future tech

Next Digital
Ciberseguridad

La ciberseguridad engloba el conjunto de procedimientos y herramientas que se implementan para proteger los activos de información que se generan y procesan a través de computadoras, servidores, dispositivos móviles, redes y sistemas electrónicos. Los activos de información pueden incluir datos, software y hardware, y las amenazas a estos activos son variadas pudiendo originarse tanto desde fuera como desde dentro de una organización.

Tanto la ciberseguridad como los ciberataques han ido evolucionando a la vez que evoluciona la tecnología de la comunicación. Se ha recorrido un largo camino desde los cifrados simples hasta algoritmos muy sofisticados para proteger los datos y la comunicación. Los **procedimientos de autenticación multifactorial integrados, mejores técnicas de cifrado y el uso de redes privadas virtuales** se han ido convirtiendo en algo más común cada día. **La inteligencia artificial (AI) y el aprendizaje automático** han permitido que se detecten amenazas en tiempo real y que se produzcan respuestas automatizadas a incidentes, así como un aprendizaje continuo y mejora de los procedimientos.

La COVID-19 causó una adopción masiva del trabajo en remoto en tiempo récord a expensas de los protocolos y perímetros de seguridad informática de las empresas. El aumento de la dependencia tecnológica, no sólo a nivel laboral, sino también en lo educativo, la salud, el comercio, la banca o la propia vida social, se tradujo en un incremento en las vulnerabilidades, las pérdidas de datos y los ataques de *ransomware* (secuestro de datos) dirigidos.

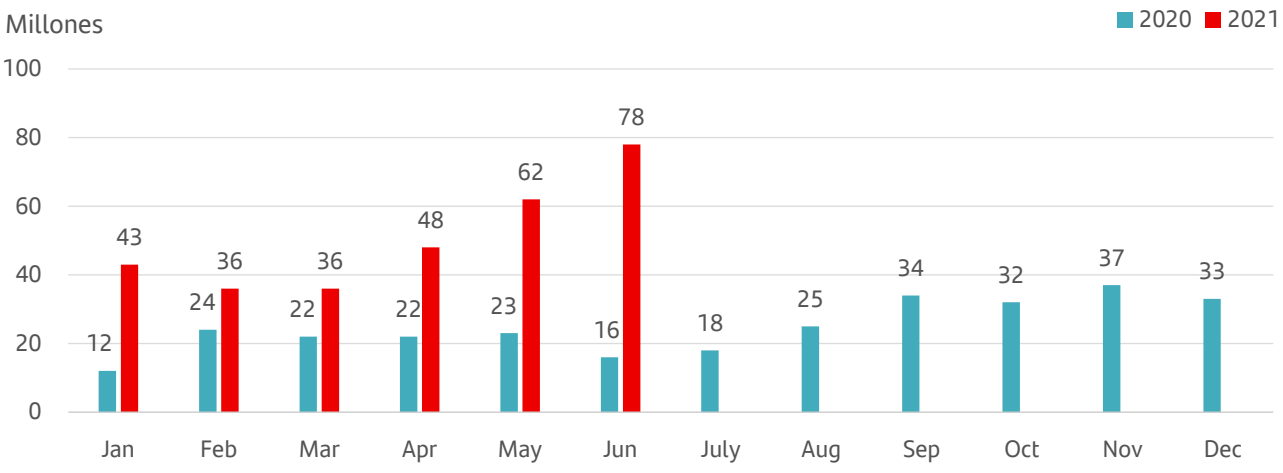
Según el reporte de SonicWall "Mid-Year Update: 2021 SonicWall Cyber Threat Report" **en los primeros seis meses de 2021 los intentos de ataque ya superan el total de 2020.** (ver gráfico)

Según los datos del estudio "*Cost of a Data Breach Report 2021*" producido por el Ponemon Institute y patrocinado por IBM, **en 2020, el coste medio de una filtración de datos fue de 3,86 millones de dólares en todo el mundo, y de 8,64 millones en Estados Unidos.** Estos costes incluyen los gastos de descubrimiento y respuesta a la violación (*breach*), el coste del tiempo de inactividad y la pérdida de ingresos, y el daño a la reputación a largo plazo de una empresa y su marca. Según este mismo estudio, en el último año (2020-2021) el coste promedio por cada *breach* se ha incrementado en un 10% y, el 20% de esas violaciones se debe inicialmente a credenciales comprometidas.

Actualmente el ciberespacio es internacional y relativamente nuevo, con lo que no existen prácticamente normas o leyes que lo regulen. En ese sentido, **la inversión en ciberseguridad se ha hecho más fundamental que nunca** para proteger a gobiernos, organizaciones e individuos, así como a sus activos físicos, digitales, financieros y hasta sus propias marcas. Según Canalys, una empresa especializada en el análisis del sector tecnológico, en Estados Unidos en el año **2020 las inversiones en ciberseguridad registraron un crecimiento del 10%, alcanzando los 53.000 millones de USD.** Se espera que ese crecimiento anual de gasto de alrededor del 10% se mantenga en los próximos años.

Volumen de *ransomware* global (número de intentos de ataques)

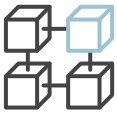
Fuente: Mid-Year Update: 2021 SonicWall Cyber Threat Report



Principales innovaciones en Ciberseguridad

Firmas y Certificados Digitales

Debido a los rápidos avances en el comercio electrónico, existe una creciente necesidad de seguridad y autenticación en línea. Se están desarrollando muchas tecnologías avanzadas para asegurar la autenticación en Internet. La **firma digital es un mecanismo criptográfico que, aplicado a un documento, permite al receptor identificar al firmante de manera inequívoca y garantizar la integridad del documento firmado.** Permite a las organizaciones autenticar y asegurar la identidad y los registros del cliente y ofrece posibilidades muy valiosas para que las organizaciones formalicen contratos. Existen plataformas de firma electrónica que permiten enviar y firmar contratos electrónicamente de forma segura. El **certificado digital, por otro lado, es una certificación o documento electrónico expedido por una autoridad de certificación que vincula a una persona con una clave pública y confirma su identidad.** Este permite realizar trámites por internet, entre ellos firmar documentos digitalmente. Según datos de Statista, un portal de estadística en línea, en 2019 el mercado de las firmas digitales estaba valorado en 958 millones de dólares, y se espera que crezca hasta 4.800 millones de dólares para el año 2026.



Seguridad de las redes

La seguridad de la web consiste en **cada acción o herramienta utilizada para evitar que la información esté expuesta o propensa a ataques por parte de ciberdelincuentes.** No sólo protege a las compañías sino también a los usuarios. **Entre las principales herramientas encontramos el firewall, el servidor proxy, software antivirus, cifrado de punto final y escáner de vulnerabilidades.** *El* ***firewall*** (cortafuegos) monitoriza el tráfico entrante y saliente y decide si debe permitir o bloquear un tráfico en función de un conjunto de restricciones de seguridad ya definidas. El **servidor proxy** es un intermediario entre las conexiones de un cliente y el servidor filtrando todos los paquetes entre ambos que impide que el servidor conozca la identidad del cliente permitiendo una navegación privada y anónima. El **software antivirus** tiene como objetivo detectar, eliminar y bloquear virus informáticos. El **cifrado de punto final** (*endpoint encryption*) asegura que un mensaje sea convertido en mensaje secreto en su envío original y se descifra sólo por el destinatario final. Finalmente, el **escáner de vulnerabilidades** web es un software que permanentemente hace análisis automáticos de cualquier aplicación, sistema o red en busca de cualquier posible vulnerabilidad. Estimaciones de Statista indican que el mercado de seguridad de las redes, que incluye aplicaciones, software y servicios basados en la nube, estaba valorado en 29.500 millones de USD en 2020 y se espera que supere los 4.600 millones de dólares en ingresos en 2021.

Aprendizaje automático

La creciente adopción del aprendizaje automático en los negocios de todas las industrias refleja la eficacia de sus algoritmos, marcos y técnicas para resolver rápidamente problemas complejos. El **aprendizaje automático o *machine learning* (ML, por sus siglas en inglés) es un tipo de inteligencia artificial (AI) que permite a los ordenadores la capacidad de aprender sin ser programados explícitamente. Consiste en desarrollar patrones y, a través de algoritmos, modificar esos patrones a medida que se van conociendo nuevos datos.** Para desarrollar estos patrones, se necesitan datos en grandes volúmenes porque los datos deben representar todos los resultados potenciales de todos los escenarios que sean posibles.

Con el aprendizaje automático, **los sistemas de ciberseguridad pueden analizar los patrones y aprender de ellos para ayudar a prevenir ataques similares y responder ante los cambios.** Puede ayudar a los equipos de ciberseguridad a ser más proactivos en la prevención de amenazas y en la **respuesta a ataques activos en tiempo real.** Puede reducir la cantidad de tiempo dedicado a tareas rutinarias y permitir a las organizaciones utilizar sus recursos de manera más estratégica. En resumen, el aprendizaje automático puede hacer que la ciberseguridad sea más sencilla, más proactiva, menos costosa y más eficaz.

Innovadores en Ciberseguridad

VMware, Inc. es una empresa situada en Palo Alto, California que desarrolla un **software utilizado para crear y gestionar máquinas virtuales, es decir, funciones informáticas repartidas en varios sistemas. Las empresas utilizan sus aplicaciones basadas en la nube y en las instalaciones para integrar y gestionar de forma más eficiente las funciones de servidor**, **almacenamiento y red, lo que reduce sus costes de TI**. VMware también ofrece mantenimiento y soporte de software, formación, servicios de consultoría y servicios alojados. La estrategia global de la empresa para la nube contiene tres componentes clave: continuar con la expansión más allá de la virtualización informática en la nube privada; extender la nube privada a la nube pública; y conectar y asegurar los puntos finales a través de una gama de nubes públicas.

Palo Alto Networks, Inc. es un proveedor global de ciberseguridad que ofrece a las empresas, proveedores de servicios y entidades gubernamentales la posibilidad de proteger a todos los usuarios, aplicaciones, datos, redes y dispositivos con una visibilidad y un contexto completos de forma continua en todas las ubicaciones**. Ofrece productos de ciberseguridad que cubren una amplia gama, permitiendo a los clientes finales asegurar sus redes, personal remoto, sucursales, nubes públicas y privadas, y avanzar en sus Centros de Operaciones de Seguridad ("SOC").** Sus productos incluyen dispositivos y software de cortafuegos y actualizaciones de sistemas virtuales, que son extensiones de los dispositivos. Tiene más de 80.000 clientes en 150 países del mundo. Sus ingresos provienen en un 65% de Estados Unidos.

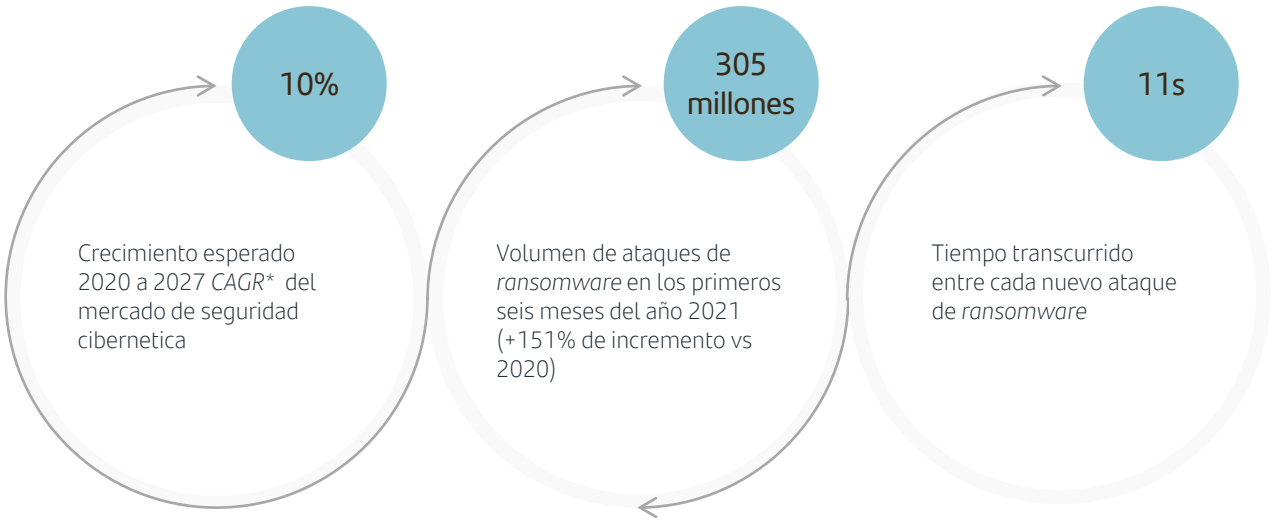
CrowdStrike Holdings, Inc. es una empresa líder en ciberseguridad que proporciona **servicios de seguridad para puestos de trabajo o *endpoints* y cargas de trabajo en la nube, inteligencia sobre amenazas y respuesta a ciberataques**. Desde 2011, cuando se fundó la compañía, se han especializado en la seguridad en la nube o *cloud*. Diseñaron la plataforma **Falcon**, sobre una arquitectura situada en la nube para detectar amenazas y detener violaciones o *breaches* sin comprometer la velocidad o el rendimiento de los ordenadores. **La plataforma cuenta con Threat Graph, que es un sistema de *machine learning* que continuamente está procesando y contextualizando los datos, correlacionándolos con diferentes eventos para enriquecer su conocimiento y poder predecir amenazas mejor y más rápido.**

Splunk Inc. desarrolló un software que recopila e indexa los datos generados por las máquinas y producidos por casi todos los equipos y programas informáticos que contienen un registro con fecha y hora de las transacciones, las acciones de los usuarios, las amenazas a la seguridad y otras actividades. **Con el software de Splunk, los usuarios pueden profundizar en los datos, analizando, supervisando y elaborando informes para la inteligencia operativa, la gestión de aplicaciones y la seguridad y el cumplimiento de normativas, así como la analítica.** La empresa se asocia con empresas como Microsoft Visual Studio y Eclipse para incluir su software en sus productos. Splunk cuenta con más de 19.000 clientes corporativos y gubernamentales en más de 130 países. La empresa depende de los clientes de EE.UU. para alrededor del 70% de sus ingresos.

DocuSign, Inc. **ha sido pionera en el desarrollo de la firma electrónica. Hoy en día ofrece la solución de firma electrónica número 1 del mundo como parte central de su plataforma más amplia para automatizar el proceso de acuerdos.** Eliminan el papel y automatizan el proceso, lo que permite a las empresas medir el tiempo de entrega en minutos en lugar de en días, reducir sustancialmente los costes y eliminar en gran medida los errores. Su plataforma basada en la nube permite a empresas de todos los tamaños y sectores convertir rápida y fácilmente en digitales casi todos los acuerdos, procesos de aprobación o transacciones, desde casi cualquier lugar del mundo y en prácticamente cualquier dispositivo. Cuenta con mas de un millón de clientes y 1.000 millones de usuarios a nivel mundial.

Fortinet, Inc. Inc. es un líder mundial en soluciones de ciberseguridad para una amplia variedad de organizaciones, incluyendo empresas, proveedores de servicios de comunicación, organizaciones gubernamentales y pequeñas empresas. **La empresa fabrica dispositivos de seguridad de red (vendidos bajo su línea FortiGate) y software que integran funciones de antivirus, cortafuegos, filtrado de contenidos, sistemas de prevención de intrusiones (IPS) y antispam para proteger contra virus informáticos, gusanos y contenido web inapropiado**. También ofrece productos complementarios que incluyen sus sistemas de gestión de seguridad FortiManager y de análisis de eventos FortiAnalyzer. Para dar soporte a su canal global ampliamente disperso y a su base de clientes finales, cuenta con profesionales de ventas en más de 80 países de todo el mundo. Más del 40% de los ingresos provienen de América.

¿Lo sabías?



(1) Fuente: eMarketer

(2) Fuente: SonicWall

Fuente: Cybersecurity Ventures

* CAGR: Compounded annual growth rate (Tasa de crecimiento anual compuesto)

www.santanderprivatebanking.com