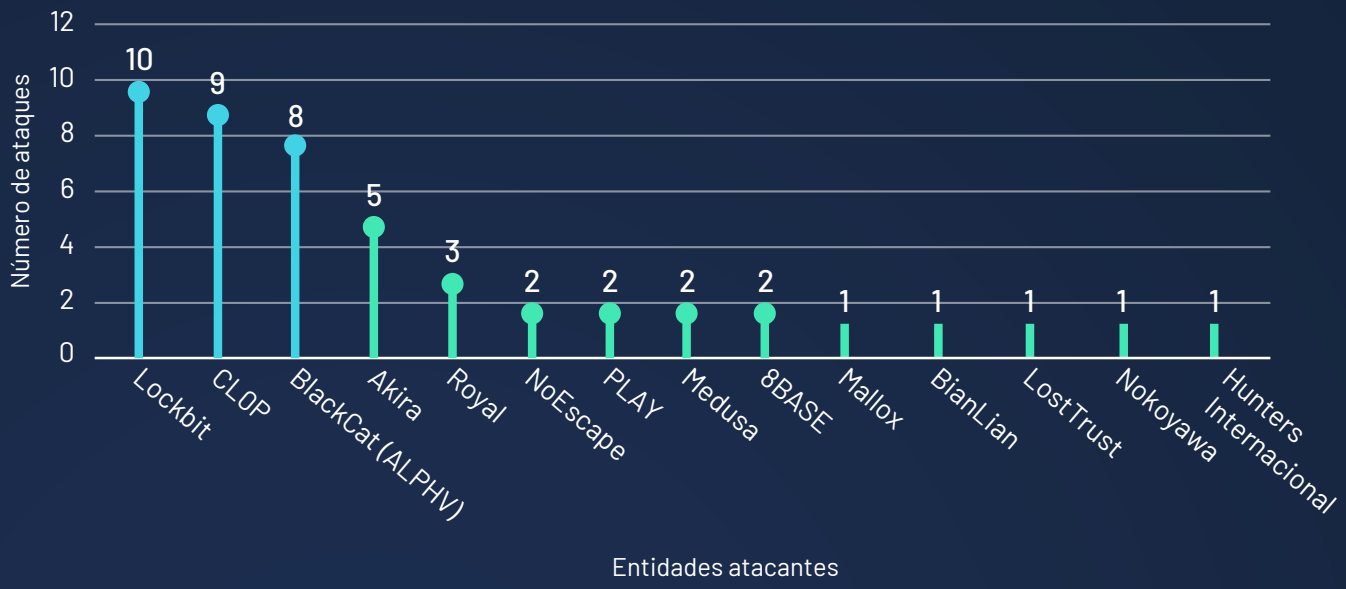
Cada uno de estos ataques no solo implicó costos económicos significativos en términos de rescate potencial y pérdida de ingresos, sino que pudo haber tenido serias repercusiones en la seguridad energética y la estabilidad de las operaciones diarias.

Hasta noviembre de 2023, la industria fue golpeada por 48 nuevos ataques. Este dato eleva la necesidad de que las empresas del sector petrolero, y de infraestructuras críticas en general, refuercen sus medidas de ciberseguridad. Esto incluye:

- La implementación de firewalls avanzados.
- La actualización regular de software y hardware.
- La capacitación de empleados en ciberseguridad.
- La colaboración con entidades gubernamentales y privadas en materia de ciberinteligencia para anticiparse a posibles amenazas.

* Fuentes: Registros internos CCI Entel Digital
https://www.stealthmole.com/
https://portal.cci-entel.cl/Threat_Intelligence/Boletines/1693/

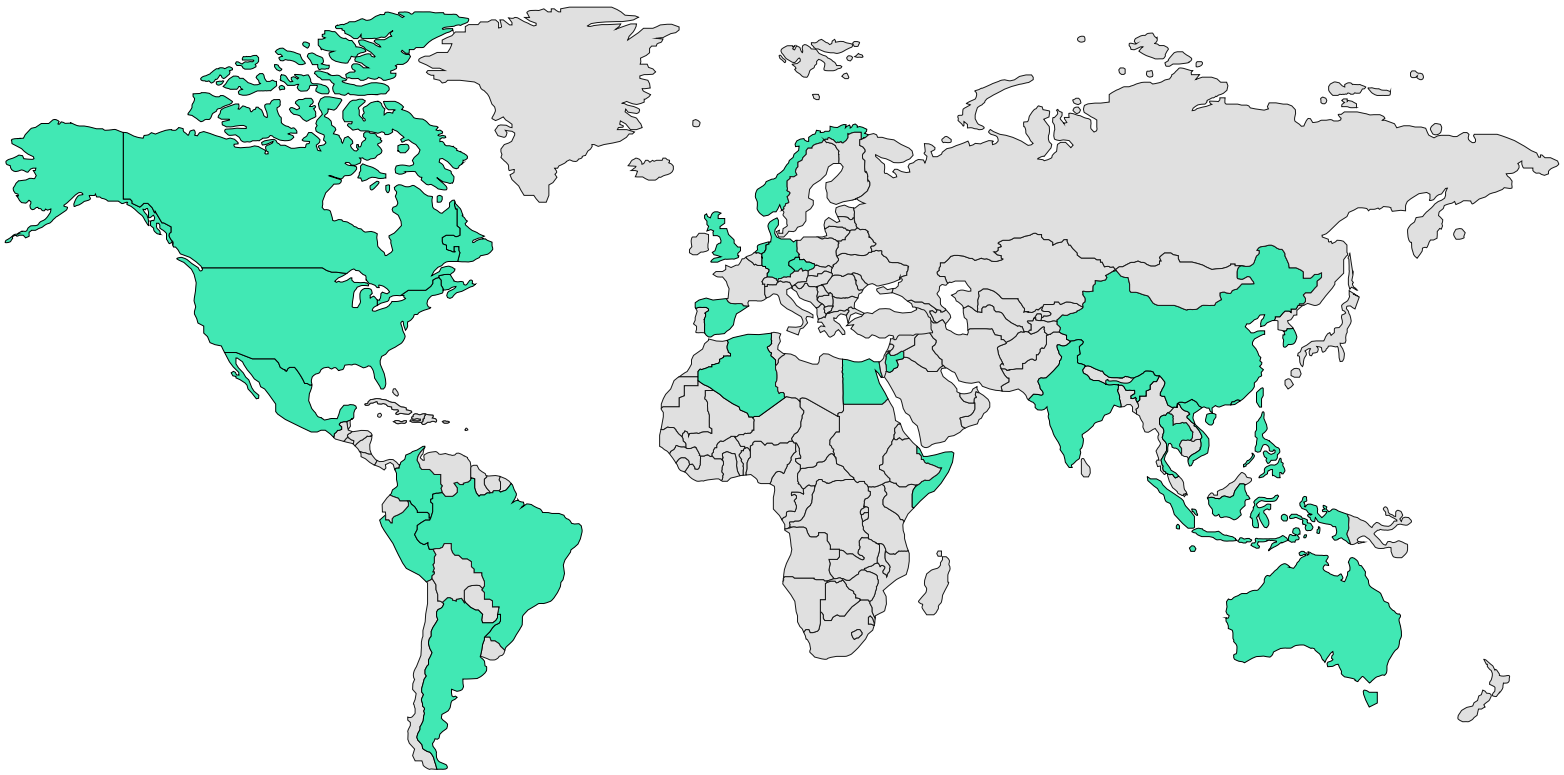
Ataques por ransomware Petróleo 2023



Empresas e instituciones deben estar preparadas para reaccionar rápidamente a los incidentes de seguridad, minimizar el daño y recuperarse con la mayor eficacia posible, pues la ciberseguridad en las infraestructuras críticas se ha convertido en una cuestión no sólo de seguridad empresarial, sino de seguridad nacional e internacional.

* Fuentes: Registros internos CCI Entel Digital
https://www.stealthmole.com/
https://portal.cci-entel.cl/Threat_Intelligence/Boletines/1693/

Países afectados industria petróleo-gas



Durante el año 2022, en nuestra región 4 organizaciones de la industria del petróleo y gas sufrieron ataques de Ransomware. Mientras tanto, hasta noviembre del año 2023, se ha detectado la misma cantidad de 4 organizaciones afectadas en LATAM.

Estos incidentes no sólo interrumpen las operaciones, sino que también pueden tener graves repercusiones en términos de seguridad energética y pérdida de confianza de los inversores y clientes.

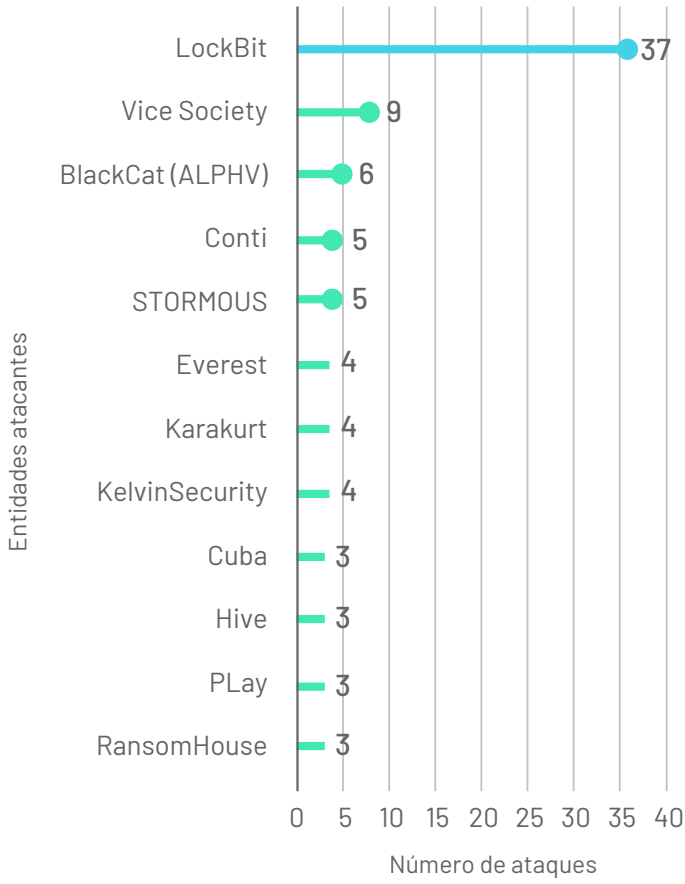
* Fuentes: Registros internos CCI Entel Digital
https://www.stealthmole.com/
https://portal.cci-entel.cl/Threat_Intelligence/Boletines/1693/

Gobierno

En los últimos dos años, se han detectado 188 ataques de Ransomware a entidades gubernamentales a nivel global, un indicador alarmante de la creciente amenaza que este tipo de ataques representa para los órganos de gobierno.

Durante el año 2022, se registraron 99 ataques diferentes. Entre ellos, **LockBit destacó como el actor más prolífico.**

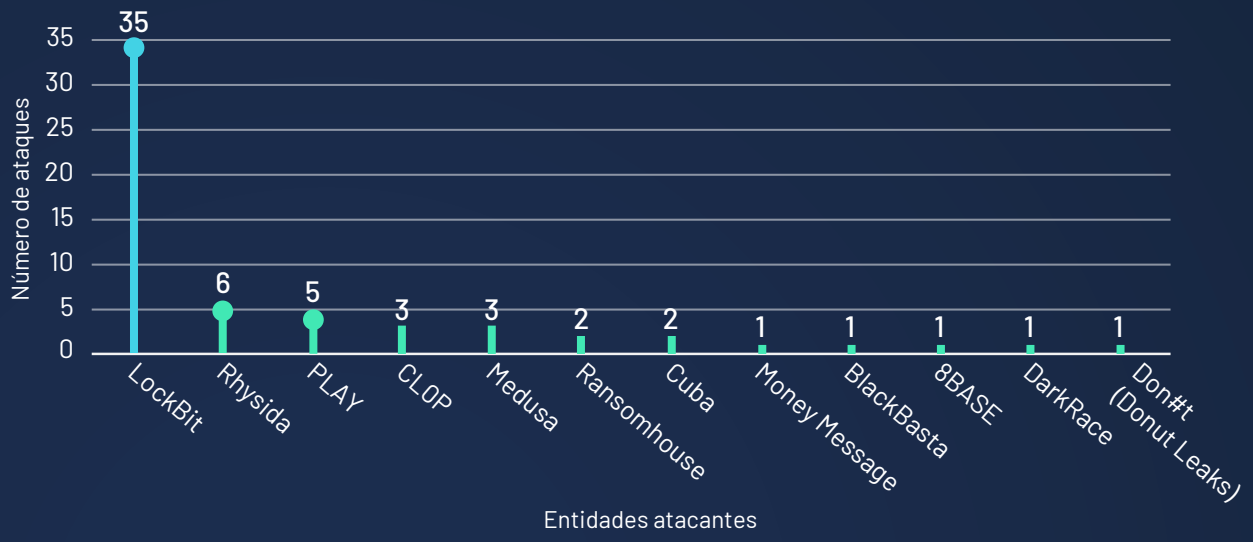
Ataques por ransomware Gobierno 2022



* Fuentes: Registros internos CCI Entel Digital
https://www.stealthmole.com/
https://portal.cci-entel.cl/Threat_Intelligence/Boletines/1693/

Hasta el mes de noviembre, se registraron 89 ataques a entidades gubernamentales 2023. Nuevamente, LockBit resultó el nombre más común.

Ataques por ransomware Gobierno 2023



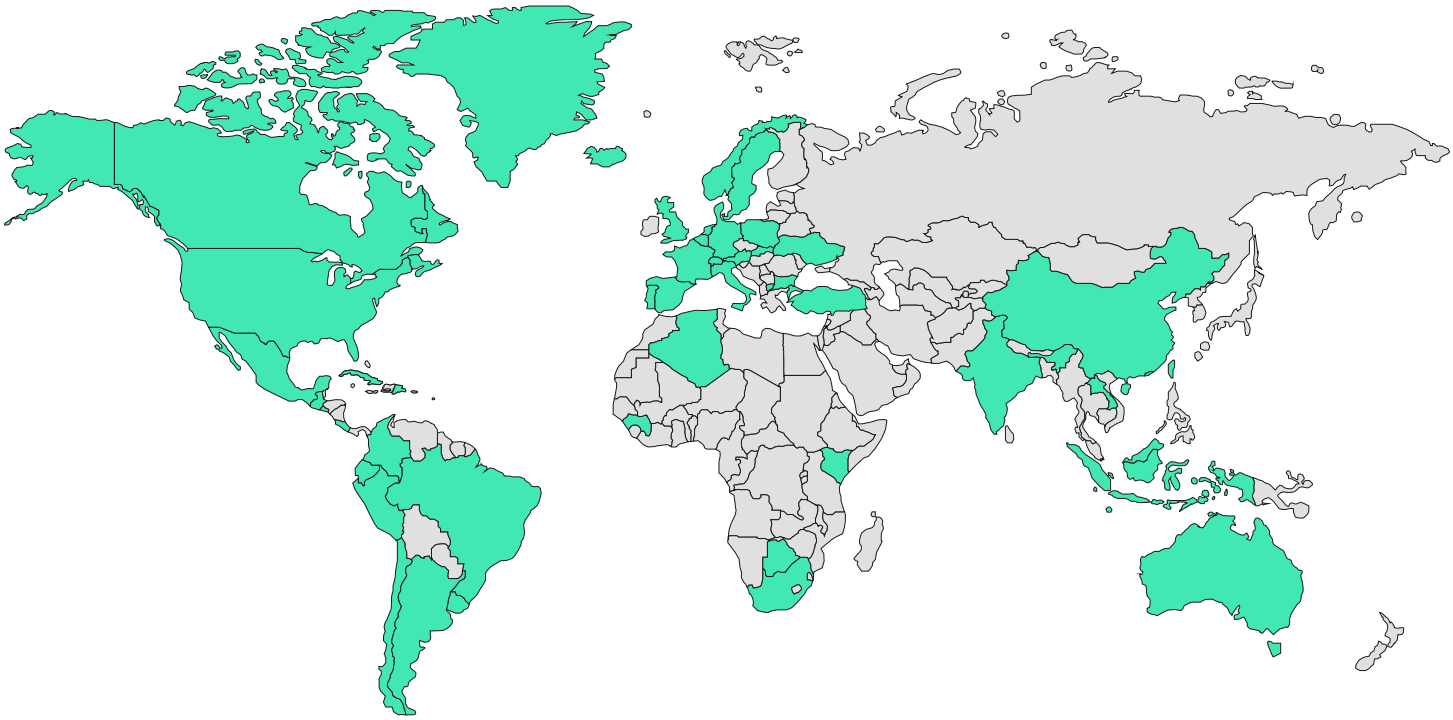
Es esencial que las entidades gubernamentales refuercen sus medidas de seguridad cibernética y adopten estrategias de ciberinteligencia para anticipar, prevenir y responder a estos ataques. Esto incluye:

* Fuentes: Registros internos CCI Entel Digital
https://www.stealthmole.com/
https://portal.cci-entel.cl/Threat_Intelligence/Boletines/1693/

Medidas defensivas: la instalación de software de seguridad actualizado y la realización de auditorías de seguridad regulares.

Medidas proactivas: la formación de personal en las mejores prácticas de ciberseguridad y la colaboración con expertos en ciberinteligencia para identificar y neutralizar las amenazas antes de que puedan causar daño.

Ataques ransomware a entidades gubernamentales 2022-2023

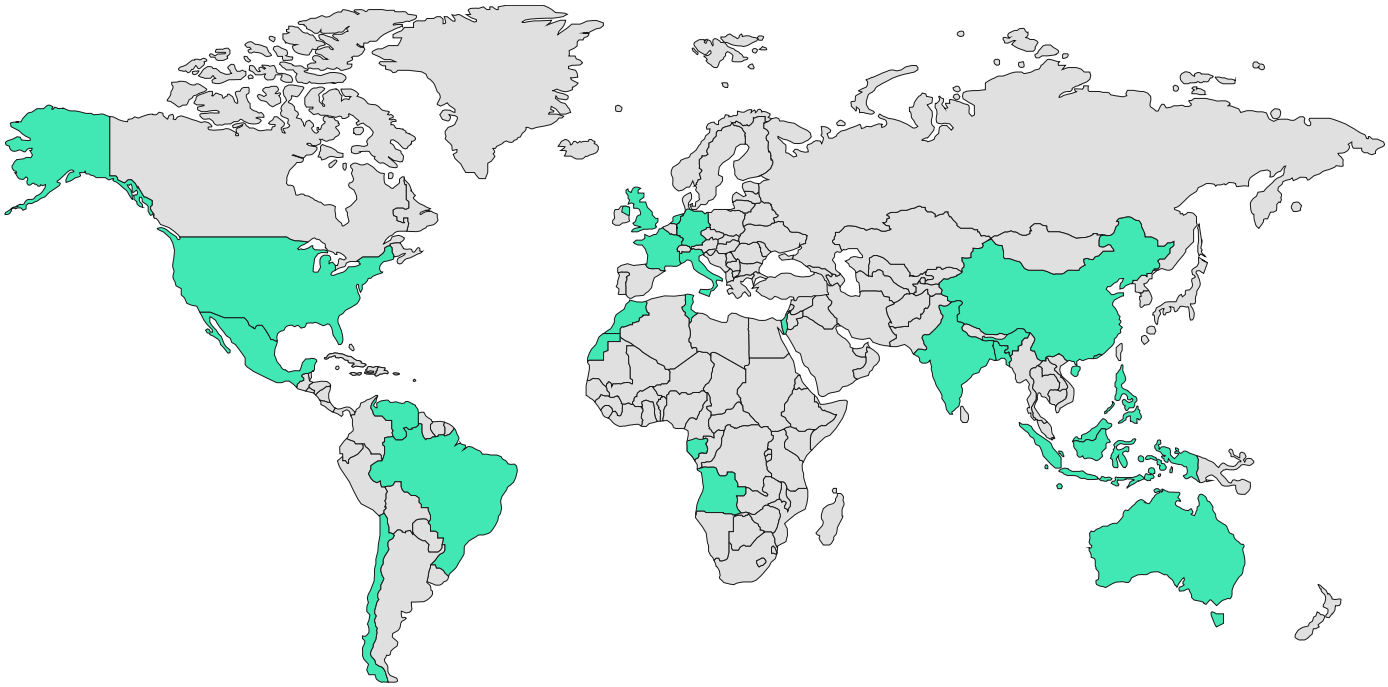


* Fuentes: Registros internos CCI Entel Digital
https://www.stealthmole.com/
https://portal.cci-entel.cl/Threat_Intelligence/Boletines/1693/

Sector financiero

Las entidades bancarias, vitales para la economía global, no han sido inmunes a las amenazas cibernéticas. Entre 2022 y 2023, se han registrado 70 ataques de Ransomware, la mayoría de los cuales se ubicó en Estados Unidos.

Países afectados por ransomware Banca 2022 - 2023

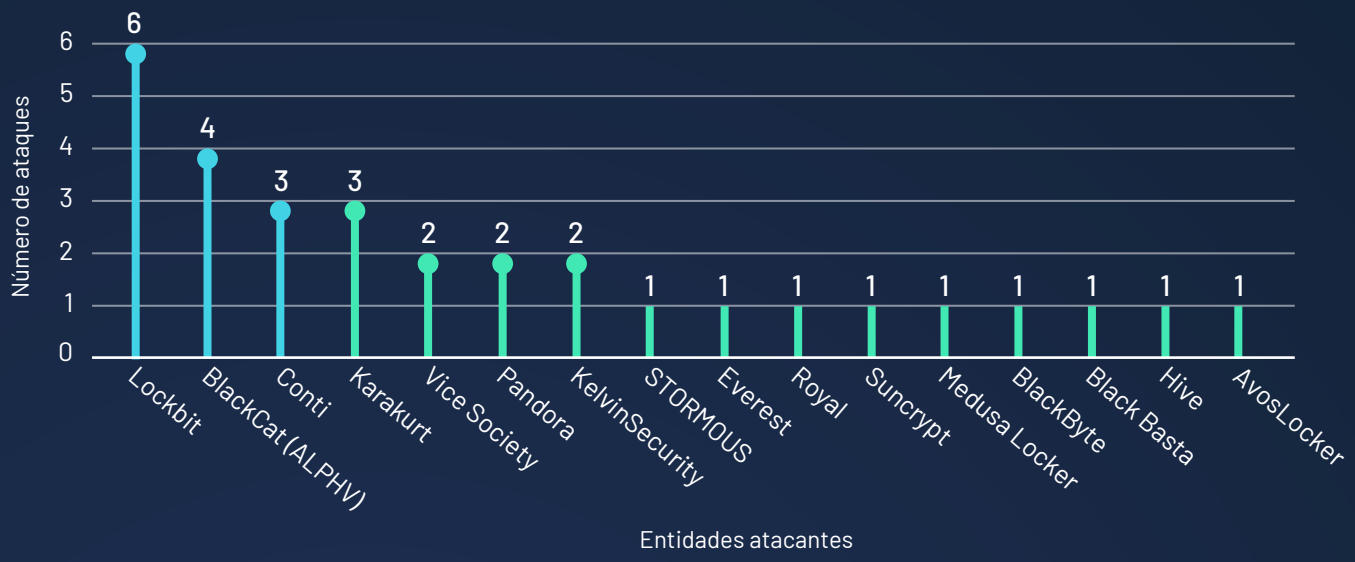


A nivel global:
2022 con 31 ataques
2023 con 39 ataques.

* Fuentes: Registros internos CCI Entel Digital
https://www.stealthmole.com/
https://portal.cci-entel.cl/Threat_Intelligence/Boletines/1693/

En 2022, se reportaron 31 de estos ataques, en tanto que en 2023 se registraron 39, un número preocupante que demuestra la creciente amenaza que los ciberdelincuentes representan para el sector financiero.

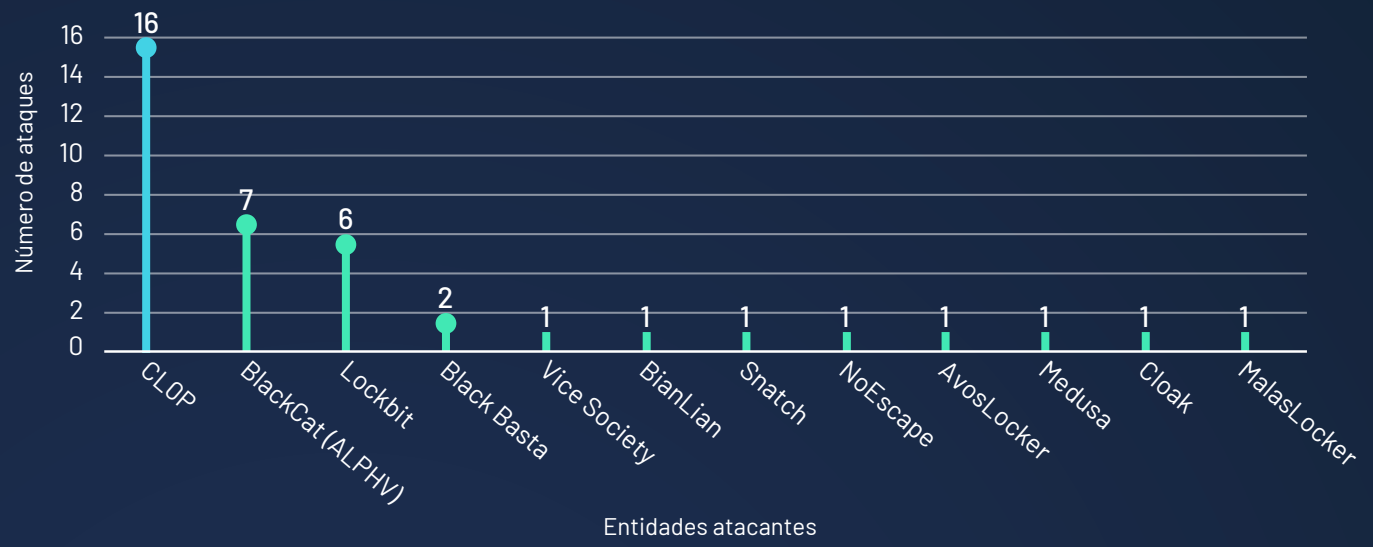
Ataques por ransomware 2022 Banca



Hasta noviembre de 2023, se registraron 39 nuevos ataques, superando en tan solo dos trimestres la cifra del año anterior. Cada uno de estos ataques puede causar interrupciones significativas en los servicios bancarios, pérdidas financieras directas e indirectas y daños a la reputación de las instituciones afectadas.

* Fuentes: Registros internos CCI Entel Digital
https://www.stealthmole.com/
https://portal.cci-entel.cl/Threat_Intelligence/Boletines/1693/

Ataques por ransomware 2023 Banca



Las grandes recompensas económicas que el mundo bancario ofrece a los actores maliciosos les permite mejorar la sofisticación de sus ataques y, en algunos casos, financiar programas de carácter tan serio como los nucleares.

De hecho, recientes estimaciones han puesto de manifiesto un hecho inquietante: **se sugiere que Corea del Norte genera cerca del 50% de sus ingresos a través de ciberataques.** Las entidades financieras y las redes blockchain constituyen sus principales objetivos actualmente. Estos ciberdelincuentes logran sustraer enormes cantidades de criptomonedas de manera anónima, lo que complica aún más la tarea de rastrear y prevenir dichas amenazas en la infraestructura crítica.

* Fuentes: Registros internos CCI Entel Digital
https://www.stealthmole.com/
https://portal.cci-entel.cl/Threat_Intelligence/Boletines/1693/

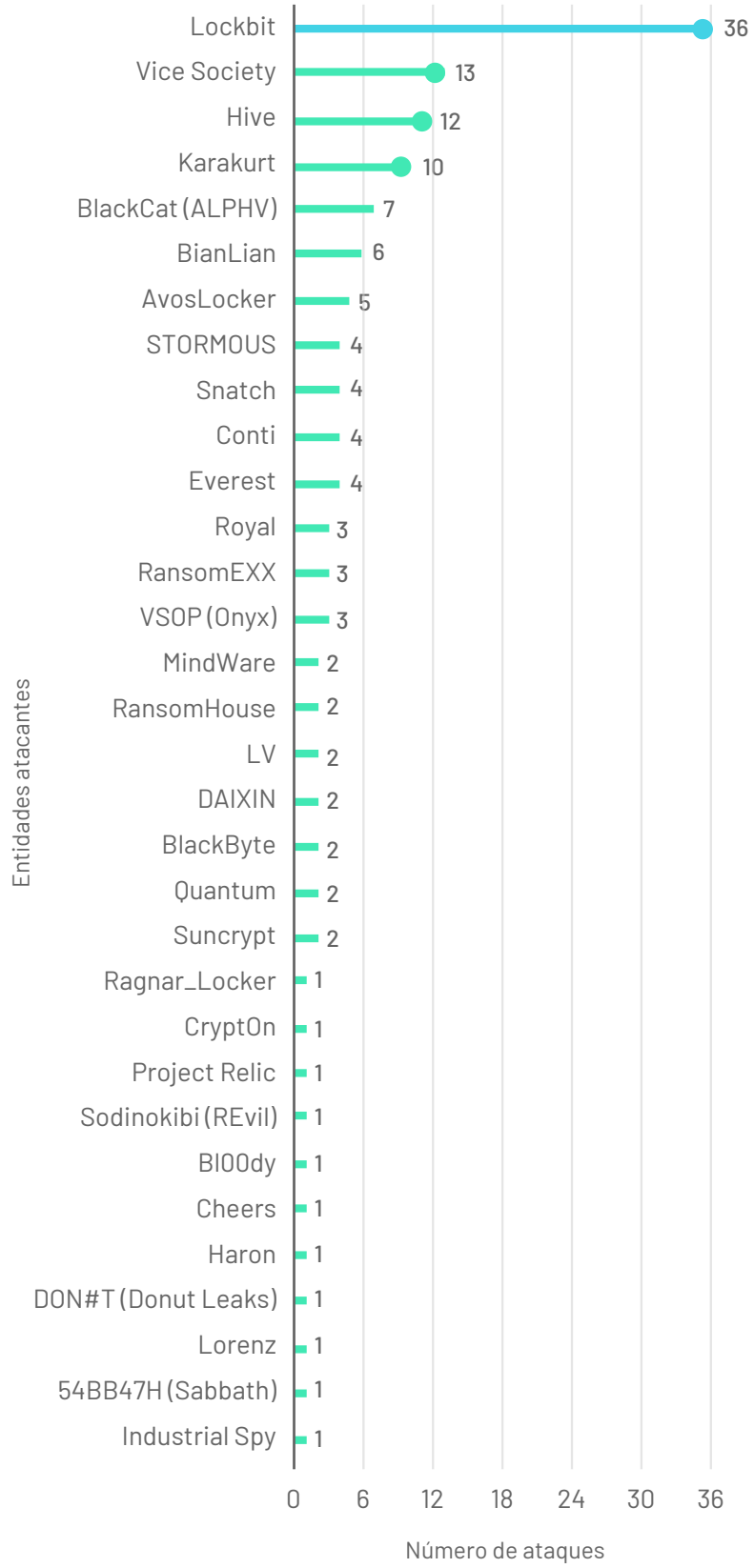
Salud

Desde enero de 2022 hasta noviembre de 2023, el sector de la salud ha sufrido de manera considerable las embestidas de los ataques de Ransomware. Se registraron 386 ataques de este tipo, lo que resalta la vulnerabilidad de una industria esencial para el bienestar de las personas.

En el año 2022, se registraron 139 de estos ataques a nivel mundial. Cada uno de ellos puede interrumpir los servicios de atención médica vitales y poner en peligro la privacidad de los datos del paciente, lo que tiene implicaciones éticas y legales significativas.

* Fuentes: Registros internos CCI Entel Digital
https://www.stealthmole.com/
https://portal.cci-entel.cl/Threat_Intelligence/Boletines/1693/

Total ataques por ransomware sector Salud 2022



* Fuentes: Registros internos CCI Entel Digital
https://www.stealthmole.com/
https://portal.cci-entel.cl/Threat_Intelligence/Boletines/1693/

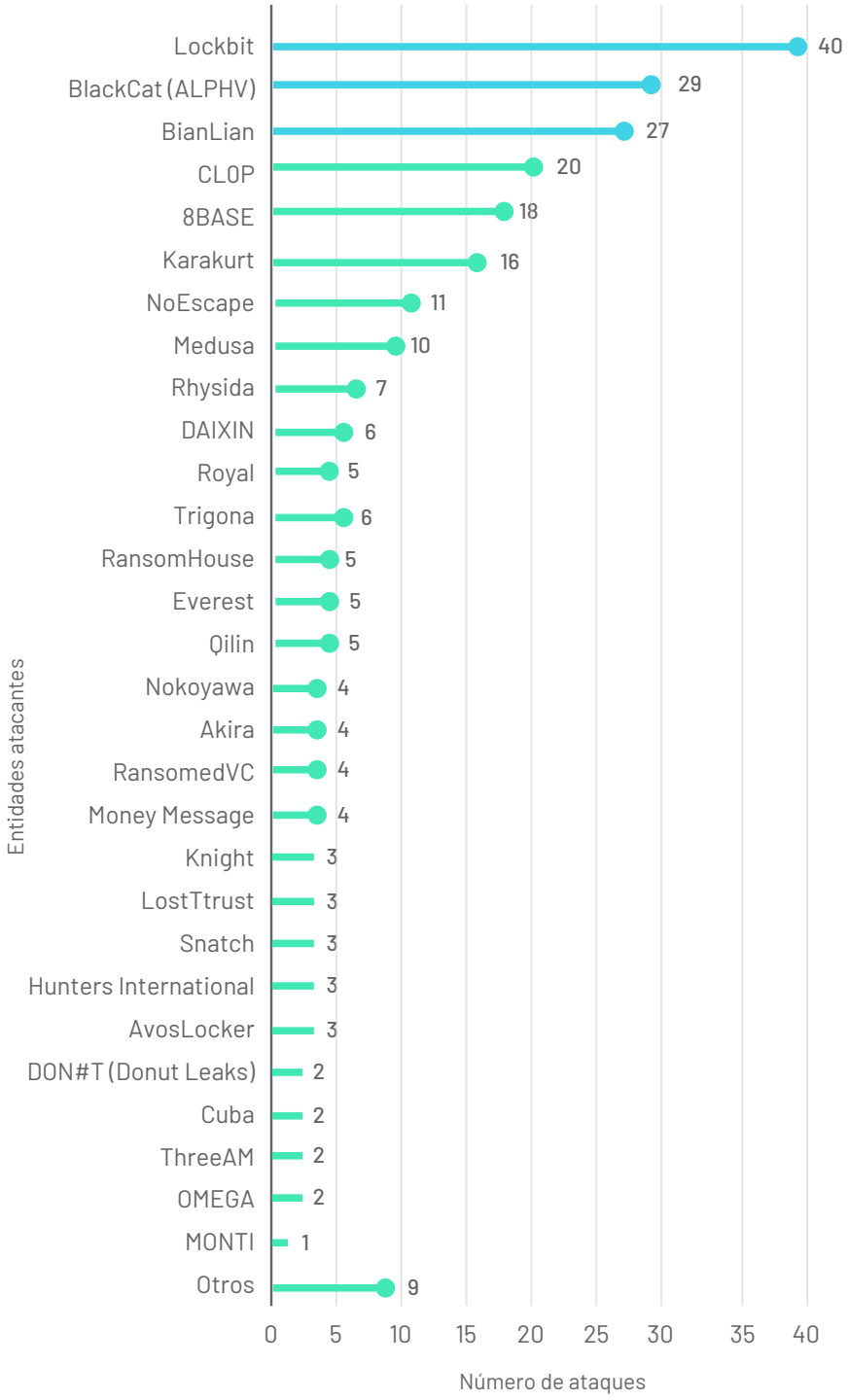
Algunos ciberactores han declarado que las organizaciones de salud no están en su punto de mira. Incluso, se ha visto a operadores de Ransomware como LockBit disculparse y proporcionar claves de descifrado gratuitas a las entidades afectadas por sus afiliados.

De cualquier manera, la dura realidad es que la mayoría de los actores de Ransomware han comprometido alguna vez una entidad dentro del sector de la salud. A pesar de las aparentes garantías, la amenaza persiste, subrayando la necesidad imperante de una ciberinteligencia robusta para proteger nuestra infraestructura esencial.

De hecho, **entre enero y noviembre del año 2023, se registraron otros 154 ataques.** Esto pone de manifiesto que el sector de la salud sigue siendo un objetivo atractivo para los ciberdelincuentes.

* Fuentes: Registros internos CCI Entel Digital
https://www.stealthmole.com/
https://portal.cci-entel.cl/Threat_Intelligence/Boletines/1693/

Ataques por Ransomware sector salud 2023



* Fuentes: Registros internos CCI Entel Digital
https://www.stealthmole.com/
https://portal.cci-entel.cl/Threat_Intelligence/Boletines/1693/

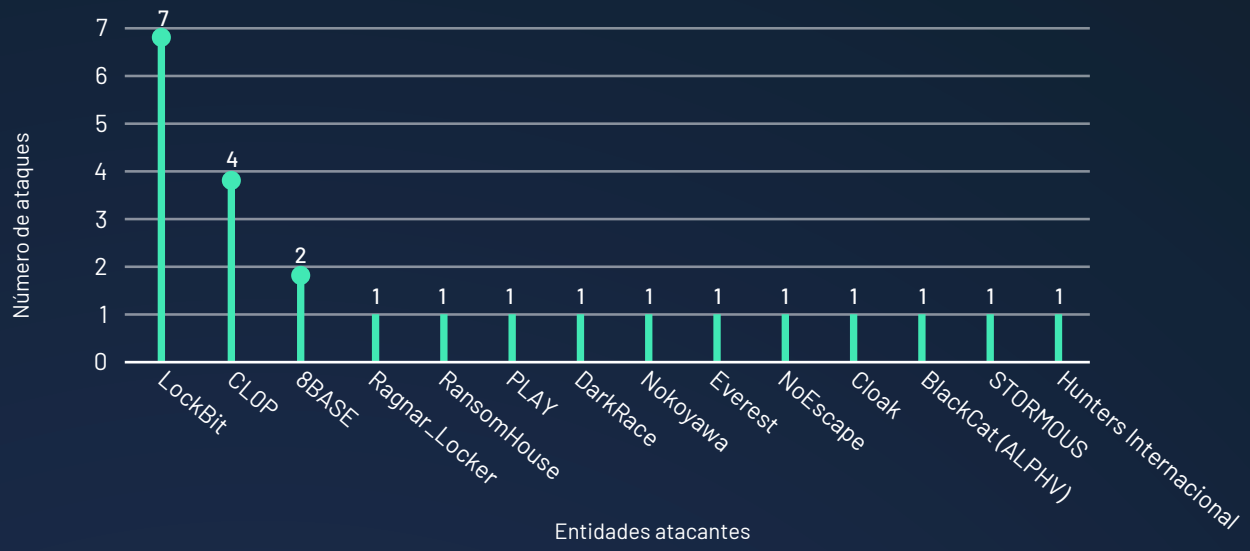
A nivel de LATAM, se registran 14 ataques al sector de la salud en los últimos dos años. El país con más incidencia ha sido Brasil con ocho ataques, seguido por tres ataques en Colombia y un ataque en Argentina, México y Chile, respectivamente.

Para hacer frente a estas amenazas, resulta esencial que las organizaciones de salud cuenten con una infraestructura de TI segura y actualizada, así como un plan de respuesta ante incidentes. Este plan debe incluir medidas para recuperar los sistemas y los datos afectados, comunicarse con los pacientes y las autoridades pertinentes.

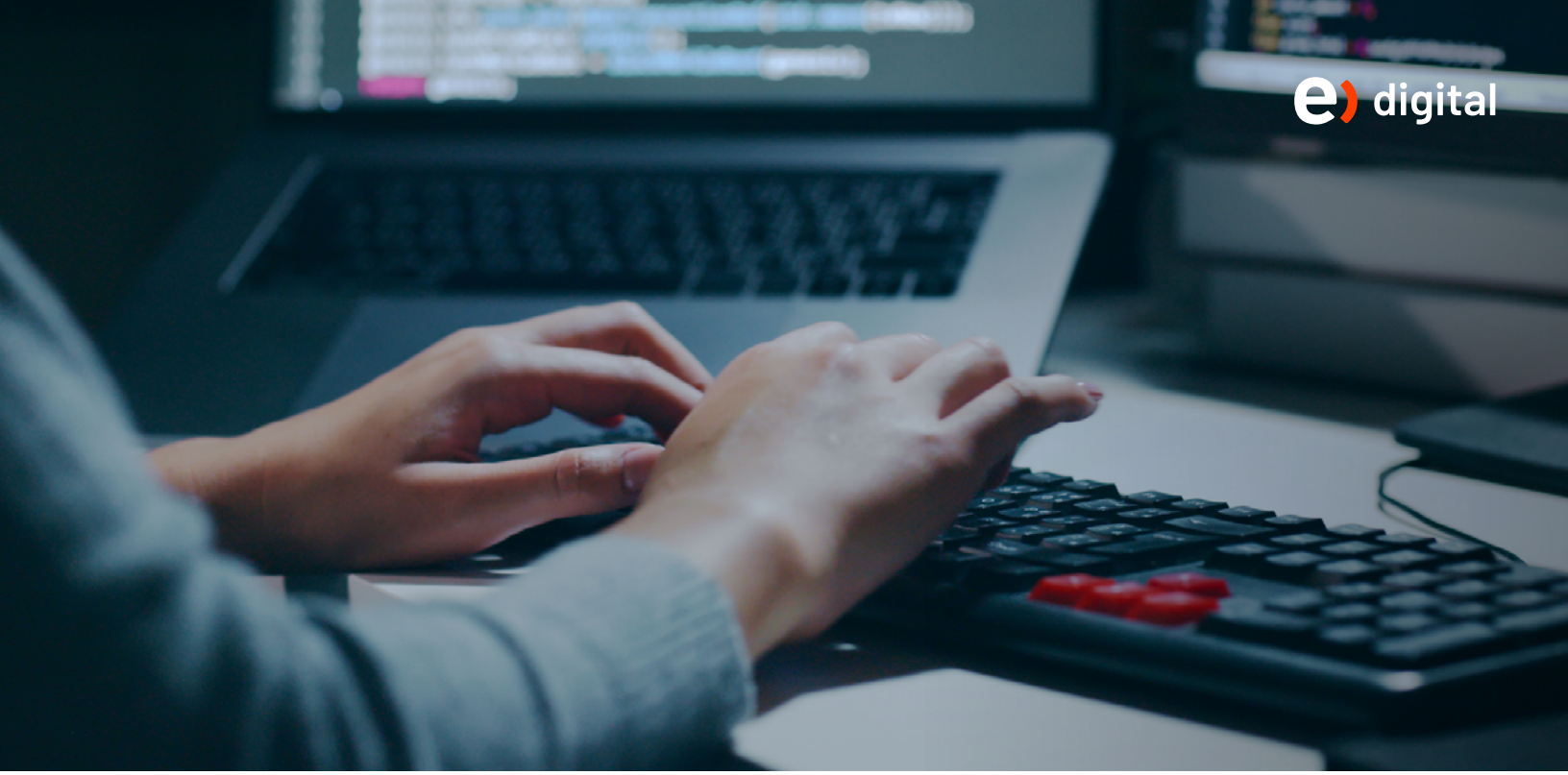
Energía

El sector energético, que constituye una infraestructura crítica para cualquier nación, también ha sido objetivo de ataques de Ransomware durante los últimos dos años. Se ha registrado un total de 32 ataques conocidos a nivel global, poniendo en evidencia la necesidad de medidas de seguridad cibernética robustas en esta industria.

Ataques por Ransomware sector energía 2023



* Fuentes: Registros internos CCI Entel Digital
https://www.stealthmole.com/
https://portal.cci-entel.cl/Threat_Intelligence/Boletines/1693/



Durante el año 2022, se reportaron 8 ataques de Ransomware, mientras que hasta noviembre del año 2023 ya se han registrado 24 ataques. Este patrón demuestra que los ciberdelincuentes están cada vez más enfocados en la infraestructura crítica y el sector energético no es una excepción.

Tan solo uno de estos ataques ha tenido lugar en nuestra región, específicamente en Argentina. Sin embargo, este hecho no debe dar lugar a la complacencia. La interconexión global de las infraestructuras energéticas y la creciente sofisticación de los ciberataques significa que ninguna región está exenta de estas amenazas.

La seguridad cibernética en el sector energético no es solo una cuestión de proteger los activos de la empresa, sino también de garantizar la continuidad de los servicios energéticos y proteger la seguridad nacional. Por lo tanto, es esencial que se realicen inversiones adecuadas en la protección de las infraestructuras energéticas.

* Fuentes: Registros internos CCI Entel Digital
https://www.stealthmole.com/
https://portal.cci-entel.cl/Threat_Intelligence/Boletines/1693/

¿Cómo avanzamos en materias de resguardo de Infraestructuras Críticas en Chile?

En abril de 2023, el senado aprobó legislar el proyecto de Ley Marco sobre Ciberseguridad e Infraestructura Crítica de la Información, En su Artículo 1, el proyecto establece los principales objetivos de la norma:

Determinar la institucionalidad, los principios y la normativa general que permitan estructurar, regular y coordinar las acciones de ciberseguridad de los organismos del Estado y los particulares.

Fijar requisitos mínimos que contribuyan a prevenir, contener, resolver y dar respuesta a los incidentes de ciberseguridad.

Precisar las atribuciones y obligaciones de los organismos del Estado, así como los deberes de las instituciones privadas y los mecanismos de control, supervisión y responsabilidad ante infracciones.

* Fuentes: https://portal.cci-entel.cl/Threat_Intelligence/Boletines/1693/
https://www.csirt.gob.cl/noticias/congreso-aprueba-ley-marco/

Creación de la Agencia Nacional de Ciberseguridad (ANCI)

En el articulado de la Ley Marco sobre Ciberseguridad e Infraestructura Crítica de la Información, cabe destacar el papel de la Agencia Nacional de Ciberseguridad (ANCI). Entre otras funciones, será la encargada de identificar a los operadores de importancia vital y servicios esenciales.

Además, la ley obligará a que los organismos del Estado y las instituciones privadas sean más proactivos ante los incidentes de seguridad cibernética. Para ello, la agencia establecerá protocolos y estándares diferenciados en función del tipo de organización.

Del mismo modo, todas las entidades públicas y privadas, con excepción de aquellas eximidas por la ANCI, deberán reportar al CSIRT nacional, en un plazo de tres horas, los ciber incidentes que puedan tener efectos significativos. Igualmente, deberán informar sobre su plan de acción. Por otro lado, se les prohíbe realizar pagos si son víctimas de ataques de Ransomware.

Finalmente, a la agencia se le atribuye la regularización, fiscalización y sanción de las acciones de seguridad informática de los organismos de la Administración del Estado y de las instituciones privadas.

* Fuentes: https://portal.cci-entel.cl/Threat_Intelligence/Boletines/1693/
https://www.csirt.gob.cl/noticias/congreso-aprueba-ley-marco/

CAPÍTULO 5

Panorama de Incident Response

El aumento de las amenazas cibernéticas y de los actores que las ejecutan representa un riesgo significativo para las operaciones de cualquier tipo de industria, lo que subraya la necesidad de desarrollar planes de identificación y contención inmediata para evitar la propagación de cualquier amenaza.

Este plan de respuesta, conocido como "playbook", debe estar alineado con un marco internacional que sea robusto y flexible. En nuestro caso, utilizamos el marco SANS, reconocido mundialmente por su eficacia en la gestión de incidentes de ciberseguridad.

Igualmente, un plan completo debe considerar todas las áreas que juegan un papel crucial en la mitigación de las amenazas y la protección de nuestros sistemas, como:

- Redes (NGFW, WAF, ADDOS)
- Endpoint (AV, EDR, XDR)
- Mensajería
- Bases de datos
- Otros

Tomando todos estos elementos en cuenta, la prioridad debe ser la de velar por una temprana identificación de amenazas con tecnologías de vanguardia y, en caso de incidencia, mantener la funcionalidad del negocio con una operación mínima aceptable mientras se dan las indicaciones de erradicación y recuperación.

* Fuente: Datos internos de IR (Incident Response) CCI Entel Digital

Monitorización de eventos

Considerando que ciertos sectores pueden ser más propensos a tipos de amenazas, es esencial adaptar nuestras estrategias de seguridad y respuesta a incidentes de manera específica, considerando las características únicas de cada industria. Sin embargo, en todo tipo de escenarios y organizaciones debemos monitorear eventos relevantes como:

- Amenazas en Antivirus (AV).
- Firmas en Sistemas de Prevención de Intrusiones (IPS).
- Seguimiento a los activos críticos.
- Autenticación y autorización.
- Cuentas privilegiadas.
- Tráfico con Indicadores de Compromiso (IoC).

Esta visibilidad nos permite identificar y responder rápidamente a las amenazas, minimizando así el impacto potencial en nuestras operaciones.

Porcentaje de tiempo por cada etapa del incidente

Con base en las estadísticas y los datos recopilados de los incidentes atendidos por nuestro equipo de respuesta durante el año 2023, se ha identificado un patrón significativo: tras un incidente de ciberseguridad, la fase de recuperación es la que supone mayores demoras.

En caso de estar frente a una amenaza o incidente de ciberseguridad, se suele destinar un 35% del tiempo en la recuperación de los sistemas.

* Fuente: Datos internos de IR (Incident Response) CCI Entel Digital

Causas que extienden la fase de recuperación

Falta de documentación completa y actualizada de la infraestructura	Esta falta de visibilidad dificulta la identificación rápida de sistemas afectados y prolonga los tiempos de respuesta durante la fase de recuperación.
Falta de un plan estructurado y definido para la recuperación ante desastres	La implementación de un DRP es esencial para facilitar una recuperación rápida y eficiente de la infraestructura después de un incidente de ciberseguridad.
Falta de profesionales capacitados en seguridad y administración de plataformas	La coordinación eficaz y el conocimiento necesario para recuperar la infraestructura de manera eficiente, a menudo se ven obstaculizados por la falta de personal capacitado.
Ausencia de procedimientos de respaldo robustos para los servidores y sistemas críticos de la organización	La falta de una estrategia de respaldo adecuada contribuye a la pérdida de datos y dificulta la restauración de la operatividad normal ante incidentes de ciberseguridad.

* Fuente: Datos internos de IR (Incident Response) CCI Entel Digital

Principales objetivos en un ataque

De acuerdo con los datos derivados de los incidentes atendidos por el equipo de respuesta ante incidentes del Centro de Ciberinteligencia de Entel Digital, se destaca que los servidores productivos son consistentemente el objetivo más frecuente, seguidos por los equipos de usuario y, en última instancia, los servidores Active Directory de las organizaciones.

Este análisis subraya la importante necesidad de tomar las siguientes medidas de protección:

› Servidores productivos

› Focalizar nuestros esfuerzos en la protección de los servidores productivos. Al ser el blanco más común y crítico, se convierten en un área central susceptible a vulnerabilidades y amenazas.

› Reforzar las medidas de seguridad en estos servidores, mediante la aplicación de parches, configuraciones seguras, monitoreo continuo y la adopción de plataformas de protección de endpoint de alto nivel.

› Equipos de usuario

› Prestar una atención dedicada a los equipos de usuario se revela como crítica, dado que constituyen otra área de interés primordial para los atacantes.

› Implementar prácticas como la concientización y la formación, junto con soluciones de seguridad sólidas.

* Fuente: Datos internos de IR (Incident Response) CCI Entel Digital

› Active Directory

› Reforzar la seguridad de esta área, mediante la implementación de políticas de acceso adecuadas, monitoreo proactivo, establecimiento de políticas de contraseñas sólidas y la elección de plataformas de protección de endpoint con altas prestaciones.

* Fuente: Datos internos de IR (Incident Response) CCI Entel Digital

Estadísticas de reincidencia

Nuestro análisis reciente ha revelado un patrón intrigante en la reincidencia de amenazas de ciberseguridad en las organizaciones apoyadas. Entre todos los tipos de incidentes atendidos durante el año, hemos observado que el único que se ha repetido en el mismo cliente son los ataques de Phishing.

A pesar de enfrentar desafíos similares, como ataques de Malware propagados a través de Phishing, hemos notado mejoras significativas en los tiempos de respuesta y en la efectividad de las medidas de mitigación.

Esta mejora se atribuye a las colaboraciones y a la implementación de estrategias de erradicación, respaldadas por las lecciones aprendidas de incidentes anteriores.

Gracias a estas iniciativas, no solo hemos logrado una disminución notable en el tiempo de respuesta ante estos incidentes, sino que también se ha mantenido ininterrumpida la producción y operación de las empresas afectadas.

La concientización y capacitación de los usuarios han desempeñado un papel crucial en este avance. Al enfrentarse nuevamente con el Phishing, los usuarios fueron capaces de escalar el incidente de manera inmediata a nuestros analistas de ciberseguridad, facilitando así la rápida identificación y neutralización del correo malicioso.

* Fuente: Datos internos de IR (Incident Response) CCI Entel Digital

Este panorama no solo refleja la capacidad de análisis y contención de nuestro centro de ciberinteligencia, sino también un fortalecimiento notable en la resiliencia en ciberseguridad de nuestros clientes.

Recomendaciones

En base a la experiencia adquirida durante la gestión de incidentes en los últimos años, se ha observado que, en la mayoría de los casos, el vector de entrada, la facilidad de propagación y el impacto resultante de los incidentes se atribuyen a fallos de configuración y malas prácticas en el ámbito de la ciberseguridad de las organizaciones. Con este contexto en mente, se presentarán a continuación una serie de recomendaciones destinadas a prevenir y mitigar el impacto en caso de enfrentar un incidente de ciberseguridad:

- Asegurar adecuadamente los sistemas y servicios de acceso remoto, como los inicios de sesión VPN, para reducir el riesgo de ataques y brechas de seguridad.
- Implementar medidas de seguridad adicionales, como la autenticación de dos factores o multifactor, para proteger el acceso remoto y prevenir la suplantación de identidad.

* Fuente: Datos internos de IR (Incident Response) CCI Entel Digital

- Monitorear de forma constante y proactiva los registros de eventos y otros indicadores de actividad sospechosa en los sistemas y redes, para detectar rápidamente las intrusiones y prevenir que el ataque se propague.
- Siempre contar con un antivirus-EDR-XDR actualizado y desplegado en todos los endpoints y sistemas de la organización, con la finalidad de detectar y prevenir la ejecución y propagación de Malware y otros ataques maliciosos.
- Implementar medidas de control de acceso y autenticación adecuadas para limitar el movimiento lateral en la red, de modo que los atacantes no puedan acceder a otros sistemas y recursos después de comprometer un solo punto de entrada.
- Asegurarse de que todos los servidores y aplicaciones se mantengan actualizados con las últimas versiones de software y sistemas operativos. Esto puede ayudar a prevenir vulnerabilidades conocidas que los atacantes pueden explotar.
- Realizar pruebas de penetración regulares puede ayudar a identificar vulnerabilidades de seguridad antes de que sean explotadas por un atacante. Las pruebas de penetración también pueden proporcionar información valiosa sobre la eficacia de los controles de seguridad existentes.

* Fuente: Datos internos de IR (Incident Response) CCI Entel Digital

- Establecer una política de actualización de software y sistemas operativos puede ayudar a asegurar que los servidores y aplicaciones se mantengan actualizados en todo momento.
- Capacitar al personal en seguridad de la información puede ayudar a prevenir errores humanos y mejorar la conciencia de seguridad de la organización.
- Aplicar el principio de menor privilegio en el entorno AD, lo que significa otorgar sólo los permisos y privilegios necesarios para que los usuarios realicen sus trabajos. Esto puede reducir la exposición a riesgos de seguridad si se ve comprometida una cuenta de usuario.
- Realizar auditorías de seguridad regularmente puede ayudar a identificar cuentas con altos privilegios que no se utilizan con frecuencia y que podrían ser eliminadas. También puede ayudar a identificar permisos innecesarios que se han otorgado por error o por malas prácticas.
- La necesidad de tener un plan de respuesta a incidentes de seguridad claro y bien definido, que incluya los procedimientos a seguir para contener el incidente, investigar la causa raíz y tomar medidas correctivas para evitar futuras brechas.

* Fuente: Datos internos de IR (Incident Response) CCI Entel Digital

CAPÍTULO 6

Tecnologías emergentes de Ciberseguridad

Estado de seguridad Cloud 2023

Entre los principales ataques que se observaron durante 2023 en Cloud se encuentran los siguientes:

- **Falta de configuración**

  Una de las principales amenazas detectadas es la de empresas que no configuran la seguridad correctamente de los entornos Cloud, lo que implica contar con contraseñas débiles, exposición de datos sensibles o falta de autenticación de doble factor.

- **Acceso no autorizado**

  El entorno Cloud no está exento de ataques de phishing y los atacantes pueden llegar a obtener las credenciales del administrador de la nube, dándoles acceso a la creación de máquinas virtuales, a los datos, a modificar imágenes, entre otras.

- **APIs inseguras**

  Hoy en día es uno de los principales mecanismos de acceso a datos utilizados para comunicar información entre múltiples servidores, y en algunos casos no son lo suficientemente seguras, permitiendo el uso no autorizado de estas, consultas por usuarios no autenticados, robo de información o incluso hacer cambios en plataformas.

- **Robo de cuentas**

  Con este método, el atacante obtiene la información de una cuenta y todos los permisos y accesos que pueda tener.

- **Exceso de información**

  Si el exceso de datos entregados por los sistemas no son bien procesados, no se obtienen alertas en caso de intrusión o en el momento en que un atacante pueda obtener acceso a un sistema.

Principales incidentes de 2023

Acorde a un estudio de IBM a 553 organizaciones de 16 países y regiones, presentes en 17 diferentes industrias, más del 80% de las filtraciones ocurridas en el 2023 involucran datos almacenados en la nube. Esto ocurrió después que se duplicaran los ataques a infraestructura en la nube entre 2021 y 2022.

Además, se reporta un aumento de casi un 70% más de ataques desde enero a septiembre del 2023 en comparación con el mismo periodo de 2022.

Ataques a la cadena de suministro

Se registró un aumento de 300% de ataques a la cadena de suministros en comparación con el año anterior, principalmente porque los sistemas basados en la nube son altamente interdependientes, siendo atractivos para los atacantes.

Ransomware Rorschach

Durante el 2023 se observaron ataques mediante el Ransomware Rorschach, el cual es considerado el más rápido para encriptar. Fue nombrado de esta manera dado que cada investigador vio algo distinto en el código de este Malware, tal como sucede con el test del mismo nombre.

Además, este fue capaz de saltarse algunas protecciones utilizando técnicas de propagación poco usuales en la actualidad, afectando la cadena de suministro de varias empresas tanto a nivel nacional como internacional, interrumpiendo miles de servicios por extensos periodos de tiempo.

* Fuentes: https://cloudsecurityalliance.org/blog/2023/07/24/highlights-from-the-2023-cloud-threat-report
https://www.apple.com/cl/newsroom/2023/12/report-2-point-6-billion-records-compromised-by-data-breaches-in-past-two-years/

6.1 Desafíos y oportunidades en la seguridad en la nube

Para 2024 se comenzará a utilizar de manera más masiva la inteligencia artificial como servicio (IAaaS), ya que permite la obtención de datos para dar servicio a los clientes o para aplicaciones de venta, por ejemplo.

Sin embargo, la adopción de esta nueva tecnología podría permitir la fuga de información y exfiltración de datos reservados de una compañía si no se prepara el ambiente adecuadamente.

Si bien el uso de la IA es un gran aporte al trabajo y mejora los tiempos de respuesta, se debe tener en cuenta la seguridad al momento de implementarla, por lo que se deben separar las áreas a las que cada cliente o usuario tenga acceso.

› MultiCloud

Otra tendencia en materia de Cloud que se puede observar para el 2024 está en el uso de múltiples proveedores de nubes públicas y privadas, que se da por la flexibilidad y seguridad que brinda este modelo. Además, permite en algunos casos bajar los costos de los servicios, aunque implica mayores riesgos si estas interconexiones no son configuradas correctamente observando la seguridad de cerca.

› Zero Trust

Para evitar ataques, se considera como tendencia la implementación de modelo Zero Trust en la nube para permitir conexiones solo de quien realmente está autorizado para acceder a las aplicaciones. Según Gartner, para el 2026 el 10% de las compañías más grandes tendrán implementado un sistema maduro de Zero Trust.

Mayor resiliencia

La resiliencia es un desafío que se debe afrontar dado el crecimiento en los ataques realizados a las nubes. Se debe contar con planes de contingencia y recuperación ante desastres sólidos con respaldos, redundancia y mitigaciones ante posibles intrusiones que permitan mantener a flote los servicios de manera eficiente.

Soluciones RASP

Las soluciones RASP (Runtime Application Self Protection) cuentan con una tecnología que permite revisar las aplicaciones durante la ejecución en el mismo servidor, con esto se puede proteger el código evitando ataques y errores de programación.

También puede ser implementada durante el ciclo de vida de desarrollo de software, y como ventajas entrega una mayor protección de ataques, es de fácil mantención, genera menor cantidad de falsos positivos, es compatible con la nube y on premise y se adapta a nuevos formatos como HTML, XML, JSON, entre otros.

Protecciones de cargas de trabajo en entornos Cloud

* Fuente:https://www.softwaretestinghelp.com/rasp-tutorial/

La Inteligencia Artificial (IA) es la capacidad de un sistema informático de simular las capacidades de aprendizaje, percepción, razonamiento y toma de decisiones de la inteligencia humana.

Inteligencia Artificial
Capacidad de sentir, razonar, interactuar y aprender

- Visión por computadora
- Lenguaje de procesamiento natural
- Reconocimiento de voz
- Robotica y movimiento
- Reconocimiento y captura
- Planificación y optimización

Machine Learning
Capacidad de apender

- Aprendizaje supervisado
- Aprendizaje no supervisado
- Aprendizaje por refuerzo

Métodos
Capacidad para razonar

- Regresión
- Árboles de decisión
- Etc.

Tecnologías
Habilitación física

- Plataforma
- UX
- Apis
- Sensores
- Etc.

Los algoritmos más llamativos que integra esta tecnología son los basados en redes neuronales, que simulan la interconexión de los procesos de pensamiento humano.

Las redes neuronales han sufrido varias transformaciones a lo largo del tiempo conforme se va optimizando la capacidad de procesamiento de los sistemas informáticos y la disponibilidad, ahora ilimitada, de grandes volúmenes de datos.

En este sentido, han surgido nuevos conceptos asociados al procesamiento de los datos que optimizan en gran medida las tareas de aprendizaje de las máquinas:

- Machine Learning.
- Deep Learning.
- Aprendizaje supervisado.
- Aprendizaje no supervisado.

6.2 Evolución de la Inteligencia Artificial en la ciberseguridad

A partir del aumento de la repercusión que la IA tiene en diferentes industrias, ha experimentado igualmente una evolución en aspectos de ciberseguridad:

› Década de 1990 - 2000

Detección de amenazas: En sus etapas iniciales la IA se utilizó para detectar patrones de amenazas conocidas mediante el ánalisis de firmas y comportamientos maliciosos.

› Década de 2000 - 2010

Análisis de comportamiento y Machine Learning: se adoptaron enfoques basados en machine learning para mejorar la capacidad de la derección de amenazas. Se utilizaron algoritmos de aprendizaje automático para analizar el comportamiento de usuarios y sistemas y detectar anomalías.

2010 - Presente

Detección de amenazas avanzadas persistentes (APT): La IA se volvió escencial para la detección de amenazas avanzadas persistentes (APT). Se implementaron modelos de aprendizaje profundo y redes neuronales para identificar patrones sutiles y amenazas persistentes.

Automatización de respuestas: La IA se emplea para automatizar respuestas a incidentes de seguridad. Sistemas basados en reglas y aprendizaje automático ayudan a responder rápidamente a amenazas conocidas y desconocidas.

Seguridad predictiva y prevención: La IA se utiliza para prever y prevenir amenazas antes de que ocurran. Los modelos predictivos basados en machine learning y análisis de big data ayudan a anticipar posibles ataques.

2020 - Presente

Adversarial AI y Defensas: Con el aumento de las amenazas adversariales, se ha desarrollado IA que puede defenderse contra ataques adversariales específicos. Las técnicas de adversarial AI se aplican tanto en ataque como en defensa.

Análisis de Grandes Volúmenes de Datos (Big Data): La ciberseguridad ha adoptado análisis avanzados de big data, con IA, que puede procesar grandes volúmenes de información para identificar patrones y correlaciones que podrían indicar amenazas.

Desarrollo de sistemas autónomos: Se están investigando sistemas de ciberseguridad autónomos que utilizan técnicas de IA, como el aprendizaje profundo y el refuerzo, para tomar decisiones de manera autónoma y adaptarse a nuevas amenazas.

Impacto de la Inteligencia Artificial en la defensa

El impacto que ha tenido la IA en la ciberseguridad defensiva ha sido muy positivo, pues ha permitido desarrollar soluciones para la detección y respuesta a amenazas, como:

- IBM Watson for Cybersecurity.
- Darktrace.
- Cylance.
- FireEye.
- Symantec Endpoint Protection.
- Cortex.

Sin embargo, a nivel de ciberseguridad ofensiva, la IA ha abierto la puerta a la aparición de nuevos riesgos y desafíos:

Automatización de ataques

Puede ser utilizada para automatizar y optimizar ataques, lo que aumenta la velocidad y la eficacia de estos.

Mayor sofisticación y complejidad de los ataques

Puede ser utilizada para crear ataques más sofisticados y complejos, lo que dificulta su detección y mitigación.

Capacidad para adaptarse y evadir defensas

Puede permitir la coordinación de ataques a gran escala y a alta velocidad, lo que aumenta el impacto y la dificultad de defensa.

Mayor capacidad de daño

Puede ser utilizada para realizar ataques más precisos y efectivos, lo que aumenta el riesgo de daño a los sistemas y datos.

* Fuentes:https://thehackernews.com/2023/11/offensive-and-defensive-ai-lets-chatgpt.html
https://www.pucara.org/post/la-inteligencia-artificial-en-la-seguridad-y-defensa

Casos de uso de la IA por actores de amenaza

A partir de su enorme potencial, algunos ciberactores de amenaza han comenzado a valerse de la IA para sus procedimientos. Algunos casos a los que es importante poner atención son:

1. **Ataques de Phishing Mejorados por IA**

Los actores de amenaza pueden hacer uso de algoritmos de aprendizaje automático para mejorar la efectividad de los ataques de Phishing. Esto les ofrece la posibilidad de analizar patrones de comportamiento en línea de potenciales víctimas y personalizar mensajes de manera más convincente.

2. **Generación de Contenido Malicioso**

Los modelos de lenguaje generativo, como GPT-3.5 y GPT-4, podrían utilizarse para crear contenido malicioso convincente, como correos electrónicos, mensajes y noticias falsas, diseñados para engañar a sistemas de detección y usuarios.

3. **Ataques de Ingeniería Social Personalizados**

La IA podría utilizarse para analizar información pública sobre objetivos específicos y generar ataques de ingeniería social más personalizados. Los algoritmos no solo pueden suplantar la imagen de las víctimas de forma más realista y eficiente, sino que también pueden sintetizar su voz.

4. **Vulnerabilidades de Seguridad en Modelos de IA**

La implementación incorrecta de modelos de aprendizaje automático en sistemas de seguridad también podría ser un vector de ataque. Los atacantes podrían intentar explotar vulnerabilidades en los modelos de IA para eludir sistemas de detección.

* Fuentes:https://thehackernews.com/2023/11/offensive-and-defensive-ai-lets-chatgpt.html
https://www.pucara.org/post/la-inteligencia-artificial-en-la-seguridad-y-defensa
https://www.esedsl.com/blog/ejemplos-de-ciberataques-lanzados-con-inteligencia-artificial

5 **Mayor velocidad en la creación de Malware adaptativo**

El Malware generado con IA puede ser capaz de adaptarse y evadir las defensas de seguridad, lo que lo hace más peligroso y difícil de combatir. Además, puede ser capaz de propagarse más rápidamente que el Malware tradicional, lo que aumenta el riesgo de infección y daño.

6 **Automatización y optimización de ataques DDoS**

Permite a los actores de amenaza la coordinación de ataques DDoS a gran escala y a alta velocidad, lo que aumenta el impacto y la dificultad de defensa.

¿Cómo detectar ataques que utilizan IA?

Identificar si un ciberataque ha utilizado o no la IA resulta complejo, ya que los ciberactores pueden utilizar una variedad indiscriminada de técnicas y herramientas para llevar a cabo sus operaciones. Sin embargo, existen algunas señales que podrían indicar la presencia de IA en un ciberataque, como:

- **Automatización avanzada**

  Si el ataque parece estar altamente automatizado y coordinado, es posible que se esté utilizando IA para optimizar y ejecutar el ataque.

- **Patrones de comportamiento inusual**

  Si el ataque parece estar utilizando patrones de comportamiento inusual o no humanos, es posible que se trate de uno coordinado con IA.

- **Adaptabilidad y evasión de defensas:**

  Si el ataque parece ser altamente adaptable y capaz de evadir las defensas de seguridad, es posible que se esté utilizando IA.

* Fuente: https://www.esedsl.com/blog/ejemplos-de-ciberataques-lanzados-con-inteligencia-artificial

Brechas de seguridad que proporciona el mal uso de la IA por el usuario común

Los datos son el alimento de las IA generativas para entrenarse a sí mismas, pues se nutren de cada dato (en tiempo real) para clasificarlo, manipularlo, reutilizarlo y proporcionar las respuestas necesarias para otros usuarios. En ese sentido, los datos que entregamos a la inteligencia artificial pueden no estar seguros.

› Caso real

Un caso muy conocido de este hecho es la brecha de seguridad que sufrió la compañía **Samsung Electronics** por parte de **ChatGPT**, a mediados de marzo del 2023:

Algunos colaboradores ingresaron el código fuente de sus sistemas y base de datos empresariales al chatbot, con el fin de solucionar errores de programación y optimización de los algoritmos. El problema es que la información confidencial quedó disponible para todos los usuarios de OpenAI.

Por tanto, es imperativo considerar qué información proporcionamos a los chatbots de IA, ya que una vez que un usuario común entrega datos confidenciales a un chatbot, pierde el control sobre su seguridad.

* Fuente: https://economist.co.kr/article/view/ecn202303300057

¿Cómo hacer frente a los desafíos que plantea la IA en el sector cibernético?

Hacer frente a los desafíos que plantea la IA en la ciberseguridad requiere:

- Desarrollo de estrategias avanzadas.
- Protección de sistemas de IA.
- Colaboración entre la IA y el conocimiento humano.
- Adaptación constante a los cambios en el panorama de amenazas cibernéticas.

Algunas medidas clave para lograr esto son:

1. **Capacitación y concientización**

   Proporciona una formación continua y una comprensión sólida a los profesionales de ciberseguridad sobre las tecnologías de IA, capacidades, limitaciones y riesgos asociados.

2. **Evaluación de riesgos y auditorías**

   Realiza evaluaciones de riesgos regulares para identificar posibles vulnerabilidades en los sistemas de IA utilizados en ciberseguridad. Además, realiza auditorías para evaluar la eficacia y la seguridad de los modelos de IA.

3. **Transparencia y explicabilidad**

   Fomenta la transparencia en los modelos de IA utilizados en ciberseguridad. Asegura que los procesos de toma de decisiones sean explicables y comprensibles, especialmente en entornos críticos.

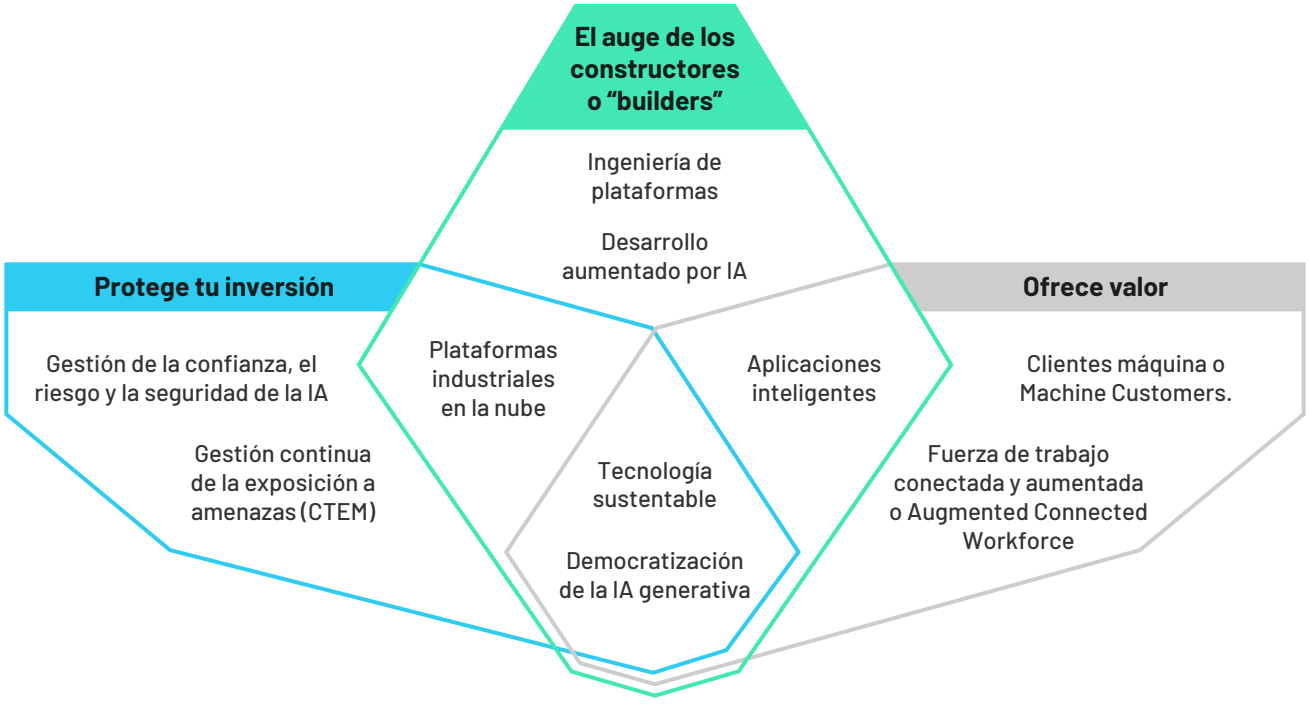
4. **Monitoreo continuo**

   Implementa sistemas de monitoreo continuo para supervisar la actividad y el rendimiento de los sistemas de seguridad basados en IA para detectar anomalías, ataques adversariales y cambios en el comportamiento del modelo.

5 **Mitigación de sesgos y equidad**	Aborda el sesgo en los datos de entrenamiento y en los modelos de IA para evitar discriminaciones. Implementa medidas para garantizar la equidad y la imparcialidad en la toma de decisiones automatizada.
6 **Enfoque multimodal y diversidad de datos**	Utiliza enfoques multimodales y Datasets diversos en el entrenamiento de modelos de IA para aumentar la robustez y la generalización. Esto ayuda a prevenir ataques que podrían explotar patrones sesgados.
7 **Colaboración y compartición de amenazas**	Fomenta la colaboración entre organizaciones y la compartición de información sobre amenazas, lo que ayuda a abordar amenazas emergentes y a mejorar la eficacia de las defensas basadas en IA.
8 **Seguridad en el desarrollo de IA**	Incorpora prácticas de seguridad desde las primeras etapas del desarrollo de sistemas de IA. Esto incluye la validación de entrada, la protección contra ataques adversariales y la implementación de medidas de seguridad estándar.
9 **Actualizaciones y mantenimiento**	Actualiza de forma regular software y la aplicación de parches que son esenciales para abordar nuevas amenazas y vulnerabilidades.
10 **Cumplimiento normativo y ética**	Cumple con regulaciones y estándares éticos relevantes en el uso de IA en ciberseguridad, ya que es crucial para garantizar prácticas responsables y transparentes.
11 **Resiliencia y planificación de incidentes**	Desarrolla planes de respuesta a incidentes que consideren los posibles fallos de los sistemas de IA y fomenta la resiliencia mediante prácticas de recuperación efectivas.

De acuerdo a un reporte de Gartner de octubre de 2023, sobre las principales tendencias tecnológicas estratégicas para 2024, hemos consolidado 2 programas que creemos que tendrán una mayor relevancia en nuestra región, y estarán en mejor sintonía para la toma de decisiones con el fin de **proteger la inversión y potenciar el crecimiento organizacional** mientras se genera valor.

En concreto, Gartner proyecta 10 principales tendencias se consideren como pilares a la hora de tomar decisiones comerciales y tecnológicas en los próximos años, ya que son capaces de impulsar una empresa rápidamente hacia sus objetivos, especialmente en la era de la Inteligencia Artificial (IA) la cual se encuentra en rápida evolución.



* Fuente: https://www.gartner.es/es/articulos/las-10-principales-tendencias-tecnologicas-estrategicas-de-gartner-para-2024

Considerando las tendencias para proteger la inversión, la inteligencia artificial es una de las áreas tecnológicas con mayor proyección económica a corto y medio plazo. Tanto es así que el valor de mercado de la misma podría superar la barrera de los 300 mil millones de dólares en 2025.

A su vez, Gartner predice que para 2026, la IA generativa cubrirá significativamente el 70% del esfuerzo de diseño y desarrollo de nuevas aplicaciones web y móviles.

Crecimiento proyectado del mercado de IA entre 2021 y 2030

* Fuente: https://es.statista.com/estadisticas/1139768/inteligencia-artificial-vaolr-de-mercado/

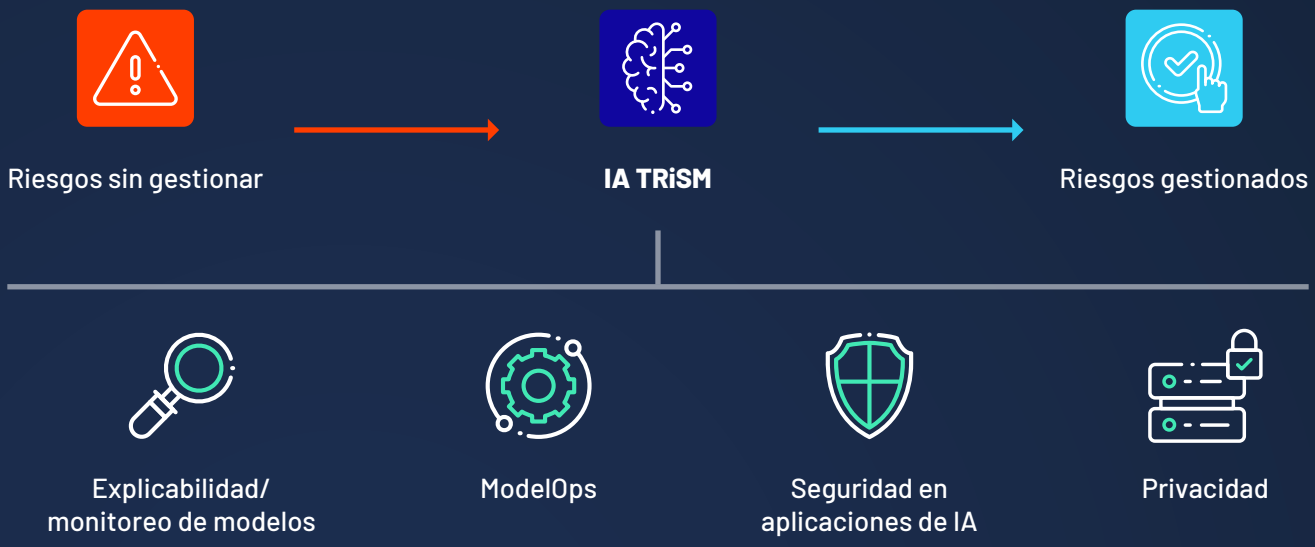
Dicho lo anterior, hemos desarrollado un programa AI TRiSM y otro de Gestión Continua de Exposición a Amenazas (CTEM).

AI Trust, Risk and Security Management (AI TRiSM)

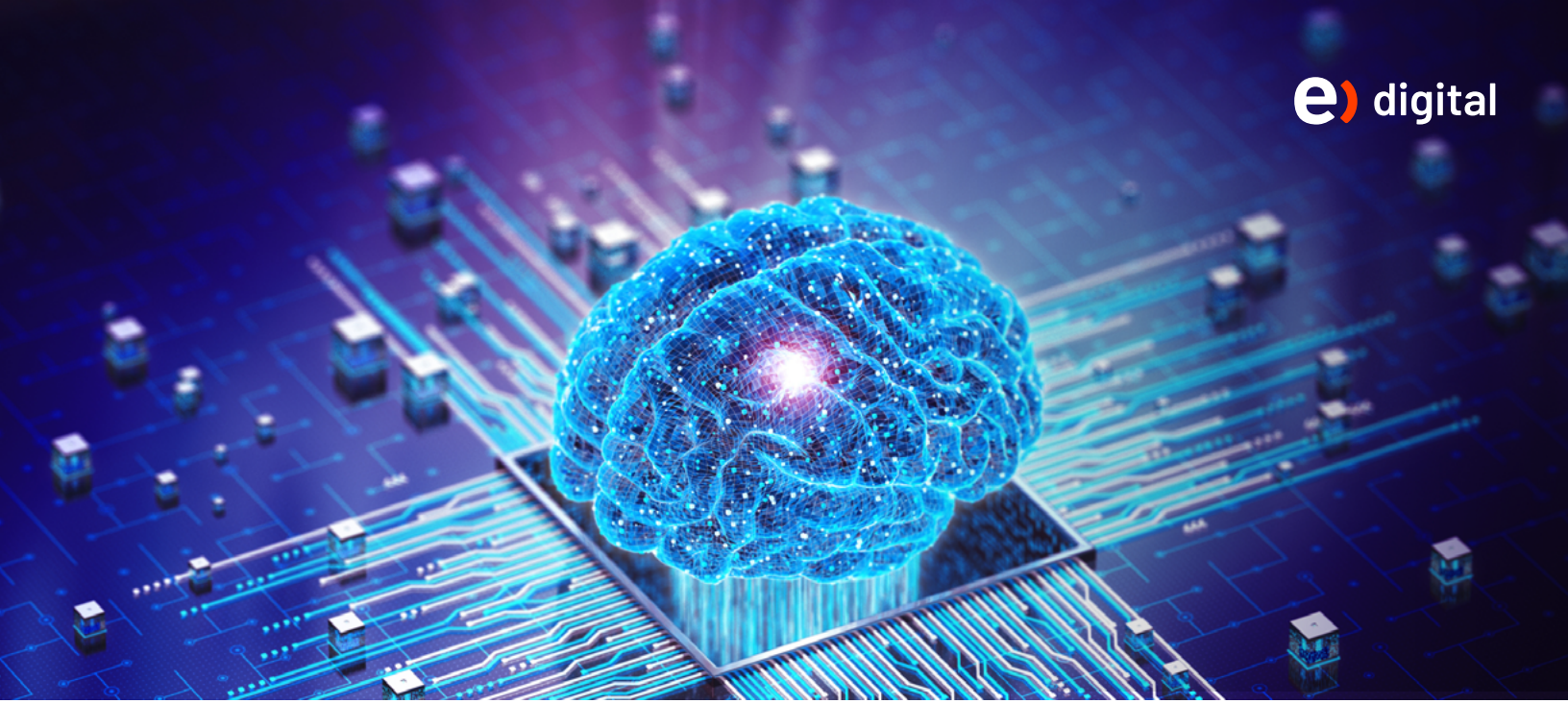
Es una estructura que permite gestionar la confianza, el riesgo y la seguridad en los modelos de inteligencia artificial, asegurando que podamos utilizar esta tecnología de manera óptima.

Considerando la premisa de que los modelos y aplicaciones de IA no son intrínsecamente fiables, dignos de confianza, justos y seguros, **planteamos a continuación un programa AI TRiSM** que nos permitirá tomar decisiones, identificar y mitigar los riesgos de forma proactiva, sin dejar de lado el cumplimiento, la confiabilidad y la privacidad de los datos.

La creación de este programa requiere un **proceso de 4 pasos**.



* Fuente: https://www.gartner.com/en/articles/what-it-takes-to-make-ai-safe-and-effective



1 Explicar claramente los términos y condiciones de la IA

› Identificar fortalezas, debilidades, comportamiento y riesgos.

› Tener visibilidad de los conjuntos de datos utilizados para entrenar los métodos utilizados para seleccionarlos. Esto puede ayudar a sacar a la luz posibles fuentes de sesgo.

2 Gestionar modelos de operación

› Mantener una política "simple", con 3 cosas que no deben hacerse y 2 que sí deben hacerse si se emplean modelos de IA de uso libre en el mercado:

1. No ingresar ninguna información de identificación personal.

2. No ingresar ninguna información confidencial.

3. No ingresar ninguna IP de la organización.

4. Desactivar el historial si se utilizan herramientas externas (como ChatGPT) que permiten esa opción.

5. Supervisar de cerca los resultados, que a veces están sujetos a alucinaciones sutiles pero significativas, errores fácticos y declaraciones sesgadas o inapropiadas.

3 Considerar seguridad en aplicaciones de IA

› Integrar procesos especializados de gestión de riesgos en los modelos de operación (Paso 2) para mantener la aplicabilidad de la IA en conformidad, de manera justa y ética.

› Agregar controles especializados de manera continua y en tiempo real, esto durante el desarrollo, las pruebas y la implementación de modelos y aplicaciones, sin olvidar las operaciones en curso.

4 Promover la privacidad de los datos

› Estar preparado para cumplir, más allá de lo que ya exigen regulaciones como las relacionadas con la protección de la privacidad, pensando en regulaciones directamente relacionadas al uso de la inteligencia artifical (Ley de IA de la UE #AIAct).

La implementación de este programa es importante, porque si no logramos **gestionar de manera consistente los riesgos de la IA** estaremos exponencialmente más propensos a experimentar resultados adversos, como faltas e infracciones en nuestros proyectos.

A su vez, los resultados de la IA que llegan a ser inexactos y/o poco éticos debido a una posible intervención de actores malintencionados, pueden provocar fallas de seguridad, pérdidas financieras, mala reputación y daños sociales. Este mal desempeño de la IA nos lleva derechamente a tomar malas decisiones que serán de impacto para nuestras organizaciones.

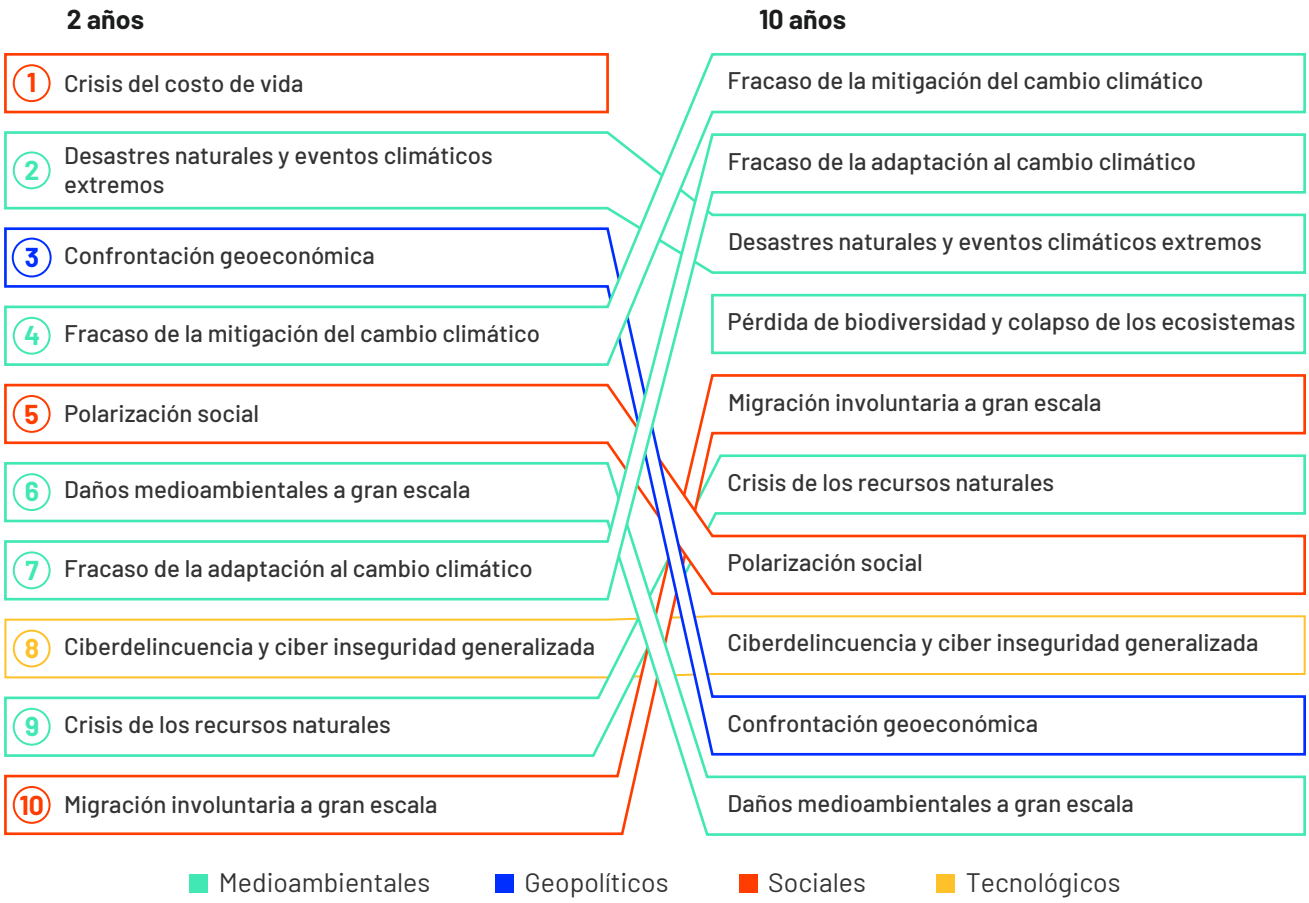
Este programa nos ayudará a definir las capacidades necesarias para garantizar la confiabilidad, la seguridad y la privacidad de los modelos de inteligencia artificial.

Impulsaremos también mejores resultados relacionados con la adopción de la IA, logrando objetivos comerciales y garantizando la aceptación del usuario. Nuestra idea es que estas dimensiones sean consideradas como un conjunto de soluciones para crear protecciones más efectivas en la entrega de inteligencia artificial y establecer un gobierno.

Para 2026, según datos de Gartner, las organizaciones que apliquen controles TRiSM a las aplicaciones de IA aumentarán la precisión de su toma de decisiones, eliminando así el 80% de la información defectuosa e ilegítima.

Continuous Threat Exposure Management (CTEM)

Es un **enfoque que permite responder a ciberamenazas nuevas o en evolución**. Se caracteriza por ser pragmático y sistémico para ajustar continuamente las prioridades de optimización de la ciberseguridad en nuestra organización.

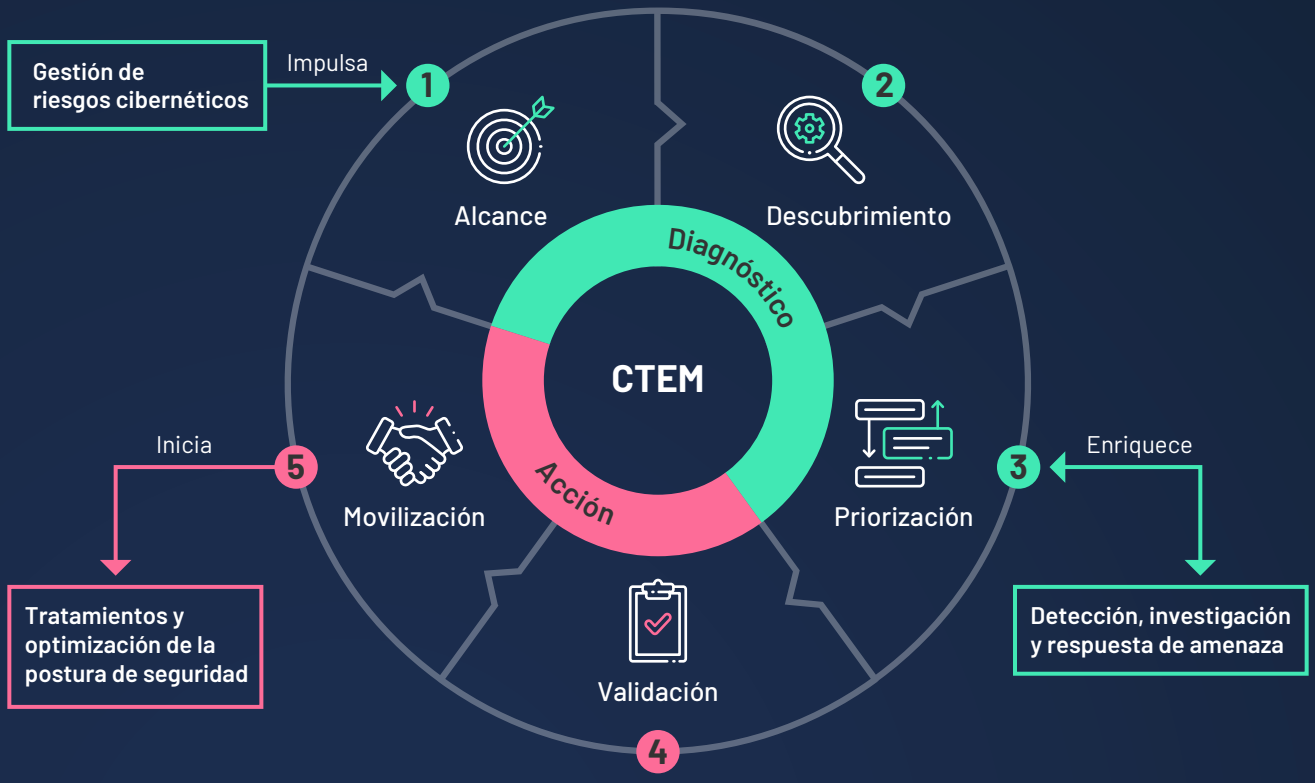


* Fuente: https://es.statista.com/

Su implementación se debe a una creciente exposición de ciberamenazas sin precedentes, ya que según una encuesta realizada por el Foro Económico Mundial en 2023 (referente al capítulo de "Mayores riesgos que acechan al mundo" para los próximos años), **la ciberdelincuencia se posiciona en el 8° lugar como riesgo global de mayor impacto o gravedad probable**.

Considerando que hoy en día ninguna organización puede asegurar estar completamente protegida frente a cualquier evento de ciberseguridad, es que planteamos a continuación un **programa de Gestión Continua de Exposición a Amenazas (CTEM)** que saque a la luz y priorice activamente las mayores amenazas a un negocio.

La creación de este programa requiere un **proceso de 5 pasos**.



* Fuente: https://www.gartner.com/en/articles/how-to-manage-cybersecurity-threats-not-episodes

1 **Definir el alcance de la ciberexposición, identificando prioritariamente las amenazas externas y SaaS**

› Se debe comenzar por determinar la "superficie de ataque" de la organización (puntos de entrada y activos vulnerables) que se extienden más allá del enfoque de los programas típicos de gestión de vulnerabilidades.

› Incluir no solo dispositivos, aplicaciones y aplicaciones tradicionales, sino también elementos menos tangibles, como cuentas corporativas de redes sociales, repositorios de códigos en línea y sistemas integrados de cadena de suministro.

2 **Desarrollar un proceso de descubrimiento de activos y perfiles de riesgo**

› Si bien muchos procesos de descubrimiento se centran inicialmente en áreas del negocio que se identificaron en el paso 1, se debe proceder a identificar activos, vulnerabilidades, configuraciones incorrectas y otros riesgos visibles y no tan visibles.

› La confusión entre el alcance y el descubrimiento es a menudo el primer fracaso al crear un programa CTEM. El volumen de activos y vulnerabilidades descubiertos no es un éxito en sí mismo; es mucho más valioso realizar un alcance preciso en función del riesgo empresarial y el impacto potencial.

3 **Priorizar las amenazas con mayor probabilidad de ser explotadas**

› El objetivo de este proceso no es solucionar todos los problemas de seguridad, la priorización debe tener en cuenta:

- Urgencia.
- Seguridad.
- Disponibilidad de controles compensatorios.
- Tolerancia a la superficie de ataque residual.
- Nivel de riesgo que representa para la organización.

› La clave es identificar los activos de alto valor del negocio y centrarse en un plan de tratamiento que los aborde.

4 Validar cómo podrían funcionar los ataques y cómo podrían reaccionar los sistemas

› Analizar todas las posibles rutas de ataque al activo e identificar si el plan de respuesta actual es lo suficientemente rápido y sustancial para proteger la organización.

› Es clave convencer a todas las partes interesadas del negocio para que se pongan de acuerdo sobre qué factores desencadenantes conducen a la remediación.

5 Movilizar a las personas e inducir procesos

› No se puede confiar totalmente en la promesa de una solución automatizada, más bien, hay que comunicar el plan CTEM al equipo de seguridad y a las partes interesadas de la empresa, y asegurándonos de que se comprenda.

› El objetivo del esfuerzo de "movilización" es garantizar que los equipos pongan en práctica los hallazgos de CTEM, reduciendo cualquier obstáculo para las aprobaciones, los procesos de implementación o los despliegues de mitigación.

› Documentar los flujos de trabajo de aprobación entre los equipos.

90% de los hackeos (o ataques cibernéticos) provienen de **estafas de phishing**.

50% de los ciberataques son **en contra de pequeños negocios**.

350% **incrementaron los ransomware** en 2018.

90% de los proveedores de infraestructuras **se han visto afectados desde el 2017**.

Los ataques de **Día Cero** podrían alcanzar la cifra de uno al día en 2024.

Ransomware es el tipo de cibercrimen que crece con mayor rapidez.

La **gestión continua de la exposición a amenazas (CTEM)** es un enfoque eficaz para perfeccionar continuamente las prioridades y caminar en la delgada línea entre dos realidades de seguridad modernas. Las organizaciones no pueden arreglarlo todo, ni pueden estar completamente seguras de qué corrección de vulnerabilidad pueden posponer sin riesgo.

Por ello, este programa nos permitirá **priorizar las amenazas más importantes para cada negocio a largo plazo**.

Para 2026, según datos de Gartner, las organizaciones que prioricen sus inversiones en seguridad basadas en un programa CTEM obtendrán una reducción de un 67% en infracciones o brechas de seguridad.

* Fuente: https://accelerate-technologies.com/challenges/cyber-exposure/

CAPÍTULO 7

Predicciones y aprendizajes clave para el 2024

Aprendizajes 2023

Durante el desarrollo del año 2023, la ciberseguridad y la ciberinteligencia evolucionaron significativamente, dejando algunas enseñanzas importantes como las que se señalan a continuación:

Integración de ciberinteligencia en estrategias de ciberseguridad	Las organizaciones están utilizando ciberinteligencia para anticipar y mitigar ataques, identificando tendencias y tácticas de atacantes.
Automatización y orquestación en threat intelligence	Las herramientas de orquestación permiten integrar esta inteligencia en las operaciones de seguridad de manera más efectiva.
Aumento del uso de Inteligencia Artificial y machine learning	Estas tecnologías se utilizan para analizar grandes cantidades de datos de ciberinteligencia y detectar patrones que pueden indicar una amenaza emergente.
Enfoque en la inteligencia de amenazas	La ciberinteligencia no solo se centra en los indicadores de compromiso (IoCs), sino que también en el contexto que rodea a esos indicadores, como tácticas, técnicas y procedimientos (TTPs) de los atacantes.
Colaboración y cooperación en inteligencia	El aumento en la colaboración entre organizaciones y sectores para compartir información sobre amenazas, incluyó iniciativas públicas y privadas para mejorar la defensa colectiva contra las amenazas cibernéticas.

Enfoque en la inteligencia de amenazas para infraestructuras críticas	Se ha utilizado ciberinteligencia para anticipar y mitigar ataques específicos a infraestructura crítica.
Desafíos de privacidad y legalidad en la recopilación de inteligencia	Con el aumento en la recopilación de datos para ciberinteligencia, surgen preocupaciones sobre la privacidad y el cumplimiento legal, especialmente en diferentes jurisdicciones.
Evolución de las técnicas de Phishing	La ciberinteligencia ha revelado una evolución en las tácticas de Phishing, con ataques más sofisticados y personalizados, lo que requiere estrategias de concientización y entrenamientos más avanzados.
Importancia de las habilidades analíticas en ciberinteligencia	Además de las habilidades técnicas, las habilidades analíticas se han vuelto esenciales para interpretar y aplicar la inteligencia de amenazas de manera efectiva.
Preparación y respuesta a incidentes basada en inteligencia	La ciberinteligencia está impulsando enfoques más proactivos y basados en el conocimiento para la preparación y respuesta a incidentes, lo que permite a las organizaciones actuar rápidamente ante amenazas identificadas.

Estos aprendizajes destacan la importancia de integrar la ciberinteligencia en las estrategias de ciberseguridad y la necesidad de un enfoque proactivo, informado y colaborativo para enfrentar las amenazas cibernéticas en constante evolución.

Predicciones 2024

De acuerdo a las tendencias y desarrollos actuales en el ámbito de la ciberseguridad y ciberinteligencia, a continuación se indican algunas predicciones para el año 2024

› Avances en inteligencia artificial y automatización

Es probable que veamos un mayor uso de la IA y la automatización en la detección y respuesta a amenazas cibernéticas. Esto podría incluir sistemas autónomos capaces de identificar y mitigar ataques en tiempo real.

› Desarrollo de amenazas en IoT y dispositivos conectados

Con la creciente adopción de IoT, es probable que 2024 vea un aumento en las vulnerabilidades y ataques dirigidos a estos dispositivos, lo que requerirá enfoques de seguridad más sofisticados y específicos.

› Ciberseguridad en el espacio de trabajo híbrido

A medida que el modelo de trabajo híbrido se consolida, las estrategias de ciberseguridad deberán adaptarse para proteger redes y datos, tanto en entornos de oficina como remotos, posiblemente a través de tecnologías como Zero Trust.

- **Crecimiento en ataques de Ransomware y extorsión digital**

  Los ataques de Ransomware y las tácticas de extorsión digital es probable que evolucionen, volviéndose más sofisticados y dirigidos, afectando especialmente a las industrias más lucrativas y a las infraestructuras críticas.

- **Desafíos de ciberseguridad en inteligencia artificial**

  A medida que la IA se convierte en una herramienta más común, también lo harán los ataques dirigidos a comprometer o explotar sistemas de IA, lo que requerirá nuevas formas de protección cibernética.

- **Ciberinteligencia para prevenir ataques a la cadena de suministro**

  Los ataques a la cadena de suministro seguirán siendo un punto crítico, impulsando el desarrollo de soluciones de ciberinteligencia más avanzadas para prevenir y mitigar tales amenazas.

- **Regulaciones y cumplimiento más riguroso**

  Podríamos ver un aumento en la regulación gubernamental y los requisitos de cumplimiento en materia de ciberseguridad, especialmente en sectores como la salud, finanzas y tecnología.

- **Aumento del foco en la resiliencia cibernética**

  Es probable que las organizaciones dirijan sus esfuerzos a construir resiliencia cibernética, no solo para prevenir ataques, sino también para garantizar una rápida recuperación y continuidad del negocio tras un incidente.

- **Desarrollo de técnicas de engaño y contrainteligencia**

Podríamos ver un mayor uso de técnicas de engaño y contrainteligencia para desorientar y atrapar a los atacantes, convirtiéndolas en una parte estándar del arsenal de ciberseguridad.

- **Mayor conciencia y formación en ciberseguridad**

Es posible que la educación y la formación en ciberseguridad se vuelvan aún más críticas, tanto en el ámbito empresarial como en la educación en general, para preparar mejor a las personas contra las amenazas cibernéticas.

CAPÍTULO 8

Recomendaciones de seguridad

Hoy en día, **los riesgos en ciberseguridad deben ser vistos como riesgos empresariales** en lugar de simplemente desafíos tecnológicos, y para construir una defensa sólida, las organizaciones deben adoptar una perspectiva holística que abarque el fortalecimiento de sus propias defensas e impongan estándares de seguridad a sus socios estratégicos y proveedores.

Recomendaciones generales

Alcance	Contexto	Recomendación
Incident Response	En la mayoría de los casos, las incidencias se atribuyen a fallos de configuración y malas prácticas en el ámbito de la ciberseguridad.	La gobernanza es esencial para establecer políticas y controles que guíen la estrategia de seguridad de la organización. Es crucial salvaguardar los activos críticos, evaluando cada uno en términos de su importancia.
Vulnerabilidades	La asignación de recursos insuficientes en ciberseguridad seguirá representando un riesgo significativo para las organizaciones. A menudo se subestima la probabilidad y el impacto potencial de las amenazas informáticas.	Efectuar evaluaciones de riesgos periódicas puede ayudar a efectuar una asignación de recursos más precisa y mitigar las amenazas potenciales de manera proactiva (antes que sucedan).

Alcance	Contexto	Recomendación
Infraestructura crítica	Proteger las infraestructuras críticas se ha vuelto una prioridad estratégica debido a su papel integral en el funcionamiento de la economía y la sociedad.	En este mundo digital, la ciberseguridad no es solo una opción, sino una necesidad imperativa que todos, en distintos sectores, debemos adoptar.
Cloud e IA	Debido a los altos flujos de datos y procesamiento de información, todo está migrando a plataformas Cloud y apoyándose en el uso de IA, generando nuevas posibles brechas de seguridad.	Los colaboradores deben ser considerados como una parte crucial de la línea de defensa y recibir capacitación constante en temas de ciberseguridad.

Acciones específicas

Visto el contexto anterior y en base a nuestra experiencia adquirida durante la gestión de incidentes en los últimos años, hemos observado que, en la mayoría de los casos, el vector de entrada, la facilidad de propagación y el impacto resultante de los incidentes se atribuyen a **fallos de configuración y malas prácticas en el ámbito de la ciberseguridad** de las organizaciones.

Por ello, es necesario tomar ciertas **acciones específicas que ayuden a resguardar adecuadamente la información**, prevenir y mitigar el impacto en caso de enfrentar un incidente de ciberseguridad:

- **Clasificar la información en función de su importancia y sensibilidad**

  Los datos pueden clasificarse en niveles como público, interno, confidencial o reservado, lo que proporciona valor y minimiza el riesgo asociado a cada dato que se manipula.

- **Cifrar los datos**

  Garantiza la confidencialidad de la información, especialmente cuando se interactúa con entidades externas y se envían datos sensibles que podrían ser mal utilizados por terceros.

- **Controlar los accesos a la información**

  Garantiza que solo las personas autorizadas tengan permisos adecuados para acceder a ella, esto implica muchas veces contar con controles internos y métodos de autenticación adecuados, limitando el movimiento lateral en la red.

- **Realizar copias de seguridad periódicas**

  Los planes de recuperación de desastres son esenciales en caso de pérdida de datos debido a un ataque cibernético, desastre natural u otro evento, ya que permiten restaurar la información crucial para la continuidad del negocio.

- **Concientización de los colaboradores**

  Instruir a los usuarios sobre las amenazas cibernéticas, las prácticas seguras y la importancia de proteger la información contribuye significativamente a fortalecer la postura de ciberseguridad de una organización y, por lo tanto, a prevenir errores humanos.

- **Implementación de política de contraseñas**

  Se requiere una política sólida que priorice la cantidad y complejidad de los caracteres, además de un cambio frecuente de estas. También se recomienda instruir a los usuarios para que no utilicen la misma contraseña en diferentes sistemas.

- **Establecer una política de actualización de software y sistemas operativos**

  Asegurarse de que todos los servidores y aplicaciones se mantengan actualizados mediante la aplicación oportuna de parches de seguridad, es esencial para mitigar vulnerabilidades conocidas y proteger los activos informáticos contra exploits.

- **Mantener los servicios IaaS (Infraestructura como servicio) actualizados**

  Independientemente que estén en la nube, es responsabilidad del administrador del servidor mantenerlo actualizado.

- **Asegurar adecuadamente los sistemas y servicios de acceso remoto**

  Implementar inicios de sesión mediante VPN permite reducir el riesgo de ataques y brechas de seguridad.

- **Implementar medidas de seguridad adicionales**

  Contar con la autenticación de dos factores o multifactor, para proteger el acceso remoto y prevenir la suplantación de identidad.

- **Monitorear de forma constante y proactiva**

  Llevar un control de los registros de eventos y otros indicadores de actividad sospechosa en los sistemas y redes, permite detectar rápidamente las intrusiones y prevenir que el ataque se propague.

- **Contar con un antivirus-EDR-XDR actualizado**

  Desplegar estas soluciones en todos los endpoints y sistemas de la organización cumple el fin de detectar y prevenir la ejecución y propagación de Malware y otros ataques maliciosos.

- **Realizar pruebas de penetración regulares**

  Ayuda a identificar vulnerabilidades de seguridad antes de que sean explotadas por un atacante. Las pruebas de penetración también pueden proporcionar información valiosa sobre la eficacia de los controles de seguridad existentes.

- **Aplicar el principio de menor privilegio en el entorno AD**

  Significa otorgar únicamente los permisos y privilegios necesarios para que los usuarios realicen sus trabajos. Esto puede reducir la exposición a riesgos de seguridad si se ve comprometida una cuenta de usuario.

- **Realizar auditorías de seguridad regulares**

  Ayuda a identificar cuentas con altos privilegios que no se utilizan con frecuencia y que podrían ser eliminadas e identificar permisos innecesarios que se han otorgado por error o por malas prácticas.

- **Tener un plan de respuesta a incidentes**

  Es vital contar con un protocolo de seguridad claro y bien definido, que incluya los procedimientos a seguir para contener el incidente, investigar la causa raíz y tomar medidas correctivas para evitar futuras brechas.

- **Contar con el monitoreo de tráfico**

  Es altamente recomendable contar con algún monitoreo de tráfico para evitar ataques como inyección SQL o fuerza bruta.

Conclusiones

De acuerdo a nuestras predicciones, **existe certeza de que habrá un aumento de incidentes, cuyo impacto y costos serán cada vez más devastadores.**

En gran parte, esto se debe a que estamos en la cúspide de múltiples innovaciones sociales, económicas y tecnológicas que están cambiando nuestra vida tal como la conocemos, **ante una convergencia intensiva de lo digital y lo análogo.**

› Hace casi una década, un estudio de IBM proclamó que los datos prometen ser para el siglo XXI lo que la energía de vapor fue para el siglo XVIII, la electricidad para el siglo XIX y los hidrocarburos para el siglo XX.

› Según el reporte de Cybersecurity Ventures, el mundo almacenará 200 zettabytes de datos para 2025. Esto incluye datos en infraestructuras de Tecnologías de Información públicas y privadas, en infraestructuras de servicios, en centros de datos, en dispositivos informáticos personales (PC, portátiles, tablets y teléfonos) y en dispositivos IoT (Internet de las cosas).

› Durante los últimos 50 años, la superficie de ataque del mundo ha evolucionado desde sistemas telefónicos hasta una vasta esfera de datos que supera ampliamente la capacidad de la humanidad para poder protegerla.

De acuerdo a esto, **el mayor desafío de hoy es poder anticipar las necesidades tecnológicas futuras y al mismo tiempo asegurar la infraestructura y los ciberactivos existentes** (superficie de ataque en expansión) para minimizar los riesgos y aprovechar al mismo tiempo las nuevas oportunidades.

Cualquier enfoque de ciberseguridad debe estar en sintonía con los objetivos comerciales de una organización, pero el logro de esa armonía a menudo se ve desviado por numerosas fuerzas externas, como la disrupción del mercado, impulsada por el cambio tecnológico, regulaciones globales complejas, tensiones geopolíticas e incertidumbres económicas, todo esto pondrá a prueba el enfoque de las organizaciones ante el riesgo y la resiliencia.

En **Entel Digital**, estamos seguros de que nuestros servicios, soluciones, **recomendaciones y predicciones contribuirán de muy buena manera a la próxima ola de transformación tecnológica** que experimentan las organizaciones en la región, combinando inteligencia artificial, aprendizaje automático y otras innovaciones digitales que permitirán mayores eficiencias y experiencias convincentes para nuestros clientes.

A medida que los negocios alcanzan nuevas y mejores posiciones, **pondremos atención directamente proporcional a la ciberseguridad**, una tendencia que ya está en marcha y que cobrará mucha más fuerza los próximos años.

CAPÍTULO 9

Nuestro Portafolio

Durante el año 2023, hemos sido testigos de cómo evolucionaron las motivaciones de los ciberactores maliciosos, a medida que colaboran y ofrecen sus habilidades para ser contratados, con el objetivo de causar perturbaciones financieras y también caos social.

Estos grupos emplean agresivamente la inteligencia artificial, para ganar más eficiencia y precisión que nunca, lo que hace que **nuevos tipos de ciberataques sean un desafío mayor para las empresas**, lo que requiere de estrategias de ciberseguridad más proactivas y adaptables.

Hoy en día, la ciberseguridad se vuelve clave en nuestras organizaciones, considerando que se prevén costos globales de **daños causados por ciberdelitos que crecerán en un 15% anual durante los próximos 5 años**, alcanzando los 10,5 billones de dólares anuales para 2025, frente a los 3 billones de dólares registrados en 2015.

Pronóstico de costos globales por ciberdelitos para 2024:

- **$9,2 billones** de dólares **al año**.
- **$767 mil millones** de dólares **al mes**.
- **$192 mil millones** de dólares **por semana**.
- **$27,4 mil millones** de dólares **al día**.
- **$1.142 millones** de dólares **por hora**.
- **$19 millones** de dólares **por minuto**.
- **$316,667** USD **por segundo**.

(Ref: Cybersecurity ventures – Official Cybercrime report).

Desafíos actuales

El ciberdelito está afectando a empresas de todos los tamaños. Cualquiera que quiera garantizar su tiempo de actividad, reputación y seguridad de los datos (de empleados y clientes), tiene la responsabilidad de invertir en ciberseguridad y adelantarse a las disrupciones.

A medida que la guerra cibernética se extiende a lo largo de geografías globales, el aumento de la actividad maliciosa ha impulsado una mayor cooperación internacional entre los gobiernos y los proveedores de ciberseguridad para **contrarrestar tales amenazas**, empleando tácticas, técnicas y procedimientos cada vez más sofisticados.

De acuerdo a nuestra última liberación del panorama de amenazas para la región, **el crecimiento anual del número de víctimas en Chile es de un 34%**, acompañadas de cerca de 12 millones de ataques anuales, en su mayoría del tipo Phishing. Teniendo en cuenta estas estadísticas, debemos ir un paso adelante y **pasar de medidas de ciberseguridad reactivas a medidas derechamente proactivas y gestionadas**.

* Fuente: https://cybersecurityventures.com/cybercrime-to-cost-the-world-9-trillion-annually-in-2024/

Inteligencia sobre amenazas cibernéticas

Un elemento central de estos esfuerzos es la **necesidad de contar con inteligencia sobre amenazas cibernéticas**, tanto externas como internas y que sea relevante y contextual para cada organización, considerando factores como la superficie de ataque, niveles de exposición y la efectividad de sus controles de seguridad.

Este enfoque nos favorecerá a la hora de mantener el cumplimiento de las presiones regulatorias, **un área donde la inteligencia contextual sobre amenazas también ofrece un valor significativo**.

Identificar las tendencias de amenazas

En el ámbito de la ciberseguridad, **predecir exactamente lo que sucederá de un día para otro es imposible** y menos pensar en una bala de plata que solucione todos los problemas. No obstante, apoyándonos en un equipo experto y utilizando servicios de inteligencia de amenazas de carácter integral y contextual, que además considere capacidades avanzadas de IA, **lograremos identificar las tendencias de amenazas que probablemente nos afecten en un futuro**, lo que nos permitirá enfrentarlas de una mejor forma.

Recomendaciones

Inevitablemente, los ciberactores responsables de las amenazas encontrarán la forma de trabajar mejor, más rápido y de manera más inteligente.

De acuerdo a lo anterior, **elaboramos recomendaciones desde 3 perspectivas** con la finalidad de brindar lo necesario para mantener seguros los ciberactivos, se puedan complementar con los procesos de mitigación de riesgos y permitan proyectar un plan de ciberseguridad sustentable y equilibrado.

1 Ecosistema receptivo y resiliente

Es necesario ir en búsqueda de **capacidades avanzadas de detección y respuesta gestionada**, a través de un enfoque continuo de gestión de riesgos y amenazas, agregando capas de validación de los controles de ciberseguridad, acercándose lo más posible a una inmunidad digital.

Se debe considerar la **aplicación de las siguientes dimensiones**:

1.1 Gestión de exposición frente a amenazas: ajustar continuamente las prioridades de optimización de ciberseguridad, desde un enfoque pragmático, eficaz y sistémico.

1.2 Inmunidad de los sistemas digitales: a través de inversiones equilibradas en prevención, detección y respuesta, es necesario minimizar defectos y/o posibles fallas, con la finalidad de protegernos antes y durante un ciberataque.

1.3 Validación de controles de ciberseguridad: combinando técnicas, procesos y herramientas, es posible validar el cómo un ciberatacante explotaría una vulnerabilidad expuesta, y en paralelo monitorear cómo se comportan los sistemas y procesos de protección.

2 Enfoque de consolidación

Considerar **simplificar las operaciones con otras plataformas,** incorporando nuevas soluciones para tener mayor cobertura de la superficie de ataque. Es necesario aplicar las siguientes dimensiones:

2.1 Consolidación de Plataforma de Ciberseguridad: reducir la complejidad, simplificar las operaciones y buscar que los análisis sean más eficientes. Así una organización utilizará menos proveedores y se beneficiará de una mayor eficiencia e integración (más funciones en menos productos).

2.2 Transformación del modelo operativo de seguridad: distribuir la tecnología y el trabajo analítico para crecer en volumen y variedad de manejo de datos, con esto la toma de decisiones sobre riesgos de ciberseguridad será más veloz (acelerará resultados comerciales).

2.3 Seguridad Modular: dar un enfoque en que los controles de ciberseguridad se integren a nivel de diseño y luego se apliquen a nivel modular en implementaciones de tecnología flexible. La finalidad es proteger los cambios del negocio y se apliquen a todos los aspectos de un proceso comercial.

3 Equilibrio y balance

Promover un **equilibrio entre las personas, procesos y tecnología** para reducir con éxito el riesgo en ciberseguridad. Para ello es necesario considerar las siguientes dimensiones:

3.1 Diseño de seguridad centrado en el ser humano: priorizar la experiencia del usuario, en lugar de solo las consideraciones técnicas, esto en todo el ciclo de vida de la gestión de controles. Basándose en las ciencias de comportamiento, (UX) y disciplinas relacionadas, en búsqueda de minimizar el comportamiento inseguro de los colaboradores.

3.2 Mejora de la gestión de personas: cambiar el enfoque a tácticas de gestión de talento centradas en el colaborador para atraerlo y retenerlo. Cuando los directores de seguridad de la información (CISO) hacen esto, ven mejoras en la madurez funcional y en técnicas del equipo.

3.3 Aumento de la supervisión en capas directivas (C-Level): atender a la ciberseguridad como parte de las actividades de gobierno y supervisión. Esta tendencia requerirá experiencia adicional sobre ciberseguridad en el directorio.

Nuestros servicios y soluciones

En base a estos **3 pilares**, hemos diseñado nuestros servicios y soluciones de ciberseguridad.

Sobre una estructura modular e integrada, estos servicios y soluciones nos permiten **atender y gestionar de forma transversal los riesgos de ciberseguridad de las organizaciones**, estableciendo lineamientos y bases estratégicas, tácticas y operativas con el objetivo de responder de forma efectiva ante la materialización de un incidente y en consecuencia contar con operaciones de negocio más resilientes.

Tecnologías	Categorías	Servicios y soluciones
Plataforma de seguridad nativa en la nube (**CNSP**).	**Seguridad en la nube**	**Servicios CNAPP** CSPM / CIEM / CWP / CodeSec(IaC) / CloudNetSec.
Detección y respuesta extendidas (**XDR**). **NG-SIEM**.	**Gestión integral del riesgo**	**Servicios MDR** Búsqueda activa de amenazas / equipo de respuesta ante incidentes. **Servicios NG CSOC** NG-SIEM / XSOAR / XSIAM.
Escaneo e inteligencia de amenazas. Simulación de brechas y ataques (**BAS**).	**Inteligencia de amenazas**	**Servicios de gestión de la superficie de ataque** Gestión de vulnerabilidades / Exposición cibernética / Inteligencia de ciberamenazas. **Servicios BAS** Plataforma de Simulación de brechas y ataques.
Protección de **WAF** y **APIs**. Autoprotección de aplicaciones en tiempo de ejecución (**RASP**). Protección de datos y privacidad.	**Seguridad de datos y aplicaciones**	**Servicios WAPP** WAF / API / Bots /DDoS / ATO /CSP. **Servicios de protección de aplicaciones en tiempo de ejecución** Autoprotección de aplicaciones en tiempo de ejecución / DevSecOps. **Servicios de data fabric** DBF / Enmascaramiento / Encriptación.
PAM / IAM / **Autenticación**.	**Gestión de identidades**	**Servicios de verificación y acceso** PAM / IAM / IGA.
Borde de servicio de **acceso seguro** y **ZTNA**. Torre de seguridad **Entel Secure Cloud**.	**Arquitectura de malla de ciberseguridad**	**Servicios de acceso a la red de confianza cero (ZTNA)** NGFWaaS / SWG / CSB / ADEM. **Seguridad como servicio (SECaaS)** NGFW / Prevención de amenazas / WAF / AniDDoS.

Ecosistema de Socios Tecnológicos

Nuestros servicios y soluciones están respaldadas por tecnologías de vanguardia y **alianzas con partners tecnológicos de primer nivel**, las cuales agrupamos según nivel de expertise y posicionamiento estratégico.

Nivel de socio Premier

paloalto NETWORKS | imperva | IBM Security

FORTINET | MANDIANT NOW PART OF Google Cloud | VIRUSTOTAL

CISCO Partner | Microsoft Gold Partner | Google Partner

Nivel de socio Advanced

TREND MICRO | tenable | txOne networks

radware | kaspersky | Cymulate

Nivel de socio Select

Trellix | proofpoint. | FORCEPOINT

Outpost24 | KnowBe4 | f5

Nivel de socio Reseller/Distributor

appdome | appgate | THALES

vicarius | OFFENSIVE security | CYBERARK

COMMVAULT | SecurityScorecard

Glosario de términos

- **2FA:** Doble Factor de Autenticación
- **AD:** Active Directory
- **APT:** Advanced Persistent Threat (Amenaza persistente avanzada)
- **AV:** Antivirus
- **BackDoors:** Puerta Trasera
- **BITB:** Browser In The Browser
- **C&C:** Command and Control (Mando y control)
- **CA:** Autoridad Certificadora
- **CaaS:** Cibercrimen como servicio
- **CAPTCHA:** Prueba pública de turing completamente automatizada para diferenciar a la computadora de los humanos
- **CISA:** Agencia de Ciberseguridad y Seguridad de la Infraestructura
- **CVE:** Common vulnerabilities and exposures (Vulnerabilidades y exposiciones comunes)
- **CVSS:** Common Vulnerability Scoring System (Sistema de puntuación para los CVE)
- **Data Breach:** Robo de datos de organizaciones debido a malas prácticas en configuraciones de seguridad
- **Data Leak:** Robo de datos mediante un ciberataque que ha comprometido parte de la infraestructura de una organización
- **DDoS:** Acrónimo de denegación de servicio distribuida. Técnica que utiliza numerosos hosts para realizar el ataque
- **DDW:** Dark o Deep web
- **DNS:** Sistema de nombres de dominio
- **DoS:** Denegación de servicio
- **Dwell Time:** Tiempo de permanencia
- **Framework:** Esquema o marco de trabajo que ofrece una estructura base
- **FTP:** Protocolo de transferencia de archivos
- **FW:** Firewall
- **HaaS:** Hacking as a Service
- **Hostings:** Alojamiento web
- **HTTP:** Protocolo de transferencia de hipertexto
- **HTTPS:** Protocolo seguro de transferencia de hipertexto
- **HUMINT:** Inteligencia que proviene de la información obtenida y facilitada por fuentes humanas.
- **IAM:** Gestión de identidad y acceso
- **ICS:** Abreviación de sistema de control industrial. Es un sistema de información utilizado para controlar procesos industriales como la fabricación, el manejo de productos, la producción y la distribución.
- **IoA:** Indicadores de amenaza
- **IoC:** Indicadores de compromiso
- **IT:** Tecnología de la Información
- **Leak:** Fuga de información
- **MaaS:** Malware as a service (Malware como servicio)
- **MDR:** Detección y respuesta gestionada
- **MISP:** Malware Information Sharing Platform
- **OT:** Tecnología de las operaciones
- **PoC:** Prueba de concepto
- **RaaS:** Ransomware as a service (Ransomware como servicio)
- **RAT:** Remote Access Trojan (Troyano de acceso remoto)
- **RR. SS.:** Redes Sociales
- **SIEM:** Security Information and Event Management (Correlacionador de eventos)
- **SOAR:** Security Orchestration, Automation and Response (Herramienta de seguridad, orquestación y respuesta automatizada)
- **SOC:** Security Operations Center
- **SSL:** Secure Sockets Layer (Seguridad de la capa de transporte)
- **TLD:** Top Level Domain
- **TLP:** Traffic Light Protocol
- **TTP:** Tácticas, Técnicas y Procedimientos
- **VM:** Virtual Machine (Máquina virtual)
- **VPN:** Red Privada Virtual
- **WAF:** Web Application Firewall
- **XDR:** Herramienta de Detección y Respuesta Extendida
- **Zero-Day:** Vulnerabilidad de software, totalmente desconocida tanto para el fabricante del software, como para los motores de detección de amenazas

Sobre los Autores

El presente informe del estado de la ciberseguridad fue confeccionado por la Unidad Especializada de Ciberseguridad de Entel Digital y su Centro de Ciber Inteligencia (CCI).

Autores del Informe:

- **Gerente de la Unidad de Ciberseguridad**
  Cyril Delaere
- **Director del Centro de Ciberinteligencia**
  Eduardo Bouillet Carroza
- **Jefe de Área CSOC**
  Matias Villegas Becerra
- **Especialista Senior Operación Ciberinteligencia**
  Jonathan Armijo Catalán
- **Experto en Ciberseguridad**
  Luis Elola Aránguiz

Equipo Centro de Ciber Inteligencia:

- Álvaro Salinas Jiménez
- David Andrade Bermudez
- Joaquín Miranda Gajardo
- Ernesto Lavanderos Saavedra
- Inés Von Borries
- Lorena Pérez Contreras
- Marco Arancibia Ocampo

Equipo de Marketing y Comunicaciones:

- José Balmaceda Bull
- Marcela Pastor
- Andrés Bahamondes
- Ronald Caro


digital
Juntos, tu empresa evoluciona