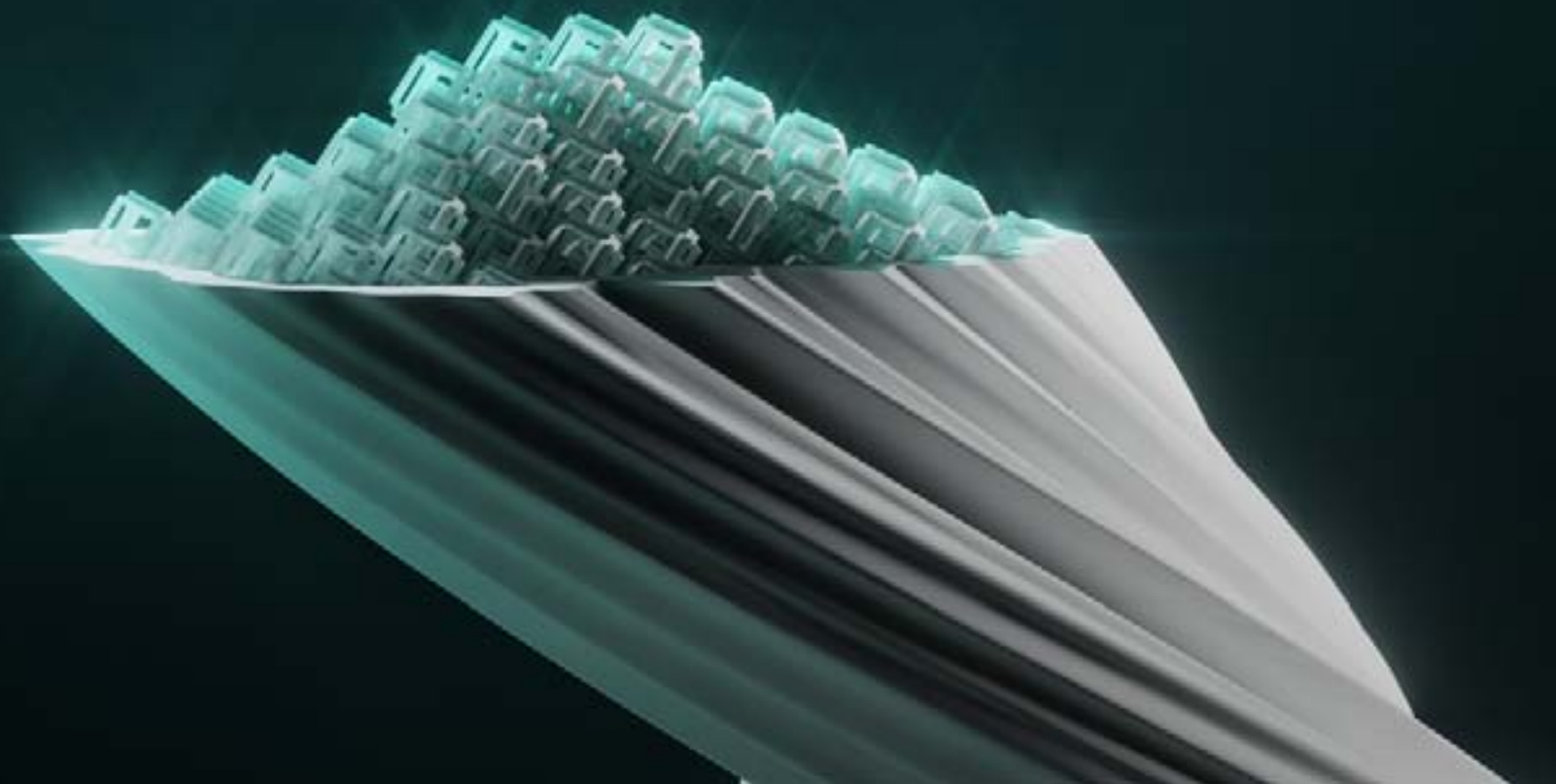
# LOS 5 PRINCIPALES DESAFÍOS DE SEGURIDAD PARA LOS CISO

¿Qué tener en cuenta en la era pospandémica?



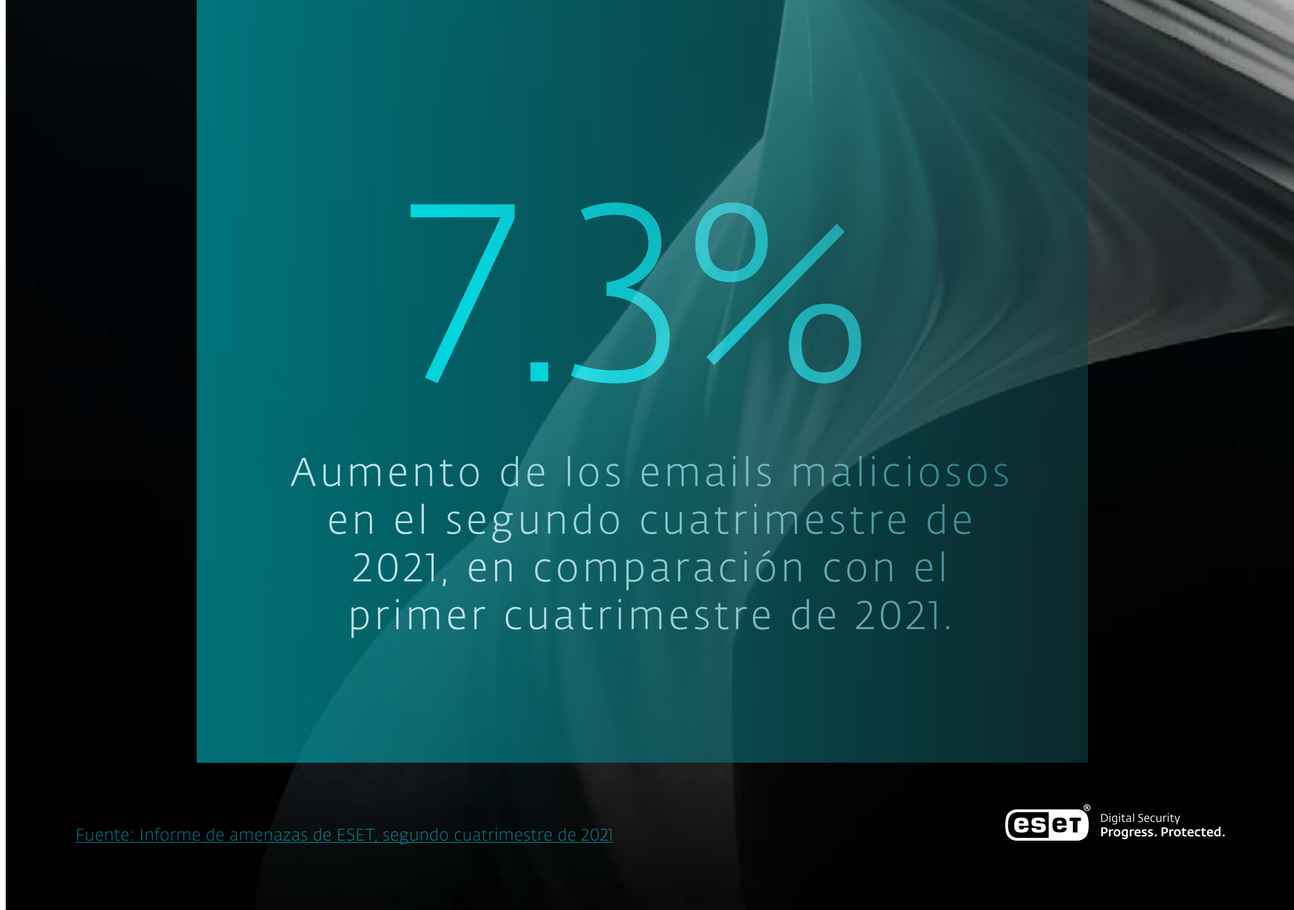
ESET®

Digital Security
**Progress. Protected.**

Los CISO (directores de seguridad de la información) saben que las tendencias de ciberseguridad evolucionan con relativa lentitud de un año a otro. Rara vez se produce una innovación repentina en el crimen cibernético que requiera una reestructuración radical de la estrategia de defensa. Sin embargo, la pandemia cambió por completo este cálculo.

Prácticamente de la noche a la mañana, las organizaciones se vieron obligadas a revisar a fondo los procesos empresariales para hacer posible el trabajo masivo desde casa y diseñar nuevas formas de llegar a sus clientes. En ESET hicimos la transición de cientos de empleados al trabajo remoto en pocos días, luchando mientras tanto contra los cuellos de botella de las redes VPN y la nube, y los desafíos que presentaban los dispositivos.

Lamentablemente, en muchos casos, estas nuevas inversiones digitales y prácticas de trabajo crearon nuevas oportunidades para los actores de las amenazas. La cantidad de ataques de phishing se disparó. Los actores del ransomware se aprovecharon de las vulnerabilidades de las VPN y de la mala configuración del protocolo RDP en las endpoints. Las aplicaciones en la nube desprotegidas se convirtieron en un importante foco de ataque. El aumento de las amenazas ha revelado a las organizaciones lo que los CISO ya sabían: que dar prioridad a la continuidad del negocio por encima de todo lo demás conlleva riesgos significativos.




Fuente: Informe de amenazas de ESET, segundo cuatrimestre de 2021

“Son tantos los colaboradores que siguen trabajando desde casa, que muchas tareas administrativas se realizan por vía electrónica, y los ciberdelincuentes se están aprovechando de ello.“

**Jiří Kropáč**

Jefe de los Laboratorios de Detección de Amenazas de ESET

Fuente: Informe de amenazas de ESET, segundo cuatrimestre de 2021

## ¿Cómo mitigar los riesgos emergentes?

Ahora que estamos saliendo de lo peor de la crisis, las organizaciones deben reevaluar su tolerancia al riesgo y lograr un equilibrio entre las operaciones comerciales y la seguridad. El lugar de trabajo híbrido que la mayoría está adoptando es un entorno más fluido y abierto que su equivalente anterior a la pandemia. Por lo tanto, para muchos, la atención ahora debe centrarse en mitigar los riesgos sin que esto afecte excesivamente la productividad.

Por suerte, aunque las organizaciones están atravesando otro intenso período de cambios, las mejores prácticas de seguridad siguen siendo tan válidas hoy como siempre, mientras que los nuevos enfoques ofrecen soluciones innovadoras para los desafíos emergentes. Este manual ayudará a los CISO a predecir dónde puede ser más acentuado el riesgo y qué medidas pueden mitigarlo mejor.

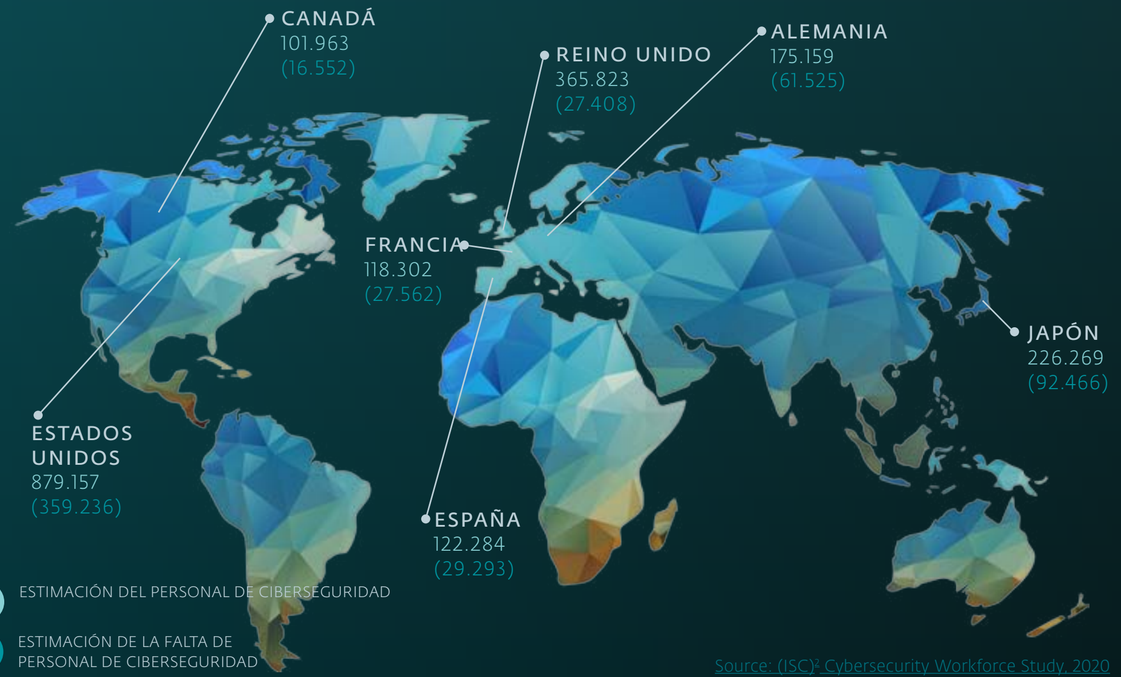

# 1. Afrontar la gran crisis de la falta de profesionales de seguridad

Todos sabemos que cada vez es más difícil reclutar especialistas en seguridad. Aunque la carencia de personal se redujo por primera vez en 2020, el déficit mundial de profesionales cualificados sigue siendo de más de tres millones, incluyendo más de 359.000 en los Estados Unidos. El rápido crecimiento de la nube, los dispositivos de la IoT y otros proyectos de transformación digital ha creado una demanda de especialistas en seguridad que supera con creces la oferta. A medida que estas inversiones continúen en la era pospandémica, la escasez de competencias se agudizará, en especial cuando se jubilen los profesionales de mayor edad. La necesidad de profesionales especializados en la seguridad en la nube es particularmente grande. El aumento de los incidentes como consecuencia de la mala configuración en los últimos tiempos pone de manifiesto el impacto potencial para las empresas.

Los planes del gobierno para incentivar el ingreso de más estudiantes a la industria son bienvenidos, pero incluso si tienen éxito, tardarán años en dar resultado. Mientras tanto, los CISO deben intentar aprovechar la tecnología y la tercerización de modo de mitigar los peores efectos de la falta de especialistas. Eso significa recurrir al Machine Learning y a la automatización para aliviar el trabajo de la gestión de cuentas, la optimización de políticas, las auditorías de código, y la detección y respuesta ante amenazas. En cuanto a lo último, una creciente gama de servicios de detección y respuesta gestionada (MDR) les ofrece a los CISO nuevas oportunidades para delegar la responsabilidad de operar las soluciones EDR y XDR. Esto no solo ayuda a atenuar los problemas de falta de especialistas, sino que pone estas capacidades en manos de expertos formados, que también pueden aportar su experiencia y conocimientos de todo el sector.



## Estimaciones del personal de seguridad y de la falta de ellos en el mundo

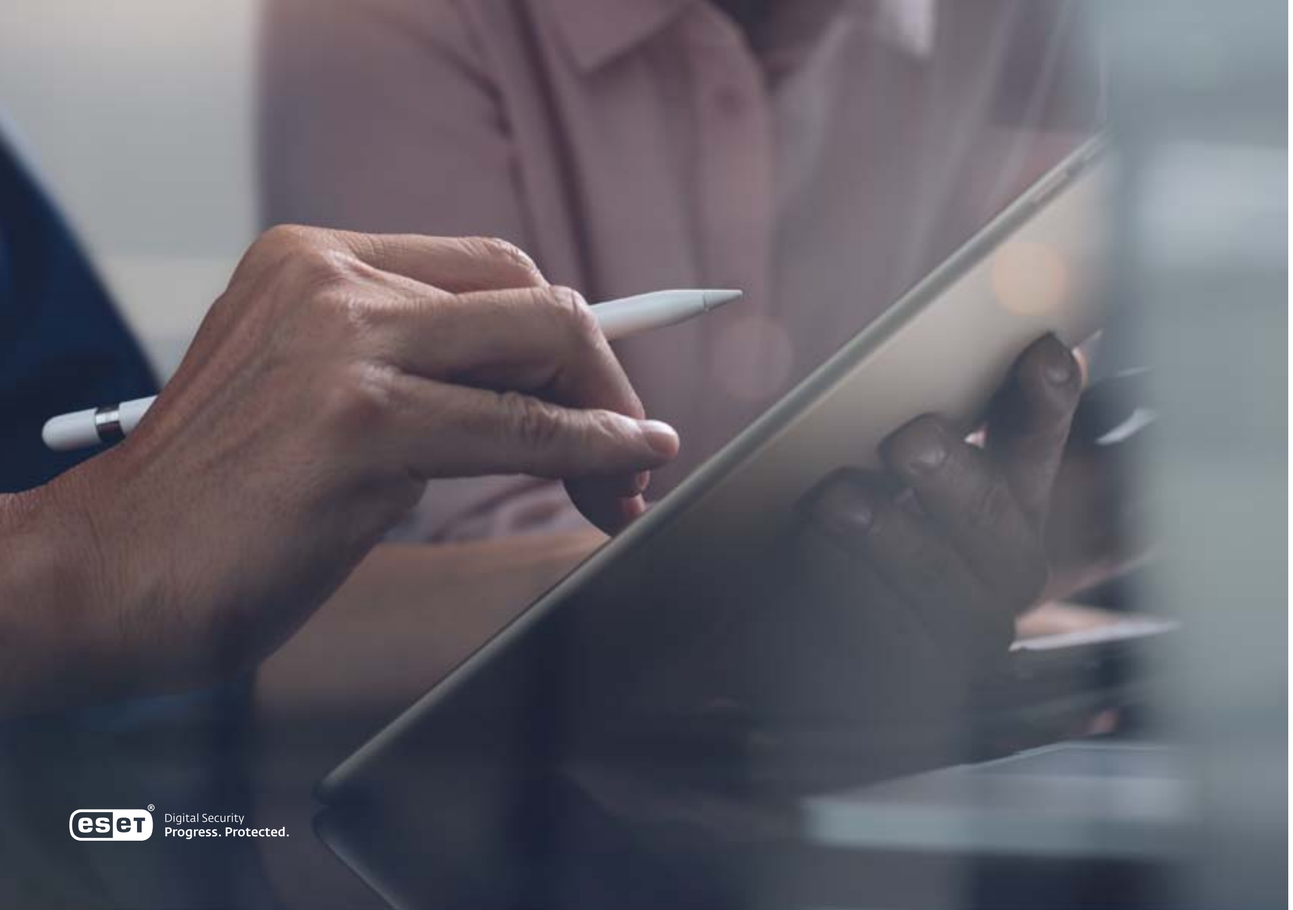



Source: (ISC)² Cybersecurity Workforce Study, 2020

Las empresas de TI también tienen un papel que desempeñar. Mediante la creación de centros informáticos, programas educativos y otras actividades de divulgación, incluyendo el trabajo voluntario (como hacen muchos empleados de ESET), pueden ayudar a mejorar la concientización sobre la seguridad y fomentar el interés por ella en los estudiantes de edad escolar.

**67%** de los líderes empresariales comprenden la importancia de la seguridad en los entornos de trabajo remotos. La falta de concientización tiene un impacto real sus equipos.

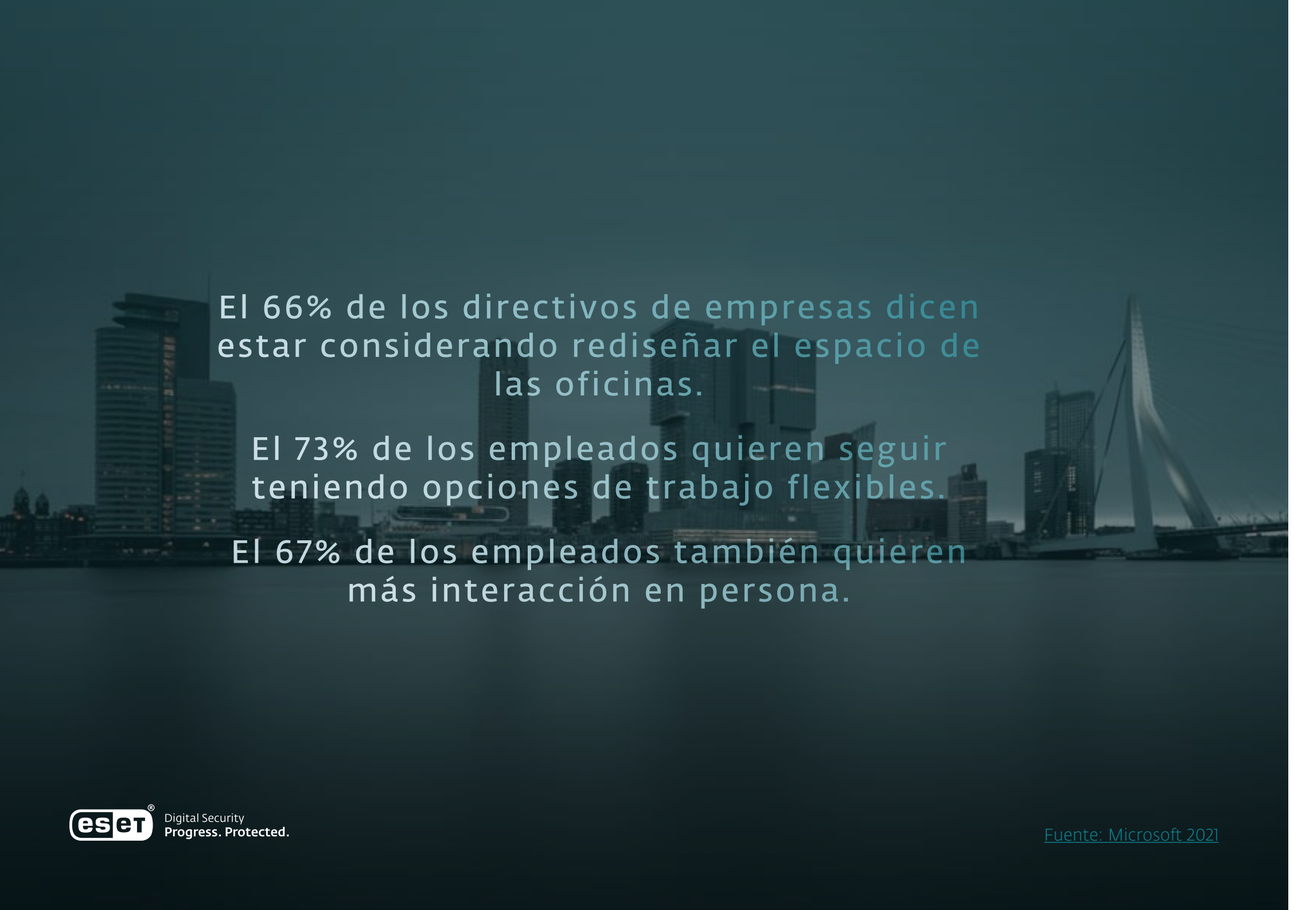
Fuente: (ISC)² Estudio sobre el personal de ciberseguridad 2020




# 2. Gestionar el riesgo de terceros

Las cadenas de suministro han sido objeto de un minucioso examen durante la pandemia. De hecho, muchas empresas las han dado por sentado hasta tal punto que ni siquiera están seguras de cuántos proveedores externos les suministran productos y servicios esenciales. Además, las personas que contratan terceros para su organización también pueden representar un importante riesgo cibernético, especialmente si se les permite el acceso a las redes y recursos corporativos. Un estudio de 2018 reveló que los empleados y los terceros contratados negligentes se consideran el eslabón más débil de la cadena de seguridad, potencialmente responsables de las vulneraciones de datos, los ataques de phishing y las infecciones de ransomware. El problema se ve agravado por el hecho de que las empresas contratadas no suelen estar incluidas en los programas de formación y concientización sobre seguridad para el personal.

Idealmente, los CISO deberían querer que sus proveedores tengan el mismo o mejor nivel de seguridad que su propia organización. Para ello es necesario realizar una evaluación continua, que puede basarse en cuestionarios elaborados a partir de las políticas y normas internas. Las certificaciones de los proveedores también proporcionan información útil sobre la adopción de controles y algunas pueden evaluarse automáticamente. De hecho, la automatización mediante las herramientas de gestión de riesgos de los proveedores (VRM) es útil para comprobar los datos abiertos y estimar la postura de seguridad en diversas áreas de las empresas contratadas. Ciertos proveedores incluso tienen honeypots (equipos utilizados como trampas de malware) privados para comprobar si hay ataques. Las organizaciones deben preguntarse primero cuáles son sus prioridades con respecto a la gestión de riesgos de los proveedores y, en función de sus respuestas, desarrollar la estrategia correspondiente.




# 3. La nueva realidad del lugar de trabajo híbrido

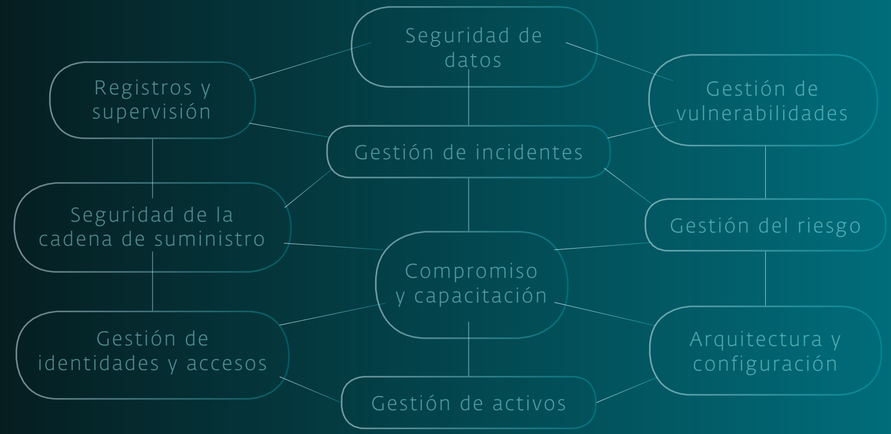
El trabajo híbrido es una oportunidad para tener lo mejor de ambos mundos: satisfacer las nuevas expectativas de los empleados en cuanto a la conciliación de la vida laboral y familiar, al tiempo que se impulsa la innovación a través de las interacciones cara a cara. Sin embargo, también expone a las organizaciones a los riesgos asociados al trabajo remoto: usuarios distraídos, endpoints e infraestructura de acceso remoto sin parches instalados, contraseñas de cuentas débiles y uso de la nube mal configurada. Por otra parte, cuando los empleados vuelven a viajar al trabajo, hay que sumarle la creciente amenaza de la pérdida o el robo de dispositivos, el robo de datos confidenciales espiando al usuario por sobre el hombro mientras navega, y las redes Wi-Fi no seguras.

Los CISO deben replantearse la política de seguridad corporativa poniendo el foco en este nuevo panorama. Esto podría significar la implementación de la autenticación en varias fases, controles de acceso más estrictos y la microsegmentación como parte de una campaña basada en el enfoque de confianza cero. También podría significar la tercerización de la detección y respuesta a las amenazas a través de servicios MDR, y la creación de nuevos cursos de concientización y formación para los empleados. Lo más importante es que sea una combinación de personas, procesos y tecnologías basada en las mejores prácticas, como las que enumeramos a la derecha.

## MÁS INFORMACIÓN SOBRE CÓMO PROTEGER A SUS COLABORADORES REMOTOS.

## 10 pasos para lograr la seguridad IT

¿En qué debe centrarse para proteger su empresa?




Fuente: NCSC, 2021


# 4. Aplicar el enfoque de confianza cero

El lugar de trabajo híbrido se caracterizará por el uso de los dispositivos propios de los empleados para trabajar (BYOD), los entornos en la nube híbrida y el movimiento habitual de los empleados dentro y fuera del perímetro corporativo tradicional. Este tipo de complejidad es difícil de gestionar manteniendo a su vez la productividad y una experiencia de usuario fluida. Para esto se creó el enfoque de confianza cero. Descrito por primera vez hace más de una década, se basa en la noción de "nunca confíe; siempre verifique" para reducir el impacto de las vulneraciones. Esto significa tratar todas las redes como si no fueran de confianza; autenticar continuamente a los usuarios y dispositivos; aplicar el principio del mínimo privilegio; y asumir que ya ha sido vulnerado.

La buena noticia es que muchos de los pasos necesarios para implementar la confianza cero (como el 2FA, la microsegmentación, las soluciones EDR, los firewalls basados en el host, el cifrado y la gestión de vulnerabilidades) probablemente ya formen parte de su configuración actual.

## Áreas clave en las que los CISO pueden actuar


Fuente: Brian Kime, Forrester, analista senior y orador invitado en ESET World


# 5. Llegó el momento de la seguridad proactiva

Los CISO comprenden instintivamente que mitigar el riesgo cibernético es más barato y más fácil cuando se hace con antelación, a través de medidas proactivas. El reto consiste en encontrar suficientes recursos y saber hacia dónde orientarlos para obtener el mejor valor.

Las pruebas de penetración son útiles para encontrar vulnerabilidades y ayudan a priorizar los esfuerzos de aplicación de parches. De todas formas, si estas herramientas no están integradas en los procesos de desarrollo/operativos, pueden ralentizar la velocidad de la corrección. Lo mejor son las soluciones de instalación automática de parches basadas en el riesgo, para ayudar a las organizaciones a priorizar la enorme cantidad de vulnerabilidades CVE que los desborda cada semana.

Otro paso es desplegar soluciones EDR y XDR para identificar en forma proactiva y rápida las amenazas ocultas. De esta forma, gracias a la correlación y el análisis, se descubren actividades que los ojos humanos pueden pasar por alto. Aquí hay algunos consejos útiles. Con respecto a la mala configuración, el cifrado de los datos, las verificaciones automatizadas de la configuración de las políticas durante las primeras fases del ciclo de vida del desarrollo y la auditoría continua a través de las herramientas de gestión de la seguridad en la nube (CSPM) pueden ayudar a mitigar los riesgos.

Sobre todo, a medida que su organización sigue cambiando y su modelo de negocio evoluciona, es importante garantizar que la estrategia y la cultura de seguridad vayan a la par. Esto no solo significa desplegar controles adicionales y ampliar la función en sí misma a medida que el entorno informático se hace más grande y complejo, sino también formalizar los procesos mediante un marco de gestión adecuado. Este es el tipo de madurez organizativa que su empresa puede llegar a necesitar y en el que los CISO deberían enfocarse, a medida que llega un nuevo período de crecimiento pospandémico.



## Más de 18.000 vulnerabilidades CVE

se conocieron en 2020: más que en cualquier otro año.

## Más de 7 mil millones de registros vulnerados

en 2019 se debieron a errores de configuración evitables.

Fuente: Análisis de vulnerabilidades Redscan del instituto NIST, 2020

# ¿DESEA COMENZAR UNA GESTIÓN DE DETECCIÓN Y RESPUESTA PARA ENDPOINTS EFECTIVA?

## La solución EDR de ESET brinda una visibilidad completa y una remediación sincronizada

MÁS INFORMACIÓN

eset Digital Security
Progress. Protected.

Por más de 30 años, ESET® ha estado desarrollando soluciones de seguridad líderes en la industria para las empresas y los consumidores de todo el mundo. Con las soluciones de seguridad que van desde la protección de endpoints y dispositivos móviles, hasta el cifrado y la autenticación en dos fases, los productos de alto rendimiento y fáciles de usar de ESET les ofrecen a los usuarios y a las empresas la tranquilidad que necesitan para disfrutar de su tecnología a pleno. ESET brinda protección y supervisión en forma discreta las 24 horas, los 7 días de la semana, y actualiza las defensas en tiempo real para mantener a los usuarios seguros y a las empresas funcionando sin interrupciones.



Digital Security
**Progress. Protected.**