Progress. Protected.

SECURITY REPORT

< LATINOAMÉRICA 2022 >

CONTENIDOS

INTRODUCCION

El **ESET Security Report** (ESR) es un informe publicado cada año, en el cual desde el laboratorio de ESET Latinoamérica se aborda el estado de la ciberseguridad corporativa en la región. Este se basa en el análisis de encuestas realizadas a profesionales de tecnología y gerencias de compañías del continente latinoamericano.

La edición de 2022 es **resultante de la combinación de más de 1800 encuestas dirigidas a profesionales**, que fueron completadas en eventos realizados por ESET -principalmente en formato digital- en 17 países, e información obtenida de datos telemétricos de los sistemas de ESET, así como tendencias y noticias relacionadas al ámbito de la ciberseguridad, tanto a nivel regional como global.

Uno de los eventos más relevantes en materia corporativa del año 2021 es el **asentamiento del teletrabajo como realidad**. En la mayor parte del continente se produjo una relajación de las medidas de aislamiento impuestas por la pandemia del COVID-19 que regían el año anterior, lo cual significó un abandono del trabajo remoto como obligación. Sin embargo, compañías de todo calibre y trabajadores encontraron en esta modalidad una variedad de beneficios, como un mejor balance de vida personal y profesional, o mejoras de resultados, y es por ello que la modalidad no fue abandonada inmediatamente. Esto, como se reflejará más adelante, tiene un impacto en la seguridad corporativa.

Otros de los eventos importantes que marcaron al año 2021 en materia de ciberseguridad y cibercrimen en el ámbito corporativo fueron los **grandes ataques y caídas de bandas de ransomware, las vulnerabilidades de gran criticidad y gran presencia como Log4Shell y el aumento desmedido de ataques que utilizan la modalidad de afección a la cadena de suministros**.

Los datos presentados ofrecen una mirada amplia: **desde el lado ofensivo reflejado en las preocupaciones e incidentes recibidos en las compañías; y desde el lado de defensa de los activos de las compañías, como tecnologías de seguridad implementadas y medidas en materia de gestión**. Como agregado se obtiene información en cuanto al presupuesto destinado a estas, así como indicadores relacionados al trabajo remoto, dos variables que son indispensables a la hora de analizar las primeras.

HALLAZGOS

El país con la mayor cantidad de detecciones es **Perú** (18%), seguido inmediatamente por **México** (17%), **Colombia** (12%), **Argentina** (11%) y **Ecuador** (9%).

Dos tercios de los encuestados señaló la **infección con códigos maliciosos** como la mayor preocupación en materia de ciberseguridad. A esta le sigue la preocupación por el **robo de información** (62%).

El **48%** de los encuestados afirmó haber sufrido algún **incidente de ciberseguridad**.

El **36%** de los encuestados afirmó que el **presupuesto asignado** al área de ciberseguridad **aumentó** con respecto al año anterior, pero más de la mitad (**63%**) considera que **no es suficiente**.

La adopción de **soluciones de seguridad para dispositivos móviles** sigue presentando un porcentaje de adopción bajo, con apenas un **10%** de los encuestados utilizando alguna.

Los **troyanos** que descargan o liberan amenazas en los dispositivos siguen siendo de los más detectados, con **más de 2 millones de detecciones** en el año.

El **phishing** se presenta como una vía de infección estable en el tiempo, contando con un promedio de alrededor de **10 mil detecciones** diarias.

Las **detecciones de vulnerabilidades** rompieron un nuevo récord en 2021, con **más de 22 mil reportes** a lo largo del año. Esto resultó en un promedio de **4100 exploits** detectados a diario.

NUEVO RECORD

PERCEPCIÓN DE LAS COMPAÑÍAS

PREOCUPACIONES

Si bien se trata de un dato subjetivo, las **preocupaciones en torno a la seguridad corporativa** le dan forma a ciertos aspectos abordados posteriormente en este informe. Por ejemplo, una mayor preocupación en cuanto a **robo de información** puede traducirse en la implementación de tecnologías para la protección de la misma, como el **doble factor de autenticación**. Además, comparar la visión sesgada de las compañías, influenciada por su capacidad de detección de incidentes y la información que poseen sobre el estado de la ciberseguridad en general, con el estado objetivo de los incidentes **a través de la telemetría de los sistemas de ESET, puede permitir un análisis más profundo sobre la capacidad de detección y autoconocimiento en materia de seguridad de la información de las mismas.**

Estas preocupaciones pueden ser influenciadas por una **multitud de factores**. Entran en juego variables dependientes de las mismas compañías, como los **sistemas en funcionamiento que posean** y las **medidas de protección que adopten**, pero también influyen eventos como la **visibilidad de noticias y ataques** o **el clima** tanto nacional como internacional en la temática.

Como resultado de las encuestas realizadas a personal de compañías en toda Latinoamérica, la principal preocupación sigue siendo la **infección con códigos maliciosos** (**66%**). Esta tendencia, que también se ubicó en el primer lugar en el ESR 2021 y presenta un ligero aumento en esta edición, indica que **dos de cada tres encuestados** afirma tener a incidentes **relacionados a malware como una preocupación latente**. Nuevamente, esto podría deberse al aumento de incidentes y noticias destacadas relacionadas a infecciones de códigos maliciosos, tanto propias como ajenas, nacionales o internacionales, de distintos rubros corporativos, entre otros.

DOS DE CADA TRES ENCUESTADOS AFIRMA TENER PREOCUPACIÓN CON LOS INCIDENTES RELACIONADOS A MALWARE

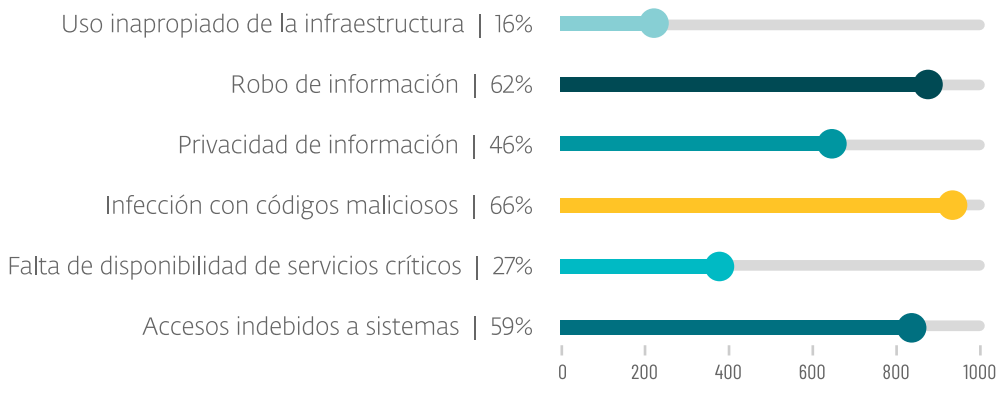

GRÁFICO 1. *Principales preocupaciones de las empresas de América Latina en temas de seguridad.*

En segundo lugar se encuentra el **robo de información**, con el **62%**. Esta categoría, que engloba ataques como el espionaje o robo de archivos confidenciales, obtiene su relevancia por amenazas como el **ransomware**, los **códigos espía** y las **intrusiones por vulnerabilidades** o **backdoors**, ataques que se solidificaron como realidad en estos últimos años y que combinan las dos principales preocupaciones con la tercera: los **accesos indebidos a los sistemas corporativos**.

Finalmente, la preocupación por la **falta de disponibilidad de servicios críticos** sufrió una ligera caída con respecto a la edición 2021. Esto puede deberse, en parte, a la vuelta a la presencialidad en los espacios de trabajo, siendo el día a día del negocio menos dificultoso o dependiente de un servicio crítico que no se encuentre disponible.

INCIDENTES REPORTADOS

En un mundo atravesado por factores tecnológicos, y en donde transacciones y negocios no son ajenos a esta característica, es sencillo ver por qué los incidentes relacionados a la seguridad de los activos de una compañía pueden traer consecuencias altamente relevantes. **Desde interrumpir la operatoria, pasando por la ruptura de confianza con clientes, hasta la pérdida de dinero de manera directa**.

Existen varias formas para medir esta variable -la de incidentes provocados- y una de ellas es la consulta directa a las compañías dentro de la región. Sin embargo, entrelazado a este se encuentra otro aspecto: la **capacidad de detección de incidentes de manera interna**, que también da forma a la percepción subjetiva de la ciberseguridad de las compañías de Latinoamérica, así como al estado de la temática en la región.

Dentro de los incidentes que pueda recibir una compañía, es inevitable que solo un porcentaje de ellos sean detectados. Este porcentaje dependerá de varios factores como la complejidad de los ataques, pero principalmente recaerá en las herramientas tecnológicas, humanas y de gestión que se utilicen dentro de la misma. En otras palabras, **una corporación tiene conocimiento de tantos incidentes en su red como buenas son sus capacidades de detección**, más aun considerando que las detecciones de amenazas dirigidas a corporaciones vienen aumentando año tras año.

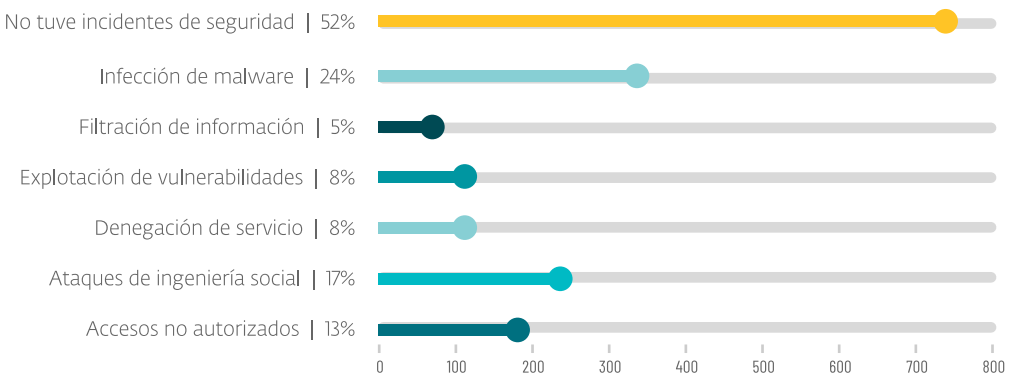

GRÁFICO 2. *Indicentes de seguridad reportados por empresas de América Latina en 2021.*

En este sentido, y dentro de las encuestas realizadas por ESET a compañías de toda Latinoamérica, la mitad de los encuestados afirmó **no haber sufrido incidente alguno**. Sin embargo, si esto es acompañado con el aumento año a año de detecciones, puede ser un dato que da a pie una reinterpretación: el **52%** de los encuestados **no reconoció incidentes de seguridad** en los activos de su organización, más allá de efectivamente haberlos sufrido o no. Este número sufrió un gran aumento, en comparación al informe del año anterior, el cual agrupaba al 39% de los encuestados en esta categoría.

Por otro lado, los incidentes relacionados a infecciones por **malware** siguen siendo de los más recibidos, en donde **1 de cada 4** responsables **afirmó haber sufrido algún tipo de ellos**, lo cual no es un dato menor. Estos tuvieron dos principales vías de entrada, el phishing y las vulnerabilidades, como veremos a lo largo de este documento.

1 DE CADA 4 RESPONSABLES AFIRMÓ HABER SUFRIDO ALGÚN INCIDENTE VINCULADO A MALWARE

En segundo lugar, con el **17%** de afirmaciones de los encuestados, se encuentran los **ataques de ingeniería social**. No es de sorprender la ligera disminución con respecto al informe del año anterior, dado que el trabajo remoto dejó de ser una obligación para las corporaciones. Esto significa que cada vez menos interacciones entre colaboradores, como comunicaciones e invitaciones a reuniones, se realizan por medios digitales. Es decir, los cibercriminales tienen una menor cantidad de temáticas para suplantar o engañar a sus víctimas en el ámbito corporativo, en comparación a años anteriores. Sin embargo, y **gracias al asentamiento del trabajo híbrido**, engaños que utilicen como excusa herramientas, servicios o medios de comunicación introducidos por esta "nueva" modalidad laboral no desaparecerán. Más aún y para años posteriores, estas temáticas se sumarán a las usuales, tanto las que son atemporales como las basadas en temas de actualidad del momento.

INCIDENTES

A la hora de hablar del estado de la ciberseguridad corporativa, es importante conocer no solo lo que sucede dentro de la organización propia, sino también tener una **visión integral**, particularmente de la región. Poder determinar **factores comunes en campañas maliciosas** o **analizar los métodos de infección más utilizados** son algunos ejemplos de los tantos indicadores que se deben tener en cuenta al proteger una organización, observando otras en áreas, regiones o incluso tamaños similares.

El incremento del cibercrimen como negocio provoca año a año un aumento de demanda y dinero circulante en los mercados clandestinos. Esto trajo consigo una nueva tendencia, a partir del año 2021: la **exposición de los mercados oscuros en sitios y redes de acceso sencillo**. En otras palabras, los cibercriminales ya no deben acceder a lugares ocultos de la internet para poder obtener métodos de ataque, amenazas o información de sus víctimas, sino que estos se encuentran a algunos clics de distancia, disponibles para quien lo solicite tanto en sitios de la web superficial como en redes sociales anóni-

mas como Telegram. Con la facilidad de acceder a los recursos necesarios para cometer un ataque informático, combinado con los millones de dólares que el cibercrimen mueve, es lógico ver por qué cada vez más personas se unen al mundo del cibercrimen enfocado a corporaciones, **lo cual resulta en un incremento sostenido de ataques**.

RANSOMWARE

El *ransomware* continúa siendo una amenaza que figura constantemente en titulares de ciberamenazas y ataques, particularmente aquellos orientados a compañías. Sin ir más lejos, y según datos revelados por la oficina de Control de Crímenes Financieros (FinCEN) de los Estados Unidos, solo en este país entre enero y junio de este año el promedio mensual de transacciones en Bitcoin que se sospecha están relacionadas con el *ransomware* es de **66.4 millones de dólares**. Solo en el ataque a *Kaseya*, compañía prestadora de servicios que fue víctima intermedia de un ataque a la cadena de suministros, los operadores detrás del *ransomwareREvil* demandaron un pago de **70 millones de dólares** por la herramienta de descifrado para que las víctimas **pudieran recuperar los archivos secuestrados**.

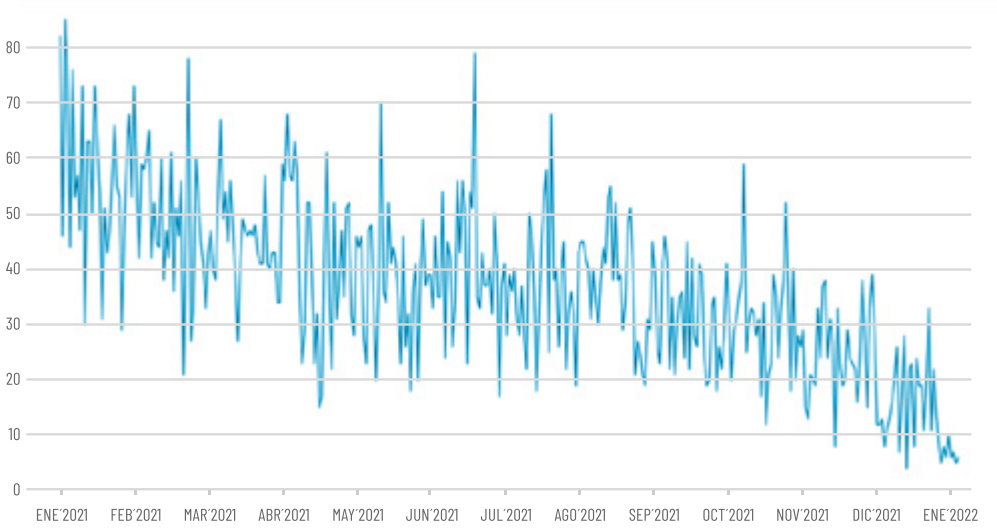

Gráfico 3. *Detecciones de ransomware durante 2021*

Si bien los datos de la **telemetría de ESET** arrojan una disminución de más de un tercio de las detecciones reportadas durante 2020, tendencia que también se dio en el informe anterior, esto **no quiere decir que hay un menor accionar en cuanto a la amenaza en ámbitos corporativos**. Sin ir más lejos, un informe de DarkTracer recopiló más de 2300 publicaciones de organizaciones víctimas en foros de bandas de ransomware operando bajo el modelo de RaaS (o ransomware como servicio). Esto, en comparación a la misma estadística durante el año 2020 en donde se encontraron **1300 artículos**, representa un aumento del **76%** de entradas en sitios web dedicados a la extorsión, filtrado de archivos y alardeo de víctimas de distintas bandas de *ransomware*. Más aún, se estima que en promedio cada víctima pasó a estas bandas **139.739 dólares** para recuperar sus archivos y sistemas, según un estudio de *Coveware*.

Entonces, y combinando esta información, queda claro que una disminución de detecciones de tipo *ransomware* no indican necesariamente una menor cantidad de códigos maliciosos. Ahora, si observamos las campañas maliciosas más complejas, como son aquellas que contienen un **ransomware como amenaza final**, podemos encontrar otro tipo de piezas de *malware* involucradas en este tipo de ataques que buscan inyectar el *malware*. Por ejemplo, el ransomware Ryuk distribuido en dispositivos previamente infectados con la botnet TrickBot, o amenazas como Conti que utilizan correos electrónicos de phishing como uno de sus principales vectores de ataque para lograr el acceso inicial a los sistemas víctima. Aquellos ataques que son interrumpidos por tecnologías como las soluciones de **ESET**, no siempre llegan a desplegar el ransomware final, sino que se detectan y se detiene el ataque en el vector de infección (phishing, explotación de vulnerabilidades) o en la amenaza previa que descargaría esta última y generaría persistencia (droppers, downloaders, botnets). Este punto será retomado en la sección "Troyanos: amenazas en amenazas".

UNA DISMINUCIÓN DE DETECCIONES DE TIPO RANSOMWARE NO INDICA UNA MENOR CANTIDAD DE CÓDIGOS MALICIOSOS

Ataques memorables de este tipo afectaron a los gobiernos de la región, tanto durante 2021 como lo que llevamos de 2022. Para el primero, se destacaron infecciones a los gobiernos de los países de **Argentina** y **Panamá**. Para este año, el gobierno de Costa Rica sufrió variadas infecciones en sus organismos: el Ministerio de Ciencia y Hacienda por la banda detrás de *Conti*, y el organismo de seguridad social por Hive. Además, durante enero, se vio comprometido el senado de Puerto Rico. Internacionalmente, además del ataque a Kaseya, vale mencionar al incidente de Colonial Pipeline. Todos ellos fueron afectados por la **modalidad RaaS** que incluye métodos extorsivos como el **print-bombing** o el **cold-calling**, el pedido del pago de rescate en criptomonedas, y la filtración de la información robada si la víctima no accede al pago.

Esos códigos maliciosos involucrados en este tipo particular de ataque **suelen ser confeccionados a medida de sus víctimas**: desde la búsqueda de archivos específicos, hasta el método por el cual se realiza la infección cero. Sin embargo, el *ransomware* más presente en la región siguen siendo las **campañas masivas**, en donde el objetivo no está definido, y afecta tanto a individuos como compañías por igual.

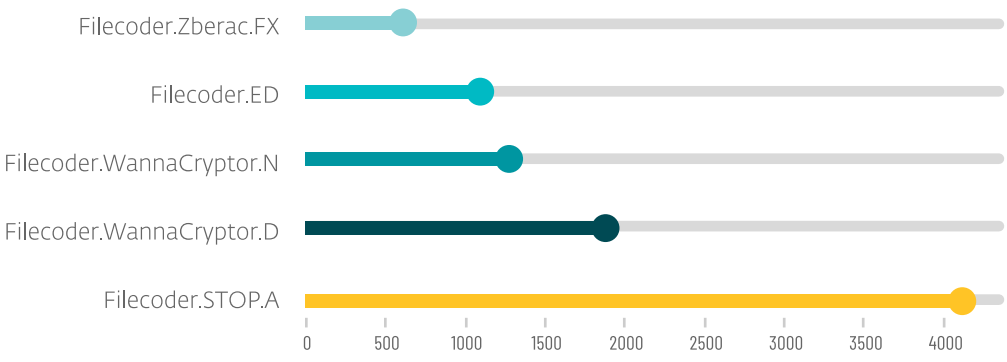

Gráfico 4. *Top 5 detecciones de ransomware*

Entre los **5 códigos maliciosos** de tipo ransomware más detectados en la región, se encuentran **campañas de distribución masiva**, que llegan a sus víctimas mediante **descargas de cracks o programas fraudulentos, comunicaciones maliciosas vía correos electrónicos** o **aplicaciones de mensajería instantánea**. Y si bien estas piezas de código malicioso suelen ser genéricas, con solo la capacidad de encriptar archivos y extorsionar a la víctima para obtener una ganancia monetaria, dos de estas amenazas merecen una mención especial: tanto **Filecoder.WannaCryptor.N** como **Filecoder.WannaCryptor.D** son variantes del infame ransomware **Wannacry**, amenaza del mismo tipo que sacudió al mundo durante el año 2017. Más aún, estas variantes también suelen aprovecharse de la misma vulnerabilidad que la original, la cual afecta a productos de Microsoft y cuenta con un parche desde hace ya 5 años. Esto se traduce en **equipos existentes**, tanto corporativos como personales, **que no se actualizan periódicamente**, una tendencia que se repetirá a lo largo del presente informe.

SPYWARE

La aceleración digital que vemos desde hace algunos años, se vio potenciada de manera exponencial por una pandemia que obligó a cientos de miles de usuarios a consumir cada vez más servicios y productos **de manera online**, y a las compañías a **digitalizar procesos que previamente se realizaban de manera física**.

Esta combinación de factores da sentido al nuevo apodo que los expertos en ciberseguridad han denominado como el **"nuevo oro": los datos e información**. Ya sea información crediticia o financiera, de salud, de accesos a cuentas, gubernamental o de un simple registro, tanto de usuarios, interna o externa, los cibercriminales la persiguen con finalidad de conseguir una ganancia monetaria. Esta se obtiene mediante la venta de la información robada en mercados negros, la extorsión a las víctimas para no revelar la información o la ejecución de otros ataques usando los datos.

No es de extrañar, entonces, que existan amenazas diseñas específicamente para el robo de datos y el espionaje, denominadas **Spyware**. En esta categoría encontramos a los keyloggers, **RAT** (o herramientas de acceso remoto), **troyanos bancarios**, **infostealers**, entre otras amenazas. Además, casi todos los códigos maliciosos contienen algún tipo de módulo o funcionalidad que involucra **acciones asociadas a los anteriores**.

CONTRARIO A LA CREENCIA POPULAR, EL CIBERESPIONAJE ES UN PROBLEMA CRECIENTE DENTRO DE LATINOAMÉRICA

Contrario a la creencia popular, el ciberespionaje es un problemática creciente dentro de Latinoamérica. Desde el laboratorio de **ESET Latinoamérica** hemos cubierto campañas de espionaje dirigidas a **entidades gubernamentales de la región**. Una de las más recientes fue la campaña llamada Operación Discordia, descubierta en mayo del **2022**, que utilizaba códigos espía y de control remoto en equipos de compañías

pequeñas y medianas, así como de entidades gubernamentales en **Colombia**. Pero en **2021** analizamos otras campañas similares, como fueron las campañas llamadas Bandidos y LuxPlague.

Sin ir más lejos, y según un informe de DarkTracer, en febrero de 2022 la cantidad de usuarios afectados por piezas de código malicioso de tipo infostealer superó los **13.000 dentro de Brasil** y los **3.000 en Argentina**. Entre estos dos países, las víctimas ascienden a un total de **27.578** solamente en los **dos primeros meses del año**.

Dentro de los ataques **dirigidos a compañías** como lo son el ransomware como servicio, el ciberespionaje y los ataques a la cadena de suministro, el rol de este tipo de amenazas es fundamental, persiguiendo objetivos como los anteriormente mencionados, predominando el **filtrado de la información robada** y la **venta de la misma** en los mercados negros del internet. Además, y con la llegada del trabajo híbrido y políticas como BYOD (Bring your own device), **los ataques dirigidos a usuarios finales también se trasladan a incidentes corporativos**. Por ejemplo, en diciembre de 2021 investigadores revelaron un caso de un usuario que trabajaba de manera remota y que fue infectado con *RedLine*, un infostealer. El malware robó las credenciales de acceso a la VPN que utilizaba para conectarse a la red de la compañía, lo que permitió que actores maliciosos comprometieran la red interna de la compañía unos meses después.

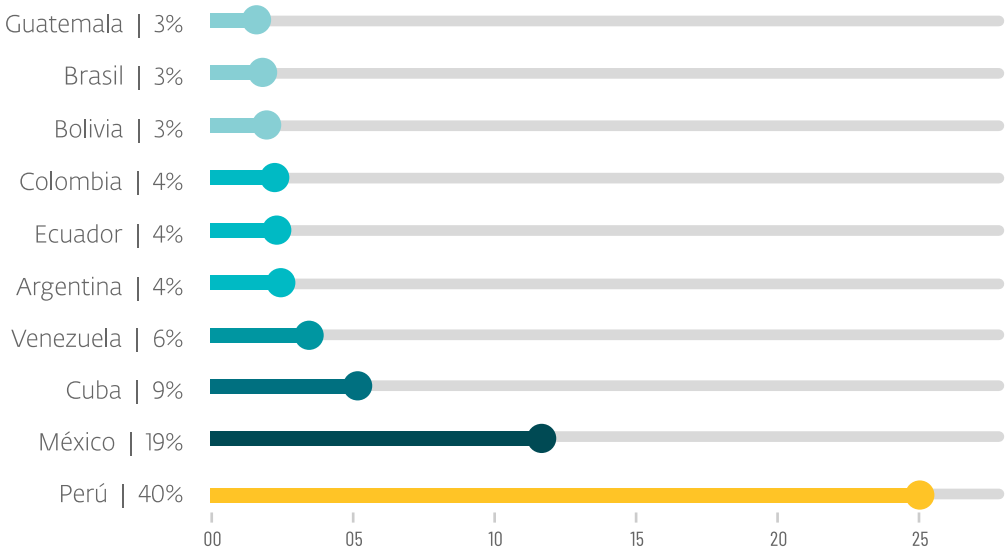

Gráfico 5. *¿A qué país corresponden las detecciones de códigos espía?*

Según los **datos de la telemetría de ESET**, el país más afectado por esta categoría de códigos maliciosos es **Perú**, con el **40%** de las detecciones. A este le sigue **México**, con el **19%**, y el resto de países con menos del 10% de malware espía detectado. Esto, sin embargo, representa una parte de las piezas de código malicioso que roban información, ya que la gran mayoría suelen contener solamente módulos secundarios con funcionalidades de espionaje y robo de información, pero no es su objetivo primordial, como el **ransomware**.

TROYANOS: AMENAZAS EN AMENAZAS

En la sección de Ransomware, se observó una leve caída en las detecciones anuales de dicha amenaza, y algo similar sucede con varias categorías de códigos maliciosos. Si bien una posible justificación sería pensar en la disminución del cibercrimen, hay otras variables que no acompañan este hecho, como el récord de **400 millones de dólares en criptomonedas recaudadas** solo de **ataques de ransomware** reportados en todo el mundo, entre otras tantas.

SE PODRÍA PENSAR EN UNA DISMINUCIÓN DEL CIBERCRIMEN, PERO HAY VARIABLES QUE NO ACOMPAÑAN ESTE HECHO

La adopción de cada vez más **tecnologías de seguridad corporativa** y el aumento en las **buenas prácticas de ciberseguridad** dentro de las corporaciones son dos tendencias bien conocidas por los cibercriminales, lo cual provoca que los mismos quieran complejizar cada vez más sus estrategias.

Particularmente, una gran parte de ataques dirigidos a corporaciones están compuestas por **dos amenazas**. La primera, generalmente de una familia más genérica como **troyanos de tipo dropper o downloader**, **que se encarga de realizar la infección almacenando y ejecutando la segunda amenaza en el equipo víctima**, además de generar persistencia. Así, los cibercriminales logran eludir aquellas reglas o controles de seguridad que sean demasiado laxos, o no levantar demasiadas sospechas dejando que sea el código malicioso genérico el detectado, y no aquel que podría llegar a identificar a un ataque como dirigido.

Un ejemplo memorable de estas primeras amenazas es **Trickbot**, una botnet que está activa desde fines de 2016. En sus inicios esta amenaza contenía exclusivamente características de troyano, y era solamente utilizada para robar credenciales de acceso a cuentas bancarias en línea para luego intentar realizar transferencias fraudulentas. Sin embargo, con el correr del tiempo fue mutando y se expandió, hasta convertirse en un **malware multi propósito** disponible para que otros actores maliciosos puedan distribuir su propio malware bajo el modelo de **Malware-as-a-Service** con ataques dirigidos a corporaciones y llegar a ser incluso una de las botnets más prolíficas y populares.

Durante 2021, las detecciones de tipo **dropper** y **downloader** superaron los dos millones de hits, siendo de las amenazas más vistas de manera sostenida en los últimos años.

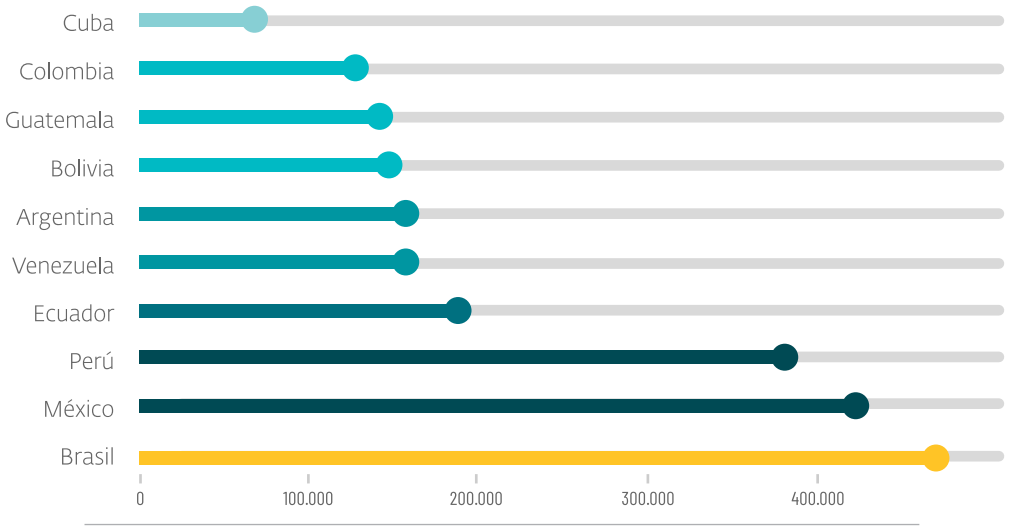

Gráfico 6. *Distribución de las detecciones de troyanos en América Latina durante 2021.*

En cuanto a la distribución de detecciones, la mayoría de ellas se encuentran en países con **alta actividad corporativa y financiera**, como lo son **Brasil**, **México** y **Perú**.

CONTROLES

La combinación de la información obtenida acerca de la **percepción corporativa** del estado de la ciberseguridad, y las estadísticas de **intentos de ataque** arrojadas por **la telemetría de ESET, culminan en una preocupación cada vez más creciente** en cuanto a la protección de los activos de las compañías de toda Latinoamérica. Esto debería traducirse en un aumento de aquellas medidas que se utilizan para combatir los mismos, que tienen como objetivo reducir o mitigar completamente los riesgos en la materia.

En esta categoría encontramos tanto **controles basados en tecnología**, como una **solución de firewall**, así como aquellos **de gestión**, centrados en concientizar o generar procesos o procedimientos en materia de protección de información, entre otros aspectos.

SOLUCIONES DE SEGURIDAD

Si de **medidas de protección** hablamos, aquellas que se componen por **programas, reglas y monitoreo tecnológico** son de las más conocidas y adoptadas. Estas ayudan a prevenir o detectar ataques complejos, que no necesariamente requieren de interacción humana, como lo podría ser una explotación de vulnerabilidad o una negación de servicio distribuida (o DDoS).

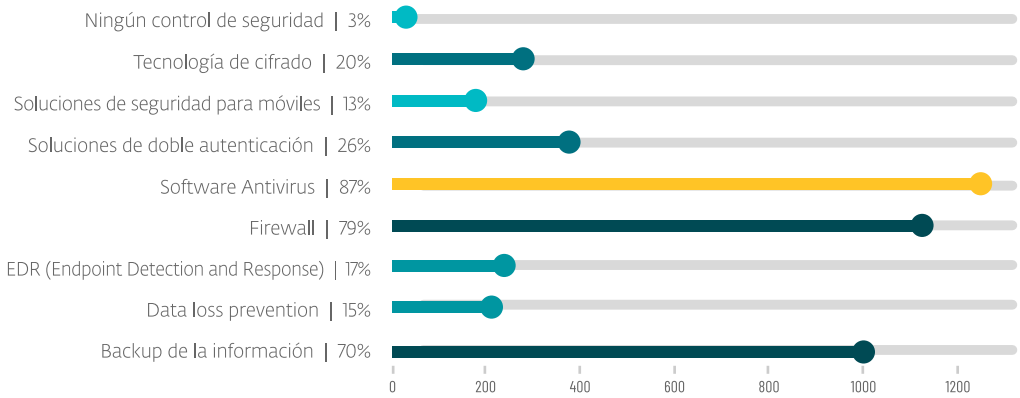

Gráfico 7. *Soluciones de seguridad más utilizadas por las empresas en América Latina.*

No es de extrañar, entonces, que las **soluciones antimalware** sean las más utilizadas (**87%**), presentando un aumento sostenido en comparación a reportes de años anteriores. En un mundo en el cual el trabajo híbrido difumina el perímetro corporativo, y en donde el cibercrimen que utiliza códigos maliciosos apuntados a organizaciones no para de crecer, **resulta vital proteger los activos con este tipo de soluciones**.

Del mismo modo, los **firewalls** siguen presentándose como la segunda herramienta más utilizada, con un **79%** de encuestados afirmando su uso. La protección de las redes corporativas también juega un papel importante, manteniéndose como **sinónimo de herramienta de protección** desde hace más de diez años en sus múltiples variantes: de manera personal, desde el host o para proteger el perímetro de la red.

Si bien la adopción de soluciones de **Backup** sigue con un ligero aumento sostenido hace algunos años (**70%**), y se presenta como una de las herramientas primordiales para mitigar ataques de secuestro de información como lo es el *ransomware*, no es la única. Las herramientas complementarias a ella, como **DLP** (*Data Loss Prevention*) o las **tecnologías de cifrado** todavía siguen presentando un **bajo porcentaje de adopción**. Esto podría disminuir la efectividad de la primera en un ataque que tenga como objetivo robar o dañar la información de la compañía víctima.

Finalmente, la adopción de soluciones para **dispositivos móviles** presenta un nivel bajo, de tan solo el **13%**. Sin embargo, el aumento de interés por parte de los cibercriminales por los dispositivos corporativos es inminente. Por ejemplo, las amenazas **dirigidas a dispositivos Android que buscan robar credenciales bancarias tuvieron un crecimiento del 428% durante 2021** en comparación con el año previo.

LA ADOPCIÓN DE SOLUCIONES PARA DISPOSITIVOS MÓVILES PRESENTA UN NIVEL BAJO: 13%

Las crecientes detecciones de este tipo de amenazas, así como la adopción cada vez más frecuente de estos dispositivos como parte de los elementos de trabajo de un colaborador, hace necesario e inminente el aumento del uso de este tipo de tecnologías.

PRÁCTICAS DE GESTIÓN

Del otro lado de los aspectos de protección, y como complementario a las herramientas tecnológicas implementadas, se encuentran las **prácticas y políticas de gestión de la ciberseguridad en las compañías**. Estas son cruciales no solo para prevenir incidentes, sino también para tomar las medidas adecuadas para **restaurar la operativa luego de un ataque informático**.

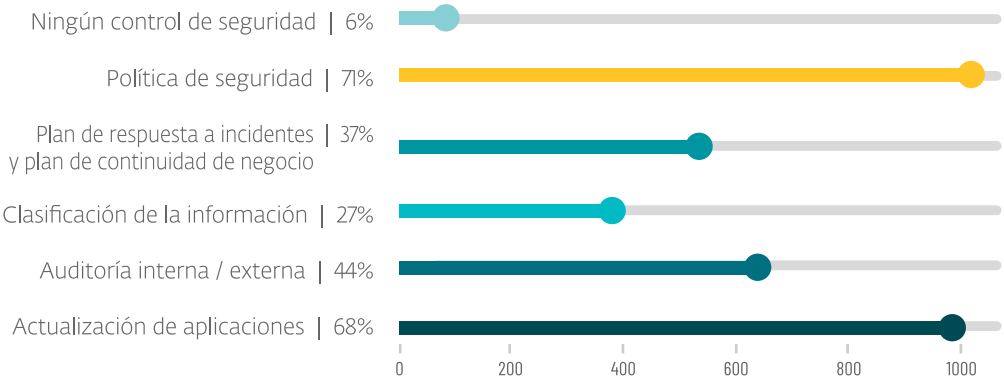

Gráfico 8. *Prácticas de gestión de la seguridad implementadas por las empresas de América Latina.*

Según las encuestas realizadas por **ESET** dentro de Latinoamérica, **1 de cada 3** compañías afirman la aplicación de **políticas de seguridad** (por ejemplo, una reglamentación formal de accesos y privilegios). En segundo lugar le sigue la **actualización de aplicaciones** (**68%**), una práctica necesaria para la disminución de ataques que utilizan vulnerabilidades en los sistemas como punto de entrada.

Sin embargo, varias de estas categorías han tenido una **leve disminución** durante el año 2021, en comparativa a los datos correspondientes al año 2020. Esto puede deberse, en su mayoría, al abandono del aislamiento y teletrabajo como obligación, ya que esto abre la posibilidad de adopción de medidas tecnológicas más fuertes.

Una herramienta en materia de gestión cuya adopción aumentó durante el año 2020 y se asentó en 2021 a raíz del aumento de la relevancia de los ataques más destructivos a compañías fueron los **ciberseguros**. Estos seguros, como cualquier otro, dan una cobertura económica en casos de incidentes informáticos según el tamaño de la corporación, los riesgos tomados, el dinero potencial a perder, entre otros. Desde el comienzo de la pandemia, la demanda y los precios de estos seguros **han aumentado**, hasta llegar a ocupar una buena parte del presupuesto asignado al área de ciberseguridad de algunas compañías. Sin embargo, esta tendencia puede ser riesgosa, ya que los seguros **son medidas paliativas** para enmendar las consecuencias de un ataque y **no para prevenirlo**.

PRESUPUESTO

Durante el año **2020**, la crisis sanitaria producida por la pandemia trajo consigo una gran **inestabilidad económica**, que golpeó a todos los países de la región por igual. Esto se vio reflejado en el manejo financiero de las compañías y, por lo tanto, en el presupuesto asignado para el área de ciberseguridad. Según la información arrojada por el **ESR 2021**, el **46%** de los encuestados manifestó la necesidad de **mayores inversiones en seguridad para el corto plazo**, para afrontar los desafíos del cambio del panorama laboral que trajo consigo el trabajo remoto.

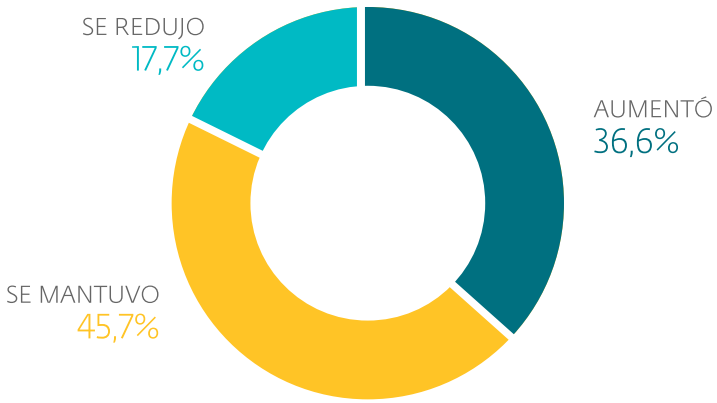

Gráfico 9. *Inversión en seguridad de las empresas de América Latina.*

Durante el año 2021, las economías golpeadas el año anterior vieron un resurgimiento de su actividad incluso hasta los niveles previos a la pandemia. Esto también se puede ver reflejado en el presupuesto del área de seguridad de las compañías encuestadas: **1 de cada 3** personas afirma que este **aumentó para el año 2021**, con respecto al asignado durante el año anterior. Si bien resulta en una mejoría con respecto a la información del año anterior, el **45.7%** de los encuestados afirma no haber visto cambios con respecto al mismo.

1 DE CADA 3 PERSONAS AFIRMA QUE EL PRESUPUESTO DEL ÁREA DE SEGURIDAD AUMENTÓ PARA 2021

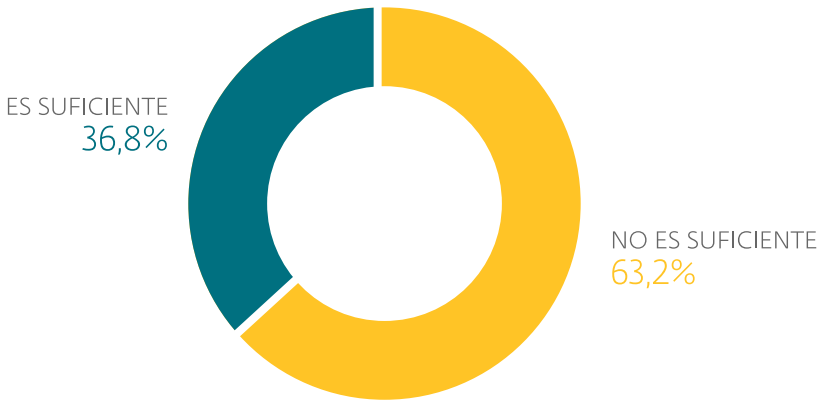

Gráfico 10. *Percepción sobre la inversión en seguridad realizada por las empresas de América Latina.*

Pese a los cambios con respecto al año 2020, y a las mejorías económicas de las compañías, el **63%** de los encuestados todavía cree que la relación entre el presupuesto recibido y las necesidades de protección cibernética de las mismas sigue siendo dispar. **Esto es, todavía, un gran punto de mejora dentro de la región**.

VULNERABILIDADES, LA VÍA DE ENTRADA PREDILECTA

Toda pieza de software, ya sea corporativa u hogareña, **puede presentar errores** en su desarrollo que resulten en la **exposición de los sistemas** en los cuales se encuentra. Y es por ello que, combinada con otros factores como la acelerada digitalización de procesos, la explotación de estos errores o vulnerabilidades sigue siendo una de las formas **más elegidas por los cibercriminales** para realizar ataques con códigos maliciosos, robo de información o intrusiones, particularmente aquellos focalizados en compañías en particular.

Durante el año **2021** se ha vuelto a romper el récord de vulnerabilidades reportadas con más de **20 mil registros**, promediando **60 reportes verificados por día** en plataformas como sistemas operativos, aplicaciones en Android, plug-ins de sitios web, entre otros. Más aún, la **criticidad** de estas vulnerabilidades se ubican **en promedio entre 5 y 6 puntos sobre 10** conforme al estándar de puntaje CVSS (o *Common Vulnerability Scoring System*), lo cual habla de una **criticidad media**. Entre los productos más afectados por estas se encuentran lectores de documentos, aplicaciones de bases de datos, administradores de servidores y servicios, herramientas de desarrollo, y más aplicativos que son utilizados ampliamente por corporaciones de todo calibre.

DURANTE 2021 SE HA VUELTO A ROMPER EL RÉCORD DE VULNERABILIDADES REPORTADAS

Según los datos obtenidos de la telemetría de **ESET**, el top 5 de exploits en la región son:

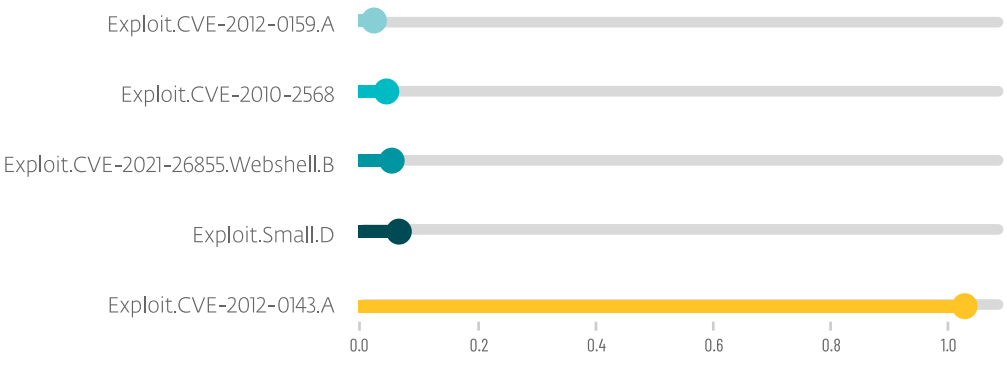

Gráfico 11. *Top 5 Exploits de la región.*

Salvo el **Exploit.Small.D**, exploit genérico para sistemas Linux, estos códigos maliciosos apuntan a vulnerabilidades disponibles en programas ampliamente utilizados en el mundo corporativo:

> **CVE-2012-0143:** disponible en versiones 2003 (Windows) y 2008 (Mac) de aplicaciones de manejo de documentos de ofimática. Permite la ejecución de código remoto y toma de control del dispositivo.

> **CVE-2021-26855:** disponible en versiones 2019 de Microsoft Exchange. Permite la ejecución de código remoto, sin requerir autenticación previa.

> **CVE-2010-2568:** disponible en Windows 7, Server 2003 y Server 2008. Permite la ejecución de código remoto y toma de control total del dispositivo, con criticidad alta. Fue utilizada en una campaña del gusano Stuxnet durante el año 2010.

> **CVE-2012-0159:** disponible en versiones 2003, 2007 y 2010 de productos de Windows Office. Permite la ejecución de código remoto.

Una característica notable de estas vulnerabilidades es su antigüedad, llegando hasta **12 años** desde su descubrimiento. De hecho, todas ellas cuentan con actualizaciones que las enmiendan, o parches, en el sitio de sus fabricantes lanzadas el mismo año en la cual se dieron a conocer. Esto indica una **falta de uso de software actualizado, ya sea por no realizar las actualizaciones correspondientes, el uso de software pirata o falta de personal capacitado**.

TELETRABAJO: ¿APRENDIZAJE?

El año 2021 significó el fin de una gran cantidad de restricciones y costumbres derivadas de la pandemia, como el aislamiento. Esto causó que el trabajo remoto dejara de ser una obligación para que las compañías continúen con su operatoria, aunque esto no significó el fin de la virtualidad para el trabajo por diversos motivos. De hecho, el **trabajo remoto llegó para quedarse**: según una encuesta realizada por Microsoft a mediados de 2021, **2 de cada 3** líderes de compañías a nivel mundial están pensando en **rediseñar la estrategia de trabajo utilizada antes del aislamiento**. Además, la productividad que **se logró mantener o incluso mejorar** en las empresas a lo largo del 2020, así como la **reducción de algunos costos**, fueron otros de los factores que demostraron a las organizaciones que esta modalidad es viable y positiva. A esto se suma que muchas personas vieron en el trabajo a distancia **una oportunidad para mejorar el balance entre su vida personal y la laboral**, lo que representa una mejor calidad de vida.

Dentro de Latinoamérica, y según encuestas realizadas por **ESET** en el año **2021**, alrededor del **80%** de colaboradores **afirmó estar continuando con una política de teletrabajo, ya sea de manera temporal o permanente**.

80% DE COLABORADORES AFIRMÓ ESTAR CONTINUANDO CON UNA POLÍTICA DE TELETRABAJO

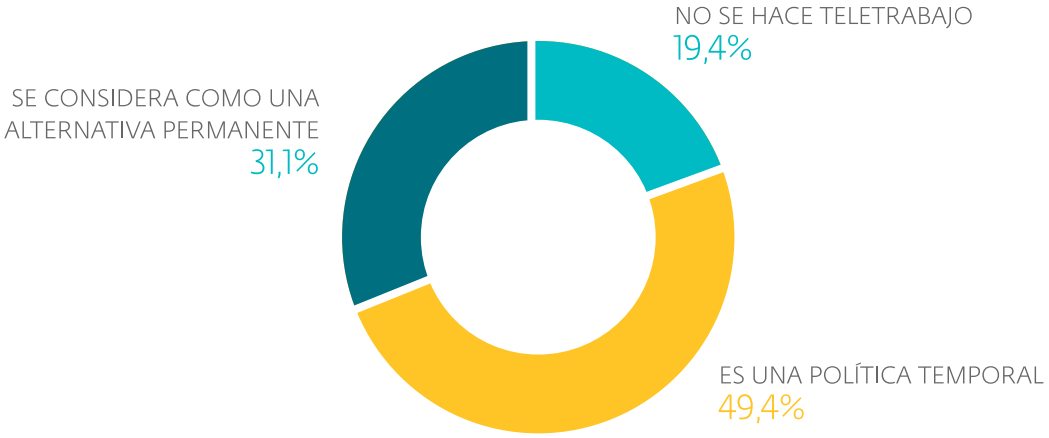

Gráfico 12. *Implementación del teletrabajo en las empresas de América Latina durante 2021.*

El llevar la operatoria, dispositivos y tareas de colaboradores fuera de la compañía implica una **multiplicidad de desafíos**, incluyendo algunos en el ámbito de la ciberseguridad. Principalmente, el perímetro de seguridad y protección de activos deja de ser, de manera obligatoria, igual al perímetro físico correspondiente a las oficinas, y con ello **las herramientas de control locales dejan de ser suficientes**. Un claro ejemplo de ello es la protección de red: un *firewall* que proteja la red corporativa no basta para proteger un dispositivo que accede a redes WiFi inseguras en espacios de trabajo compartido (*coworking*), cafés o aeropuertos.

La decisión de considerar al teletrabajo como una alternativa, ya sea a medio o largo plazo, total o parcialmente, llamó entonces a tomar **medidas adicionales en materia de protección de los activos de las organizaciones**, de manera obligatoria.

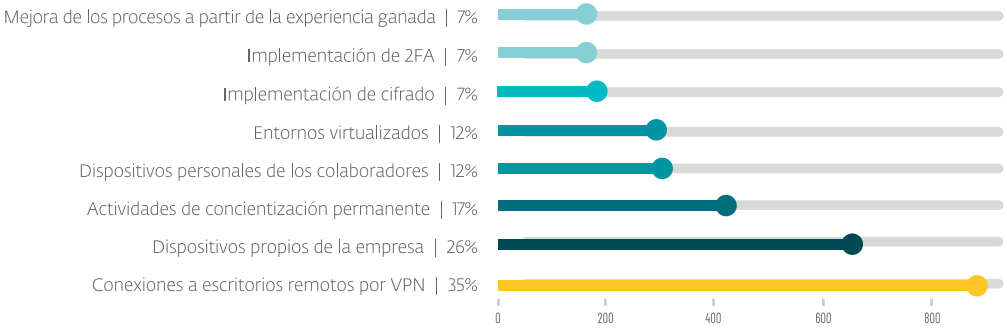

Gráfico 13. *Medidas adoptadas por las empresas de América Latina a partir de la implementación del teletrabajo.*

Según encuestas realizadas por **ESET** a colaboradores de compañías de toda Latinoamérica durante el año 2021, el **35%** de los mismos vio implementadas soluciones de **VPN para conectarse remotamente a sus equipos**. Esto resulta particularmente positivo, teniendo en cuenta que los ataques al protocolo de escritorio remoto se dispararon ampliamente durante el año 2020 y principios de 2021. Esta tecnología debe, sin embargo, aplicarse con **configuraciones y contraseñas adecuadas, para evitar que se convierta en una vía de entrada para los cibercriminales**.

En segundo lugar en cuanto a acciones tomadas gracias a la adopción del teletrabajo, se encuentra el **uso de dispositivos propios de las compañías**. Teniendo en cuenta que se trata de colaboradores trayendo equipos corporativos a sus hogares, podemos comprenderla como una política completamente opuesta a la frecuentemente implementada parcialmente BYOD (Bring Your Own Device, o Trae Tu Propio Equipo). Con este nuevo cambio, las compañías tienen más control de los dispositivos utilizados y, por lo tanto, **resulta más sencilla la aplicación de tecnologías, controles y políticas de seguridad**.

Finalmente, el **17%** de los encuestados reportó la implementación de **actividades de educación y concientización de manera permanente**, lo cual es una mejora respecto al 2020. De hecho, según los datos obtenidos en ese año, la mayoría de los encuestados realizaba estas actividades de manera ocasional, sin ninguna periodicidad. Teniendo en cuenta las campañas de ingeniería social lanzadas en torno al Coronavirus y aplicaciones utilizadas durante el trabajo remoto, es necesaria la adopción de este tipo de prácticas de manera regular.

ATAQUES A LA CADENA DE SUMINISTROS

Gracias a la cada vez más creciente visibilidad de incidentes informáticos, combinada con la acelerada digitalización que sufrieron las corporaciones, **la adopción de tecnologías y controles más fuertes de ciberseguridad es una realidad**, sobre todo en corporaciones de gran interés para los atacantes: financieras, tecnológicas, de manufactura, entre otras.

LAS EMPRESAS DE SERVICIOS TERCERIZADOS SE CONVIERTEN EN VÍAS DE ENTRADA PARA ATAQUES A LA CADENA DE SUMINISTRO

Sin embargo, estas compañías **suelen consumir servicios tercerizados** de otras que pueden no tener el mismo nivel de protección de activos e información que las primeras. Es por ello que **se convierten en vías de entrada para ataques a la cadena de suministros**, ya que es prácticamente imposible que cualquier empresa tenga el control total de la cadena para garantizar que ningún componente que se ha incorporado en sus productos o servicios, no han sido explotados en el camino hacia el eventual consumidor. **Minimizar el riesgo de un ataque de cadena de suministro implica un ciclo interminable de gestión de riesgos y cumplimiento**.

Esta modalidad ha sido utilizada extensamente **en los últimos dos años** para grandes blancos corporativos. Por ejemplo, en diciembre de **2020** se dio a conocer un ataque a la compañía **Solarwinds** que, mediante la inyección de un *backdoor* en uno de sus productos, logró afectar con grandes pérdidas a sus clientes, entre los cuales se encontraron compañías privadas como **Microsoft** o **Ford**, así como entidades gubernamentales estadounidenses como la **NASA**.

Otro ejemplo de esta modalidad fue un ataque de *ransomware* que afectó a **Kaseya**, una compañía que ofrecía software como servicio (o SaaS), en julio del **2021**. Este afectó a más de **1.000** compañías en al menos **17 países del mundo**, en donde una banda cibercriminal logró infiltrarse en los sistemas y **lanzar una actualización automática envenenada del software de gestión de IT de la compañía**, directamente en sus clientes.

Tanto el caso de **Kaseya** como el de **SolarWinds**, así como la mayoría de ataques de este estilo, parten de la explotación de vulnerabilidades, bien **0-day** o conocidos como prueba de concepto. De hecho, la cantidad de exploits que apuntan a aprovecharse de vulnerabilidades que se utilizan para, entre otras cosas, los ataques a la cadena de suministro siguen batiendo récords. Más aún, cuentan con un mercado millonario, circulando **20 millones de dólares por mes durante el año 2021**.

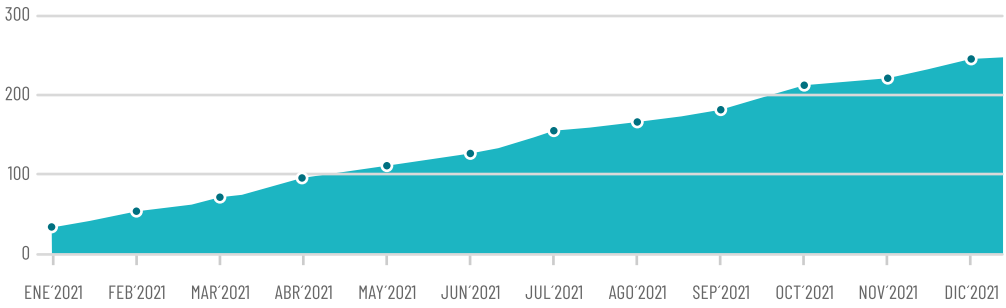

Gráfico 14. *Crecimiento del mercado de exploits.*

LOG4SHELL

Si de vulnerabilidades se trata, es imposible no mencionar la revolución que trajo consigo el descubrimiento de **Log4Shell** en diciembre de **2021**. Esta vulnerabilidad afecta a una librería del lenguaje de programación Java, en donde ciertas configuraciones y búsquedas toman parámetros laxamente verificados, que le permiten al atacante configurar un servidor que se entrometa entre las comunicaciones del equipo vulnerado. Esto derivó en la posibilidad de **ejecución de código remoto en servidores de compañías alrededor de todo el mundo, aspecto que le valió un puntaje de 10/10 en la escala de puntuación CVSS**.

Log4shell tuvo grandes repercusiones, y no solo por su riesgo teórico. En primer lugar, **la facilidad de llevar a cabo un ataque utilizando esta vulnerabilidad es alta**. Basta con utilizar herramientas y líneas de código disponibles de manera gratuita en la internet superficial para poder realizar ataques informáticos que deriven en la toma de control del equipo vulnerado, la inyección de códigos maliciosos o la interrupción de servicios críticos para la continuidad del negocio de la compañía víctima.

LOG4SHELL SE UBICÓ EN EL PUESTO NÚMERO CINCO DE VECTORES DE INTRUSIÓN EXTERNA MÁS COMUNES DURANTE EL AÑO 2021

Esta combinación de factores le valió a la vulnerabilidad el **puesto número cinco** en cuanto a **vectores de intrusión externa más comunes durante el año 2021**, según estadísticas de **ESET**. Este hecho, combinado con que el descubrimiento de **Log4Shell** haya sido en las ultimas tres semanas del año, refleja cuán rápido los actores de amenazas se están aprovechando de las **vulnerabilidades críticas emergentes**.

De hecho, a menos de una semana de su descubrimiento, **los sistemas de detección de ESET** habían arrojado intentos de ataque que buscaban distribuir distintas piezas de código malicioso: desde mineros de criptomonedas, troyanos *Tsunami* y *Mirai*, amenazas genéricas de espionaje, así como las bandas de *ransomware* responsables por grandes ataques durante el año **2021**.

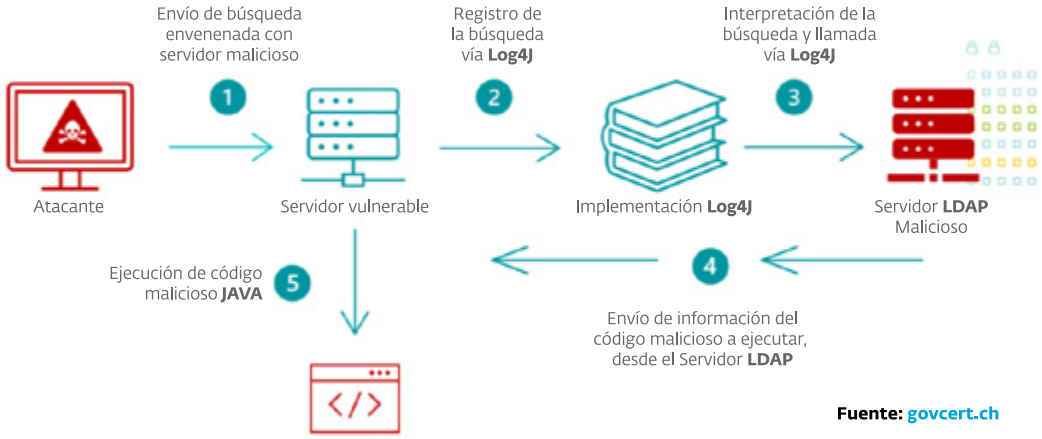

Gráfico 15. *Ejemplo de ataque que busca explotar la vulnerabilidad Log4Shell.*

En segundo lugar, la amplia utilización de la librería provoca que su solución no sea lineal. Y es que existe una lista muy larga de piezas de software de uso corporativo que tuvieron una versión vulnerable a esta: servicios de manejo web, telecomunicaciones, tecnologías cloud, entre otros. De hecho, y según una investigación de las compañías Wiz y EY, esta vulnerabilidad se encontraba en algún producto de alrededor del **93% de ambientes cloud** pertenecientes a compañías de todo el mundo. Es por esto que los expertos en ciberseguridad afirman que la problemática que trajo consigo esta vulnerabilidad no se terminará en el corto plazo, ya que **el uso de esta librería está tan extendido que es imposible determinar a cuántas piezas de software afecta** y, por lo tanto, asegurar que no existe producto alguno vulnerable dentro de una organización.

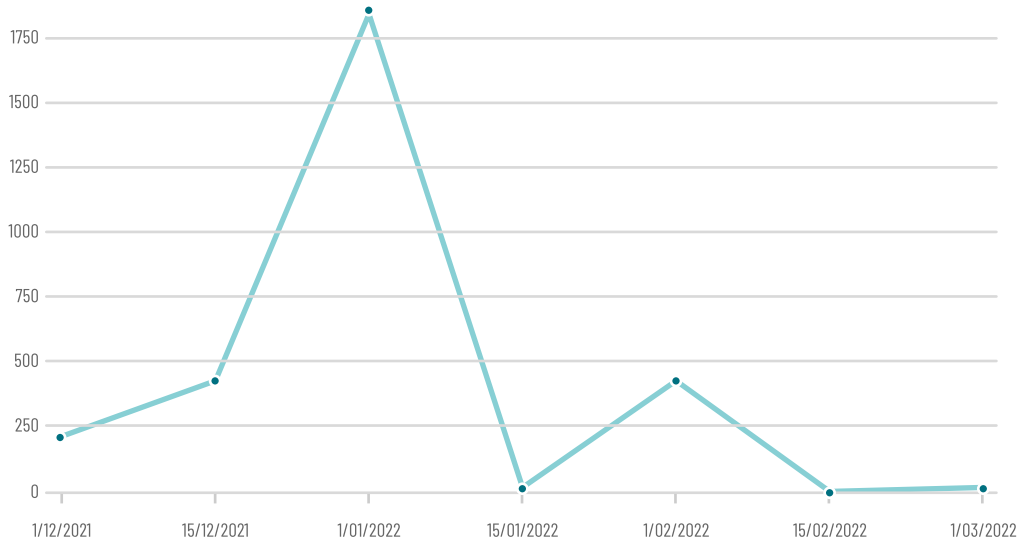

Gráfico 16. *Detecciones de ataques intentando explotar Log4Shell desde diciembre de 2021 hasta marzo de 2022.*

Si bien la actualización de la librería que enmienda esta vulnerabilidad se encuentra disponible desde mediados de diciembre de 2021, según los datos de la telemetría de **ESET**, el pico de intentos de ataque utilizando **Log4Shell** dentro de Latinoamérica se dio en **enero de 2022**. Esto resulta de una combinación de **la falta de aplicación de actualizaciones** que tiene la región, y la dificultad de encontrar las **versiones vulnerables** en sí por la lista extremadamente larga de piezas de software afectadas por ella.

CONCLUSIONES

Ciertamente el año **2021** trajo consigo otra revolución, muy distinta a la que se pudo observar durante el año anterior, y muchas de las consecuencias de esta revolución se mantuvieron en el comienzo de 2022. La adopción de una "nueva normalidad" **cambió la concepción de vida diaria que el mundo estaba acostumbrado a ejercer,** ya que la pandemia y el aislamiento resaltaron algunos beneficios de trasladar al ámbito virtual ciertos aspectos, como evitar tiempos de traslado, gastos de alquileres de oficina y pasar más tiempo en los hogares.

En el caso del trabajo remoto, las compañías vieron igualadas o incluso mejoradas su performance y los colaboradores encontraron un mejor balance entre la vida laboral y personal, dos factores que propiciaron el establecimiento de la modalidad como **una realidad del nuevo modelo de trabajo**; y ya no una obligación como lo era el año anterior a causa de las restricciones impuestas por la pandemia.

El año **2020** fue, para el ámbito de la ciberseguridad, **un año lleno de lecciones aprendidas**. Los incidentes no escasearon, desde intrusiones mediante la explotación de vulnerabilidades o malas configuraciones en software corporativo, pasando por el robo de información y credenciales utilizando ingeniería social con temáticas relacionadas al COVID-19, hasta la infección con códigos maliciosos de tipo *ransomware* con bandas multitudinarias vendiendo los archivos exfiltrados de sus víctimas en los mercados negros. Y si bien con estas lecciones aumentó la importancia que las corporaciones y gobiernos le dan al campo de la protección de activos, esto no impidió el aumento de incidentes informáticos que estas reciben. **El hecho de que la mitad de las corporaciones hayan podido detectar al menos un intento de ataque informático en sus redes no es menor.**

Los controles, tanto tecnológicos como de gestión, **son de constante necesidad ahora más que nunca.** El difuminado de la vida laboral y la personal de los colaboradores por un lado, y la desaparición del perímetro de seguridad corporativo por el otro hacen que se deba garantizar la protección integral de los activos de la compañía **aun estando fuera de ella**. Aplicativos tecnológicos como soluciones *antimalware* o VPNs ayudan al monitoreo del dispositivo físico y de las conexiones realizadas hacia la red, independientemente de la ubicación del mismo. Además, los controles de gestión como la clasificación de la información y capacitaciones constantes de los colaboradores se complementan con los primeros para **evitar un gran grupo de amenazas populares: los espías**.

El mercado del cibercrimen se agiganta a cada segundo, batiendo récords en cuanto al dinero robado a las víctimas y al circulante en los mercados negros de la internet profunda. Esto resulta en un ciclo autocumplido: cuanto más dinero fluye en el cibercrimen, más personas se sienten atraídas por este, más actores maliciosos surgen con ideas cada vez más complejas y trabajando día y noche para poder hacerse con más víctimas, lo cual resulta en aún más dinero dentro del mercado ilegal. Es por ello que, aún con los mejores controles preventivos y detectivos, la restauración de la operatoria de la compañía es necesaria, sabiendo que el mercado del cibercrimen se agiganta a cada segundo. **Las políticas como las dedicadas a respuesta a incidentes, así como las tecnologías de Backup, son claves para la continuidad del negocio luego de un ataque.**

Para el año **2022**, se espera un **asentamiento definitivo de las políticas de trabajo remoto** tomadas hace ya casi dos años. Además, nuevas tendencias adoptadas en esta materia, como la reducción de la semana laboral, deparan consecuencias aún no exploradas en el marco de la seguridad corporativa. Además, la adopción de tecnologías nuevas en materia de ciberamenazas como lo son el *machine learning* y de aprendizaje automático podrían redefinir eventualmente la estructura de un ataque informático como lo conocemos.

En este año **2022**, la mayor parte de las tendencias expuestas de este reporte **se mantuvieron**, y se espera que este año traiga desafíos para la región que tendrán consecuencias en la protección de activos corporativos, **algunos nuevos y otros viejos conocidos.** Quedará para una nueva edición de este reporte evaluar las decisiones tomadas a partir del análisis de los hechos ocurridos durante el año 2021.

SOBRE ESET

+ 110 millones de usuarios en todo el mundo	**13** centros en el mundo de investigación y desarrollo
+ 400 mil clientes corporativos	**200** países y territorios

Para conocer más información acerca de ESET visite: www.eset.com/latam

Para estar actualizado sobre todas las noticias relacionadas con la seguridad informática visite: www.welivesecurity.com/latam