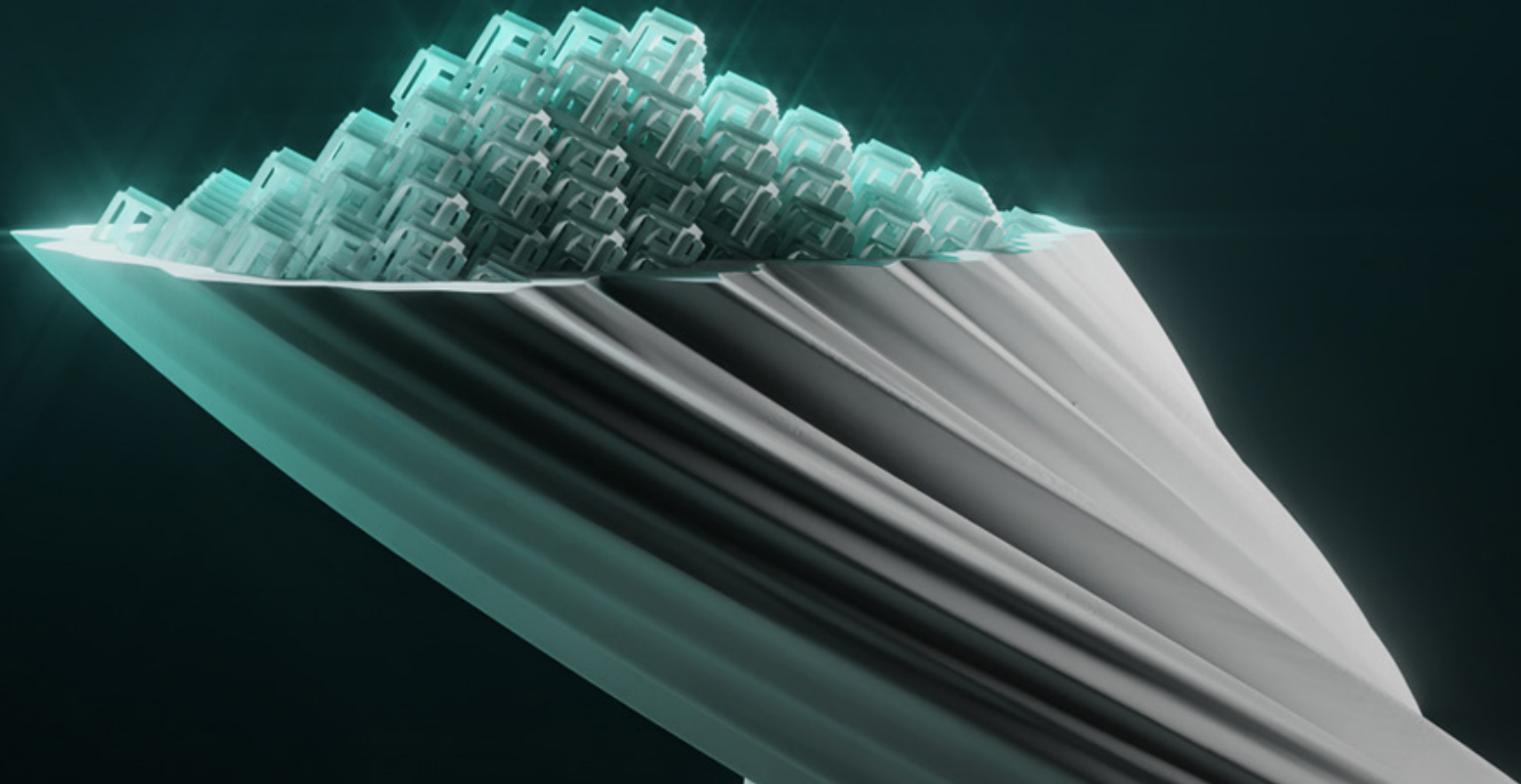


LOS CINCO PRINCIPALES DESAFÍOS PARA LOS CISOs

Qué hay que tener en cuenta en la era postpandémica



Digital Security
Progress. Protected.



Los CISO saben que las tendencias de ciberseguridad evolucionan con relativa lentitud de un año a otro. Rara vez se produce un momento de innovación en materia de ciberdelincuencia que exija una reestructuración radical de la estrategia. La pandemia cambió por completo este cálculo.

Casi de la noche a la mañana, las empresas se vieron obligadas a revisar radicalmente sus procesos de negocio, para apoyar 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 cuestión de días, luchando contra los bloqueos de la VPN y la nube y los desafíos de los dispositivos en el proceso.

Lamentablemente, en muchos casos estas nuevas inversiones digitales y prácticas de trabajo crearon nuevas oportunidades para los autores de las amenazas. Los volúmenes de phishing se dispararon. Los autores del ransomware se aprovecharon de las vulnerabilidades de las VPN y de los equipos RDP mal configurados. Las aplicaciones en la nube mal protegidas se convirtieron en un importante foco de ataque. El aumento de las amenazas indicó a las empresas lo que los CISO ya sabían: que priorizar la continuidad del negocio por encima de todo conlleva riesgos significativos.

7.3%

Aumento de los correos electrónicos maliciosos en el 2T de 2021, en comparación con el 1T de 2021.

“Como muchos siguen trabajando desde casa, los empleados se han acostumbrado a realizar muchas tareas administrativas por vía electrónica, y los ciberdelincuentes se aprovechan de ello”.

Jiří Kropáč

Jefe de los laboratorios de detección de amenazas de ESET

¿Cómo mitigar los riesgos emergentes?

Ahora que estamos saliendo de lo peor de la crisis, las empresas deben reevaluar su capacidad de riesgo y el equilibrio entre las operaciones empresariales y la seguridad. El lugar de trabajo híbrido que la mayoría está adoptando será un entorno más fluido y abierto que su equivalente anterior a la pandemia. Por lo tanto, para muchos, la atención debe centrarse ahora en la mitigación del riesgo que no afecte excesivamente a la productividad.

Afortunadamente, aunque las empresas están atravesando otro intenso periodo de cambio, las mejores prácticas de seguridad siguen siendo tan válidas hoy como siempre, mientras que los nuevos enfoques ofrecen soluciones innovadoras a los nuevos retos. El siguiente manual ayudará a los CISO a anticiparse a los lugares en los que el riesgo puede ser más agudo, y a las medidas que pueden mitigarlo mejor.



Digital Security
Progress. Protected.

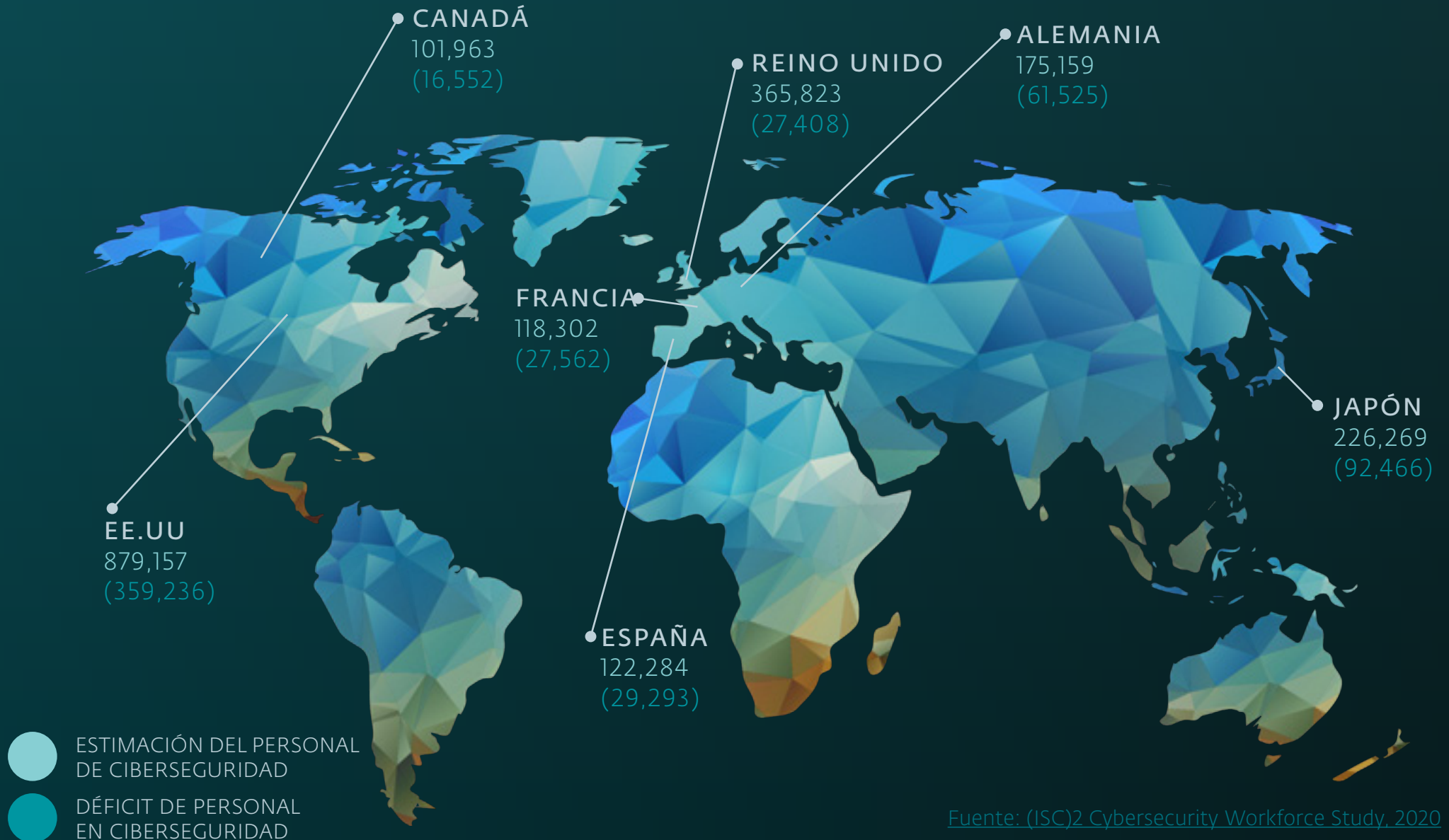
1.

Cómo afrontar la gran crisis de conocimientos en materia de seguridad

Todos sabemos que cada vez es más difícil contratar a profesionales de la seguridad. Aunque la falta de mano de obra se cerró por primera vez en 2020, el déficit mundial de profesionales cualificados sigue siendo de más de tres millones, incluidos más de 359.000 en Estados Unidos. El rápido crecimiento de la nube, el IoT y otros proyectos de transformación digital ha creado una demanda de habilidades de seguridad que supera con creces la oferta. A medida que estas inversiones continúen en la era postpandémica, la escasez de habilidades se agudizará, especialmente a medida que los profesionales de mayor edad se jubilen. La necesidad de talento para la seguridad en la nube es especialmente grande. El aumento de los incidentes de mala configuración en los últimos tiempos pone de manifiesto el impacto potencial para las empresas.

Los planes del gobierno para animar a más estudiantes a entrar en la industria son bienvenidos, pero incluso si tienen éxito, tardarán años en tener un resultado. Mientras tanto, los CISO deberían intentar aprovechar la tecnología y la subcontratación para mitigar los peores efectos de los riesgos de las competencias. Esto significa buscar el aprendizaje automático y la automatización para eliminar el trabajo preliminar de cosas como la gestión de cuentas, la optimización de políticas, las auditorías de código y la detección y respuesta a las amenazas. En cuanto a esto último, una gama cada vez mayor de servicios de detección y respuesta gestionados (MDR) ofrece a los CISO nuevas oportunidades para ceder la responsabilidad de operar las soluciones EDR y XDR. Esto no solo ayuda a aliviar los desafíos de habilidades, sino que pone estas capacidades en manos de expertos capacitados, que también pueden aportar su experiencia y conocimiento de la industria.

Estimaciones del personal de seguridad mundial y de las posibles deficiencias



Fuente: (ISC)2 Cybersecurity Workforce Study, 2020

Las empresas de IT también tienen un papel que desempeñar. Mediante la creación de centros informáticos, programas educativos y otras actividades de divulgación, incluido el voluntariado (como hacen muchos empleados de ESET), pueden ayudar a impulsar la concienciación sobre la seguridad y el interés por ella entre los estudiantes en edad escolar.

67%

de los líderes empresariales comprenden la importancia de la seguridad en los entornos de trabajo remotos. La falta de concienciación de los líderes tiene un impacto real en los equipos.

SERVICIOS DE DETECCIÓN Y RESPUESTA GESTIONADOS POR ESET

Prevenir. Reaccionar. Prever.

Benefíciate de los conocimientos de nuestros
equipos de investigación de seguridad
informática de categoría mundial

MÁS INFORMACIÓN



2.


Gestión del riesgo frente a terceros

Las cadenas de suministro se han sometido a un minucioso escrutinio durante la pandemia. Esto es algo bueno. De hecho, muchas empresas las han dado por sentadas, hasta el punto de que muchas ni siquiera están seguras de cuántos distribuidores externos utilizan para suministrar productos y servicios esenciales. Desafortunadamente, aquellos proveedores para tu empresa también pueden representar un riesgo cibernético importante, especialmente si se les permite el acceso a las redes y recursos corporativos. Un estudio de 2018 descubrió que las personas internas negligentes y los distribuidores se consideran el eslabón más débil de la cadena de seguridad, potencialmente responsable de las violaciones de datos, los ataques de phishing y los secuestros de ransomware. Para agravar el problema está el hecho de que los distribuidores a menudo no están incluidos en los programas de formación y concienciación de seguridad del personal.

Lo ideal es que los CISOs quieran que sus distribuidores tengan el mismo o mejor nivel de seguridad que su propia empresa. Para conseguirlo se requiere una evaluación continua, quizás basada en cuestionarios elaborados a partir de las políticas y normas internas. Las certificaciones de los distribuidores también pueden proporcionar información útil sobre la adopción de controles y algunas pueden evaluarse automáticamente. De hecho, la automatización es útil a través de las herramientas de gestión de riesgos de proveedores (VRM), para comprobar los datos abiertos y estimar la postura de seguridad de los distribuidores en diversas áreas. Algunos proveedores incluso ejecutan honeypots privados para comprobar la existencia de ataques. Las empresas deben preguntarse primero cuáles son sus prioridades con VRM y, en función de estas respuestas, desarrollar la estrategia correspondiente.

Amplía tu inteligencia de seguridad desde las redes locales al ciberespacio global, con los informes y fuentes de ESET Threat Intelligence

MÁS INFORMACIÓN

A dark, atmospheric photograph of a city skyline at dusk or night. The buildings are silhouetted against a dark sky, with some lights visible. The water in the foreground is dark and calm.

El 66% de los líderes empresariales dicen que están considerando rediseñar el espacio de la oficina.

El 73% de los empleados quiere seguir siendo flexible con opciones de trabajo.

El 67% de los empleados también quiere más trabajo presencial.

3.

La nueva realidad del lugar de trabajo híbrido

El trabajo híbrido es una oportunidad para tener lo mejor de los dos mundos online y offline: 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 presenciales. Sin embargo, también expone a las empresas a los riesgos asociados al trabajo a distancia: usuarios distraídos, equipos e infraestructuras de acceso remoto sin parches, contraseñas de cuentas débiles y desconfiguración de la nube. Además, existe una elevada amenaza de pérdida/robo de dispositivos, navegación ilegal y redes wifi inseguras que afectan a los empleados cuando vuelven a viajar.

Los CISO deberían revisar la política de seguridad corporativa con la vista puesta en este nuevo entorno. Esto podría significar el desarrollo de MFA, controles de acceso más estrictos y microsegmentación como parte de un impulso de confianza cero. También podría significar la contratación externa de la detección y respuesta a las amenazas a través de MDR, y la creación de nuevos cursos de concienciación y formación para los empleados. Lo más importante es que implicará una combinación de personas, procesos y tecnología basada en las mejores prácticas, como las que se enumeran a continuación.

10 medidas de ciberseguridad

¿En qué debes centrarte si quieres proteger tu negocio de forma eficaz?





Digital Security
Progress. Protected.

4.

Considera un planteamiento basado en la confianza cero

El lugar de trabajo híbrido se caracterizará por el BYOD (usar dispositivos personales para el trabajo), los entornos de nube híbrida y el movimiento regular de los empleados dentro y fuera del perímetro corporativo tradicional. Este tipo de complejidad es increíblemente difícil de gestionar a la vez que se mantiene la productividad y una experiencia de usuario fluida. Para esto se creó Zero Trust o confianza cero. Descrita por primera vez hace más de una década, se basa en la noción de "nunca confíes, siempre verifica" para reducir el impacto de las infracciones. Esto significa tratar todas las redes como no fiables y autenticar continuamente a los usuarios y dispositivos, aplicar el principio del mínimo privilegio y asumir que ya se ha producido una infracción.

La buena noticia es que muchos de los pasos necesarios para impulsar la confianza cero, como la autenticación de múltiples factores, la microsegmentación, el EDR, los cortafuegos basados en el host, el cifrado de datos y la gestión de la vulnerabilidad, pueden formar ya parte de tu configuración.

Áreas clave en las que los CISOs pueden actuar



Fuente: [Brian Kime, Forrester - analista senior y ponente invitado en ESET World](#)

SOLUCIONES DE IDENTIDAD Y PROTECCIÓN DE DATOS DE ESET

Descubre el cifrado totalmente probado y la sencilla pero potente autenticación multifactor, para garantizar que los datos de tu empresa están protegidos de acuerdo con los requisitos de cumplimiento.

MÁS INFORMACIÓN



5.

Es el momento para la seguridad proactiva

Los CISOs comprenden instintivamente que mitigar el riesgo cibernético es más barato y más fácil cuando se hace con antelación, mediante medidas proactivas. El reto consiste en encontrar suficientes recursos y saber dónde concentrarlos para obtener el mejor valor. La magnitud del reto parece abrumadora.

Las pruebas de detección ofrecen una forma útil de encontrar vulnerabilidades explotables en la empresa y pueden ayudar a priorizar los esfuerzos de aplicación de parches, aunque la falta de integración de estas herramientas en los procesos de desarrollo/operativos puede ralentizar la velocidad de corrección. Lo mejor son las soluciones de parcheo automatizadas y basadas en el riesgo, para ayudar a las empresas a priorizar el enorme número de vulnerabilidades que les inundan cada semana.

Otro paso es la implementación de EDR y XDR, para identificar proactiva y rápidamente las amenazas encubiertas a través de la correlación y el análisis que descubren la actividad que los ojos humanos pueden pasar por alto. Hay algunos consejos útiles aquí. En cuanto a la configuración errónea, el cifrado de los datos, las comprobaciones automatizadas de la configuración de las políticas en 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 tu empresa sigue cambiando y su modelo de negocio evoluciona, es importante garantizar que la estrategia y la cultura de seguridad sigan el ritmo. Esto significa no solo la implementación de controles adicionales y la ampliación de la propia función a medida que el entorno de IT se hace más grande y complejo, sino también la formalización de los procesos a través de un marco de gestión adecuado. Ese es el tipo de madurez organizativa que puede necesitar tu empresa, y en el que los CISOs deberían centrarse, al entrar en un nuevo periodo de crecimiento postpandémico.

Más de 18.000 CVEs

se divulgaron en 2020, más que en cualquier otro año.

Más de 7.000 millones de registros vulnerados

en 2019 se debieron a errores de configuración evitables.

¿QUIERES EMPEZAR CON BUEN PIE LA DETECCIÓN Y RESPUESTA A LOS EQUIPOS?

ESET EDR proporciona una visibilidad excepcional
y una reparación sincronizada

MÁS INFORMACIÓN



Durante más de 30 años, ESET® ha desarrollado software de seguridad líder en el sector para empresas y consumidores de todo el mundo. Con soluciones de seguridad que van desde la defensa de equipos y móviles hasta el cifrado y la autenticación de dos factores, los productos de alto rendimiento y fáciles de usar de ESET ofrecen a los usuarios y a las empresas la tranquilidad necesaria para disfrutar de todo el potencial de su tecnología. ESET protege y supervisa de forma discreta las 24 horas del día, actualizando las defensas en tiempo real para mantener a los usuarios seguros y a las empresas en funcionamiento sin interrupciones.



Digital Security
Progress. Protected.

© 1992 - 2022 ESET, spol. s r.o. - Todos los derechos reservados.

Las marcas utilizadas en este documento son marcas comerciales o marcas registradas de ESET, spol. s r.o. o ESET North America.

Todos los demás nombres y marcas son marcas registradas de sus respectivas compañías.