Anticipando lo desconocido

Director General de Seguridad de la Información (CISO) Reporte de Referencia

CISCO

Contenido

Introducción: nada veo, nada bloqueo

Imaginen que pueden ver en el futuro. Y también hacia el pasado al mismo tiempo. Imaginen tener visibilidad de todo lo que ha sucedido y todo lo que sucederá, en cualquier lugar, todo a la vez.

Imaginen tener un poder de procesamiento lo suficientemente potente como para dar sentido a todos estos datos en cada idioma y en todas las dimensiones. A menos que hayan alcanzado ese nirvana de datos digitales (y no nos lo hayan dicho), su mundo tendrá interrogantes.

En el mundo de la seguridad, las amenazas desconocidas existen fuera de la empresa en la forma de ciberdelincuentes, ataques patrocinados por el estado y malware que se mueve rápido y destruye todo lo que toca. Lo desconocido existe dentro de la empresa en la forma de amenazas internas de empleados sospechosos o contratistas descuidados, que representan para el 24 % de los encuestados considera el riesgo más grave para sus organizaciones. Lo desconocido existe en la forma de nuevos dispositivos, nuevas aplicaciones en la nube y nuevos datos. Lo desconocido es lo que mantiene a los CISO, a ustedes, despiertos por la noche; lo sabemos porque les preguntamos.

Este es el 12.° año consecutivo que publicamos nuestras conclusiones sobre el panorama de la ciberseguridad y el 5.° año que realizamos el estudio de parámetros de miles de líderes de seguridad. Y este informe es solo la punta del iceberg de los datos de la encuesta generada. El próximo año publicaremos más datos de parámetros por sector, geografía, tamaño de empresa y función laboral, entre otros filtros. Para actualizar este informe, hemos encuestado a más de 3200 líderes de seguridad de 18 países, con preguntas en tres categorías:

1. **Configuración**: ¿cómo se preparan para lograr el éxito con capacitaciones, presupuestos, simulacros, mejores prácticas y otras competencias?
2. **Arquitectura**: ¿cuál es el enfoque para la selección de soluciones/proveedores y la gestión de alertas?
3. **Preparación y respuesta frente a las vulnerabilidades**: ¿cómo administran las vulnerabilidades en cuanto al impacto en los sistemas, cuánto se pierde y cuánto se tarda en recuperarlo?

Entrevista a Marisa Chancellor, Directora Senior, Organización de Seguridad y Confianza, Cisco

Usted protege a 70 000 empleados de Cisco en 400 oficinas con cientos de miles de terminales.

Eso es lo que llamo mi superficie de ataque y, como puede ver, hay un montón de cosas a las que las personas intentan llegar. Sí, hay empleados y centros de datos, pero además consumimos 600 nubes y contamos con una nube verdaderamente múltiple y un escenario de nube híbrida que defender.

Háblenos de la normativa de su equipo.

Estamos preparados para defender a Cisco y focalizados en equilibrar el riesgo de Cisco como empresa haciendo lo necesario con el riesgo de las amenazas internas y externas. Y nos enfocamos en impulsar la arquitectura de seguridad adecuada en nuestra organización de TI observando los incidentes que definen la estabilidad de nuestra postura de seguridad.

(Cont.)

A continuación, comparamos el rendimiento en estas áreas para ver si, desde el inicio del seguimiento, se avanzó en la construcción de defensas, la detección de ciberamenazas y la contención de vulnerabilidades de datos. Este informe arroja luz sobre qué acciones están cosechando resultados en el fortalecimiento de la salud cibernética organizacional para que puedan aprender de sus compañeros.

Por ejemplo, cuando preguntamos, solo el 35% pudo confirmar que "es fácil determinar el alcance de un ataque, controlarlo y corregirlo de las vulnerabilidades", lo que sugiere que la visibilidad de lo desconocido es claramente un desafío clave. Tal vez fue la parte "fácil" la que los confundió, debido a que los incidentes, a menudo, no son lo que parecen. Esto significa que el 65 % de los CISO en la encuesta tiene oportunidad para mejorar. Y nos tenemos que conformar con el 46 % que dijo que "tiene herramientas vigentes que permiten revisar y brindar comentarios relacionados con las capacidades de la práctica de seguridad". Si reconocen que no pueden ver todo, como mínimo pueden medir y gestionar su capacidad para mejorar y tener mayor visibilidad.

Si bien la lucha está lejos de terminar, no todas son malas noticias. Al menos algunos encuestados parecen sentirse bien en sus puestos de trabajo. Les preguntamos si experimentaron cansancio por las ciberamenazas. Calificamos esto como un abandono virtual al tratar de mantenerse por delante de las amenazas maliciosas y los atacantes. Solo el 30 % de los encuestados afirmó que sufrió de cansancio por las ciberamenazas este año. Y aunque casi un tercio parece un gran número para alzar la bandera blanca y rendirse, la caída de la cifra del 46 % del año anterior va en el sentido correcto, por lo que vale la pena luchar.

(Cont.)

¿Qué la mantiene despierta por la noche?

Bueno, creo que para la mayoría de las personas que están en seguridad, lo que nos mantiene despiertos por la noche es lo desconocido. Cuando pienso en lo que debo proteger a diario, cuento con un equipo fantástico y tecnología muy capaz, pero nos concentramos en lo conocido cuando la verdadera amenaza es lo desconocido.

Los CISO informaron el número de alertas que tienen. ¿Cree que hay demasiadas para manejar?

Es cierto en el sector pero, diariamente en Cisco, analizamos 47 TB de eventos de red a diario, lo que se traduce en aproximadamente 22 incidentes por día, algo imposible de entender para el ser humano. Procede de todo el espectro, por lo que debemos averiguar cómo analizar dicha información y cómo hacer que la tecnología trabaje para nosotros. Poder utilizar el aprendizaje automático y la inteligencia artificial para eliminar una gran cantidad de alertas nos permite afinar las áreas más peligrosas en que centrarse. No contamos con un presupuesto ilimitado; por lo tanto, ¿cómo nos movemos a la velocidad de la máquina en lugar de la velocidad humana?

Vea más extractos de la entrevista a Marisa Chancellor en este informe.

Si se tiene en cuenta la capacidad para ver tanto el futuro como el pasado a la vez, parece una tarea fácil. Mejoremos lo que podemos ver en la actualidad y veamos algunas formas de medir bien, y no tan bien, los datos informados con anterioridad y en el presente.

"La Organización de Seguridad y Confianza es responsable de proteger a Cisco; tan sencillo como eso. Pero la otra cara es: **¿cómo nos aseguramos de que podemos acelerar el negocio?** No nos hace ningún bien bloquear el entorno completo si nada avanza."

Marisa Chancellor
Directora sénior, Organización de Seguridad y Confianza, Cisco

Mirar hacia atrás para avanzar

¿Los CISO mejoraron o empeoraron respecto del año pasado? Seleccionamos tres áreas que el año pasado fueron temas candentes y realizamos una clasificación según las respuestas de este año.

Tecnología

	Afirmó 2018	Afirma 2019	Queremos saber más porque...
Machine Learning (ML) ¿En qué medida confía del aprendizaje automático para reducir el nivel de esfuerzo requerido para proteger la organización?	77 %	↓67 %	En todo caso, las tendencias negativas en estas tres primeras preguntas probablemente provienen de la incertidumbre y la falta de confianza. O de que el aprendizaje automático no está listo en el mejor momento. De cualquier forma, queremos saber más.
Inteligencia artificial (AI) ¿En qué medida dependen de la inteligencia artificial para reducir el nivel de esfuerzo requerido para proteger la organización?	74 %	↓66 %	Podría ser que la adopción esté tan generalizada e integrada en los procesos empresariales que no valga la pena insistir.
Automatización ¿En qué medida dependen de la automatización para reducir el nivel de esfuerzo requerido para proteger la organización?	83 %	↓75 %	Es posible que se decida no ser "dependiente", sino selectivamente automatizado. Es posible que hasta las organizaciones más grandes no puedan adoptar por completo la automatización.

Costo de una vulnerabilidad

Pensando en la vulnerabilidad de más impacto que hayan experimentado en el último año, ¿cuál fue el costo total?	El 8 % afirmó que más de USD 5 millones	El 8 % afirmó que más de USD 5 millones	Las vulnerabilidades siguen siendo un consumo de recursos y su impacto es más que solo financiero.
	< USD 500 000 47 %	< USD 500 000 ↑51 %	Más del 50 % genera costos de vulnerabilidades por debajo del medio millón. ¡Excelente! Los costos disminuyen un poco o al menos están bajo control.
¿Qué mejoras se realizaron para proteger a las empresas de las vulnerabilidades de seguridad?			
Separación de las funciones de TI y seguridad	38 %	↓35 %	Este es un tema polémico y la falta de un gran viraje sugiere que están igualmente divididos como grupo.
Aumento de la cantidad de eventos de capacitación para la concientización sobre la seguridad entre los empleados	38 %	↑39 %	Siempre que las personas sean el eslabón más débil, no estará claro cuánta capacitación es suficiente.
Técnicas de mitigación de riesgos implementadas	37 %	↑39 %	Si se tiene en cuenta que este año el 20 % de los encuestados afirmó no estar muy bien informado sobre los riesgos y el cumplimiento, los marcos de riesgo se convierten en procedimientos operativos estándar.
Aumento de la inversión en soluciones o tecnologías de defensa ante amenazas de seguridad	41 %	↑44 %	Es bueno si se combina con la capacitación y la medición basada en resultados. Es bueno para las métricas de seguridad.

Nube

Trasladar la seguridad a la nube ha incrementado nuestra eficiencia, lo que permite a nuestro personal de seguridad centrarse en otras áreas	92 % De acuerdo	↑93 %	Adopción continua de la nube por las razones correctas.
El aprovechamiento de las soluciones de seguridad en la nube permite ser más eficaces que el trabajo en las instalaciones	91 % De acuerdo	↑93 %	¿Un leve aumento en la confianza de la seguridad en la nube? ¡Lo aceptamos!
¿Qué reto supone defender la infraestructura de la nube de los ciberataques?	55 % Muy de acuerdo	↓52 %	¿Una mayor disminución en la dificultad para proteger la infraestructura de la nube? ¡Incluso mejor!

Fuente: Reporte de referencia de CISO de Cisco de 2019

Estado de los CISO

Desde un tiempo hasta ahora, especialistas en amenazas han hablado sobre conocer lo desconocido. Es hora de ampliarlo a todo el espectro de la ciberseguridad: los usuarios, las aplicaciones, los datos y las nubes. No se puede proteger lo que no se ve.

Por lo general, querrán apoyar a la empresa y no embrollarla en la burocracia. Si van a ser un poco más abiertos, ¿cómo mitigan el control? Esto será diferente para cada uno. Los CISO deben lidiar con ese equilibrio de la cultura organizacional mientras se enfrentan a amenazas más graves. A veces bloquear todo no se adapta a la cultura de la empresa. Puede ser correcto para un banco, pero no para una universidad.

Los CISO enfrentan varios retos al gestionar el riesgo cibernético; sea cual sea su modelo de organización:

- Las vulnerabilidades crean efectos adversos para la rentabilidad financiera, la reputación de la marca, la seguridad de datos del cliente, la satisfacción del cliente y la continuidad del negocio.
- Las pérdidas pueden ser sustanciales y recuperables, lo que crea una mayor puntuación de riesgo para la organización respecto de la asegurabilidad.
- Con los años, las soluciones puntuales del proveedor parecían prometedoras; sin embargo, cada una genera su propio conjunto de alertas. Muchas soluciones puntuales que compiten con las alertas, dificultan la tarea de identificación de las amenazas que significan un mayor riesgo para la organización y merman los recursos.
- Generalmente la TI se aísla en la organización, lo que hace que la integración de la protección de endpoints de redes, nubes y empleados sea muy compleja.

"Te esfuerzas por entender cómo poder visualizar lo desconocido, por ejemplo, las nuevas amenazas que se acercan incluso desde tu propio entorno: dispositivos, aplicaciones, datos desconocidos. Si no se puede ver, no se puede proteger. Eso es lo que me despierta por la noche."

- No es necesaria una táctica agresiva para contratar personal de TI de seguridad, dado que el grupo especializado de candidatos no puede sostener la magnitud del problema a través de las organizaciones globales. No obstante, la escasez de talento está fuera de control y no es soluble si se intentan cubrir todos los puestos de trabajo.
- Nuevas amenazas aparecen diariamente, incluso cada hora, y ponen en práctica sus métodos más sigilosos y sofisticados. Recientemente señalamos a Emotet, Olympic Destroyer y otras amenazas frecuentes en el Informe de amenazas de Cisco de 2019. La respuesta ante amenazas como categoría debe evolucionar y se necesitan herramientas para consolidar la información y centralizar la remediación de infecciones y otros incidentes.

Tecnologías y procesos adicionales para que los CISO tengan en cuenta:

- La inteligencia artificial y el aprendizaje automático, usados correctamente, son esenciales para clasificar el volumen de trabajo.
- El costo de una vulnerabilidad disminuye...pero no se emocionen demasiado.
- Hay libertad para obtener beneficios evidentes en la mejora de los procesos, por ejemplo, la capacitación.
- Hay más confianza en la seguridad en la nube y en la protección en la nube.

Conclusiones de 2019

Nuestras conclusiones del análisis revelaron varias áreas fundamentales para fortalecer la estrategia de seguridad de la organización. Esta sección detalla nuestras conclusiones sobre dónde y cómo los CISO y sus colegas ponen en vigencia (o no) la tecnología y los procesos para mitigar el daño que las vulnerabilidades de ciberseguridad pueden tener en las organizaciones bajo los temas de mejores prácticas, enfoque arquitectónico y preparación ante vulnerabilidades.

Configuración para alcanzar el éxito

¿Qué significa ser un CISO día a día? ¿Cuál es su normativa? Nuestra encuesta actual revela varias áreas que en conjunto determinan el ciberestado de la organización, que incluye: ser prácticos sobre el riesgo, establecer criterios para la elaboración de presupuestos, colaborar entre las divisiones, educar al personal, llevar a cabo simulacros, saber cómo realizar un seguimiento de los resultados para informar las inversiones y ser estratégicos en la implementación de proveedores y soluciones.

Conozcan los riesgos

¿La gestión de riesgos es suficiente? Apenas. Entender los riesgos de los ciberataques y el panorama de cumplimiento que engloba las vulnerabilidades de seguridad es fundamental para comprender cómo defenderse y prepararse para lo peor. Al preguntar quiénes estaban bien informados sobre los riesgos y el cumplimiento, solo el 80 % de los encuestados respondió afirmativamente. Esto deja un 20 % de profesionales de seguridad que posiblemente pueda usar parte de la capacitación explicada anteriormente. Muchos interrogantes donde menos se los espera.

Cómo emplear el presupuesto

Casi la mitad, o el 47 %, determina cómo controlar los gatos de seguridad en función de los objetivos de resultados de la seguridad organizacional. Medir los resultados frente a las inversiones es el mejor enfoque basado en datos. Es más, el 98 % está totalmente o parcialmente de acuerdo en que el equipo ejecutivo ha establecido métricas claras para la evaluación de la eficacia del programa de seguridad. El 49 % de los encuestados tiene métricas que se usan en varias áreas de las empresas para comprender las decisiones basadas en los riesgos y mejorar los procesos a fin de medir la eficacia de la seguridad en toda la organización.

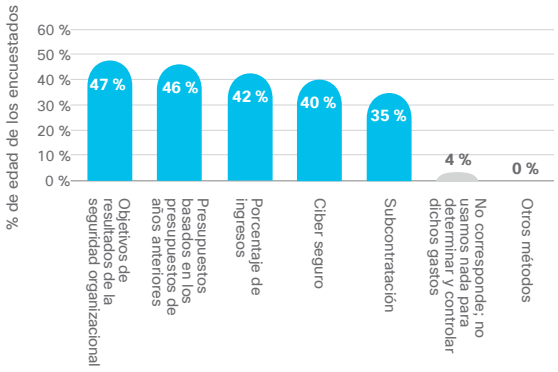
Volviendo al presupuesto y aparte de las mediciones basadas en resultados, como se muestra en la Figura 1, existen algunas opciones menos prósperas: controlar los gastos de seguridad de los presupuestos de años anteriores (46 %) y el porcentaje de los

"En algunas áreas, el riesgo no es tan alto dado que la organización tiene sólidas prácticas de seguridad; en otras áreas tenemos oportunidades para reforzar, minimizar y cerrar la vulnerabilidad de dicho riesgo. Y así es como invertimos y nos preparamos para las próximas amenazas. Debemos preguntarnos cómo podemos lograr que la arquitectura fundacional nos prepare de la mejor manera para lo que hay a la vuelta de la esquina."

ingresos respectivamente (42 %) eran dos opciones populares, pero no necesariamente correlativas con una mejor seguridad. El panorama de vulnerabilidades cambia anualmente y el presupuesto del año anterior o el porcentaje de los ingresos pueden tener poco que ver con el costo de defenderse frente a futuras amenazas.

El cuarto enfoque más confiable para determinar los gastos de seguridad es el ciber seguro: **el 40 % usa el ciber seguro, al menos en parte, para establecer los presupuestos.** La adopción de este enfoque comienza con una evaluación de riesgos para identificar los riesgos de seguridad con precisión y garantizar su mitigación mediante el seguro o protección mediante controles. Para algunas empresas, las directrices de ciber seguro pueden desempeñar un papel en la selección de la tecnología o el ajuste del presupuesto. En cualquier caso, merece una investigación posterior en informes subsecuentes.

Figura 1 ¿Cuáles de las siguientes usan sus organizaciones para determinar o controlar los gastos de seguridad?
Porcentaje de encuestados: N = 3259

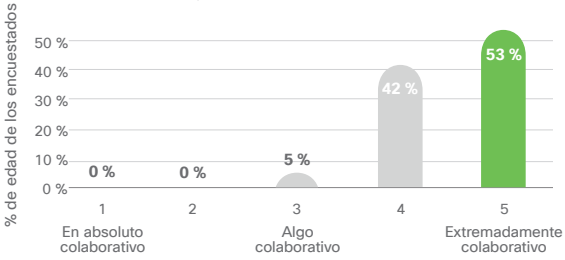


Fuente: Reporte de referencia de CISO de Cisco de 2019

Colaboración, no aislamiento

En encuestas anteriores, nos dijeron que dividen la seguridad por debajo de la TI y que han creado el rol de CISO. Afortunadamente, actúan bien en el campo con sus colegas de redes. La Figura 2 muestra que el 95 % se juzga como muy o extremadamente colaborativo entre los equipos de seguridad y redes. No trabaja aisladamente y tiene un alza financiera tangible.

Figura 2 Los encuestados de diferentes cargos informaron acerca de los niveles de colaboración entre la red y la seguridad en toda la empresa.
Porcentaje de encuestados: N = 3248



Fuente: Reporte de referencia de CISO de Cisco de 2019

¿Cuál es el porcentaje del incentivo financiero? Resulta que **el 59 % de quienes eran muy o extremadamente colaborativos entre la red y la seguridad ha experimentado una repercusión financiera de la vulnerabilidad más impactante de menos de USD 100 000; la categoría más baja de costos de vulnerabilidad.**

Esto claramente merece un análisis adicional y potencialmente requiera una mayor necesidad y posible establecimiento de más equipos de desarrollo, seguridad y operaciones. La colaboración se convierte en una cuestión de deber, no de coincidencia, especialmente en la era del desarrollo ágil.

Y esto se reconoce en los niveles ejecutivos más altos. Según un estudio reciente del director general de información (CIO) publicado por IDG: "El 82 % de los CIO esperan que su estrategia de seguridad y TI se integre estrechamente en los próximos 3 años".*

* Fuente: Una alianza segura: cómo la relación entre los CIO y los CISO fortalece la TI y los negocios, IDG, febrero de 2019

Participación de los empleados: simulacros y ejercicios

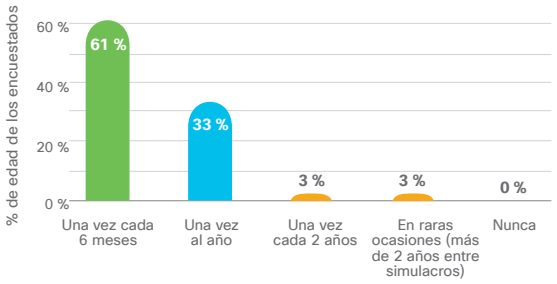
"¿Qué sucede si capacitamos a nuestro personal y se van?", es la pregunta. "¿Qué pasa si no lo hacemos y se quedan?" Lo mismo ocurre desde una perspectiva de seguridad. Sí, nos centramos en la tecnología, pero también deberíamos dedicar el mismo tiempo al proceso y las personas en el lado empresarial, puesto que, nuestra gente es la primera línea de ayuda para proteger a nuestras organizaciones.

Si las personas y los usuarios se citan como el eslabón más débil en la seguridad, contar con un proceso que comience con la incorporación de nuevos empleados tiene sentido común. O por lo menos eso pensarían ustedes: solo el 51 % considera que hace un excelente trabajo de gestión de recursos humanos en seguridad a través de la incorporación integral de empleados y los procesos adecuados para manejar las transferencias y salidas de los empleados. También parece contraproducente que la tendencia de capacitación del personal a raíz de un incidente se haya mantenido estable interanualmente en solo el 39 % de los encuestados.

La ocurrencia de un desastre puede ser peligrosa sin la preparación adecuada. Potencialmente existe un margen de mejora en esta área cuando el 61 % de las organizaciones lleva a cabo un simulacro o ejercicio cada seis meses para probar los planes de respuesta ante incidentes de ciberseguridad (Figura 3). Los simulacros pueden reforzar la capacidad de contar con los controles adecuados vigentes para detectar y responder lo antes posible a fin de mitigar los daños.

"Gran parte de lo que atrapa a las personas cuando sufren una suplantación de identidad (phishing) es una respuesta emocional y eso es lo que hacen los hackers; intentan y provocan una respuesta emocional. Es lo mismo que intentamos y hacemos en nuestras simulaciones de suplantación de identidad con nuestros empleados. Todo se basa en el contexto; cuando un correo electrónico aparentemente indica que hay un paquete esperando, ¿quién no quisiera enviar o recibir un montón de paquetes?"

Figura 3 ¿Con qué frecuencia (si existe) la organización practica un simulacro o ejercicio para probar el plan de respuesta frente a un incidente de ciberseguridad?
Porcentaje de encuestados: N = 3321



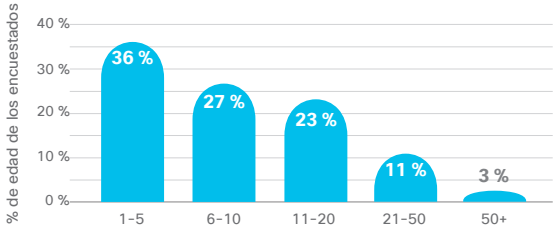
Fuente: Reporte de referencia de CISO de Cisco de 2019

Arquitectura: cómo navegar por el bufete de proveedores

Debido a que ha crecido la necesidad de un enfoque integral de protección contra las ciberamenazas, las organizaciones se precipitaron a adquirir varias soluciones puntuales. Sabemos esto porque, en 2018, el 21 % de los encuestados tenía más de 20 proveedores y el 5 % contaba con más de 50. Este año ha descendido a 14 % y 3%, respectivamente. Hemos encontrando que la tendencia de la cantidad de proveedores y soluciones ha descendiendo; sin embargo, múltiples soluciones de proveedores no están integradas y, por lo tanto, no comparten la clasificación de alertas y la priorización de los paneles limitados. Nuestra encuesta concluyó que incluso aquellos CISO con menos soluciones puntuales podrían gestionar mejor sus alertas a través de un enfoque de arquitectura empresarial.

Para gestionar mejor las alertas, una de las mejores prácticas de seguridad es reducir la cantidad de proveedores y soluciones puntuales. En 2018, el 54 % de los encuestados contaba con 10 o menos proveedores en su entorno, mientras que ahora esta cifra ha aumentado a 63 % (Figura 4). Esto significa que más encuestados tienen menos proveedores; la consolidación de proveedores, por una serie de motivos posibles, es real y cuantificable.

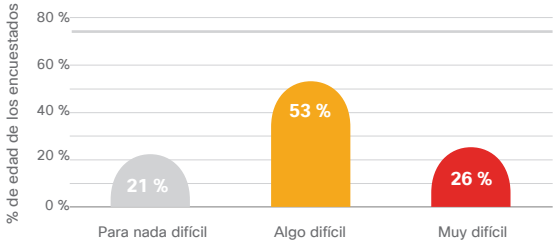
Figura 4 Número de proveedores de seguridad (marcas y fabricantes).
Porcentaje de encuestados: N = 3248



Fuente: Reporte de referencia de CISO de Cisco de 2019

No se fíe solo de nuestra palabra. Este enfoque de múltiples proveedores (en lugar de un enfoque integrado) hace que el reto persistente de alertas continúe: el 79 % de los encuestados dijo que era un poco o muy desafiante organizar las alertas de productos de múltiples proveedores en comparación con el 74 % en 2018 (Figura 5). Por ende, mientras los profesionales de seguridad intentan abordar la dispersión de los proveedores y los problemas de los asistentes, su gestión no se ha vuelto más fácil y necesita más mejoras a fin de optimizar los recursos. Aquí es donde la inteligencia artificial, el aprendizaje automático y el análisis de seguridad pueden ayudar enormemente mediante la automatización de las etapas iniciales de gestión y priorización de alertas. Pero este año, las malas tasas de adopción de estas nuevas tecnologías parecen haberse tambaleado ligeramente.

Figura 5 Gestión de alertas de múltiples proveedores de seguridad.
Porcentaje de encuestados: N = 3248



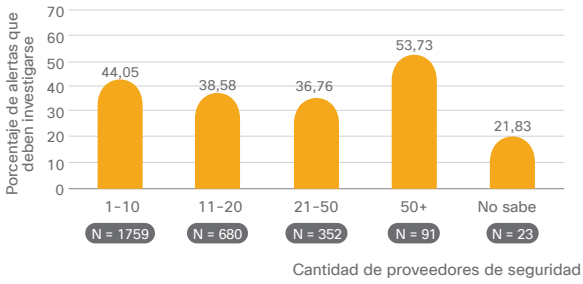
Fuente: Reporte de referencia de CISO de Cisco de 2019

"Si podemos reducir la cantidad de los proveedores y tener una arquitectura más integrada, nos ayudará significativamente. Prefiero tener más automatización en la unidad interna a través de una arquitectura integrada que tener que colocar algo encima y escribir scripts nuevos para combinarlo."

Aunque el tamaño de su organización puede contribuir sin duda a la cantidad de alertas y proveedores, los datos nos indican que menos proveedores pueden hacer que la gestión de alertas sea más eficiente (consulte la Figura 6). En el extremo superior del canal, el 63 % de las organizaciones con solo 1 a 5 proveedores y el 42 % de las organizaciones con 6 a 10 proveedores experimentaron menos de 5000 alertas al día. Por supuesto, esto puede indicar que tienen alertas desactivadas.

Reducir la cantidad de proveedores que se debe administrar ayuda a que los equipos se enfoquen en trabajos más importantes, como la remediación. Las organizaciones con menos de 10 proveedores tuvieron una mayor tasa de respuesta promedio, lo que remedió el 44 % de las alertas legítimas en lugar del 42 %. Se adquiere eficiencia disminuyendo la cantidad de proveedores de seguridad, como se muestra en la Figura 6.

Figura 6 Contraste de la cantidad de alertas que debe investigar el espacio de proveedores de seguridad.
Alertas: N = 2905



Fuente: Reporte de referencia de CISO de Cisco de 2019

Por último, hemos descubierto que el 65 % de las organizaciones que están muy actualizadas y que constantemente se modernizan con las mejores tecnologías disponibles experimentó más a menudo un menor recuento de alertas de seguridad diarias (hasta 10 000 al día). La siguiente mejor opción, reemplazar o actualizar las tecnologías de seguridad de forma periódica (pero no necesariamente estar equipados con las mejores y más recientes herramientas), tuvo un 60 % de probabilidad de recibir hasta 10 000 alertas al día.

"Al final del día, se trata de recopilar toda la información de alertas y aquí es donde establecemos estrategias para analizar la información. Entonces, si empezamos a ver un determinado tipo de evento, esto es lo que activará un incidente para nosotros."

Desafío de la gestión de alertas: no se sabe lo que no se conoce

Hablar de muchas alertas a cualquier persona en seguridad es como hablar del reto del tráfico a cualquier persona en una gran ciudad. Es malo, lo sabemos, sigamos adelante. Sin embargo, generalmente hacemos algo al respecto: compartimos el transporte, evitamos la hora pico, trabajamos desde casa. Las alertas son la clave para lo desconocido y no podemos ignorarlas. En la pila de información hay un 1 % de amenazas que atraviesan incluso los mejores niveles de defensa.

Existen cinco conclusiones relacionadas con el panorama de alertas en relación con nosotros:

1. Ha habido un cambio interanual en los encuestados que ven menos alertas, lo que significa menos alertas para gestionar y, en teoría, facilidad para recibir las alertas importantes. El grupo con el menor volumen de alertas ve 10 000 alertas o menos al día; el 59 % se encuentra en este grupo en comparación con el 50 % de la encuesta del año anterior.
2. ¿Diez mil alertas diarias siguen siendo mucho? Sin duda, pero cuando tenemos en cuenta que el 41 % ve más de 10 000 alertas y que algunos afirman ver más de 500 000 alertas (aunque sea solo el 1 %), la cifra de 10 000 al menos se mueve en el sentido correcto.
3. Se terminaron las buenas noticias. Se responde al 50,7 % de las alertas en comparación con el 55,6 % en 2018. Esto sugiere que, mientras que algunos ven menos alertas, lo que debería facilitar el trabajo, muchos realmente responden a menos alertas.

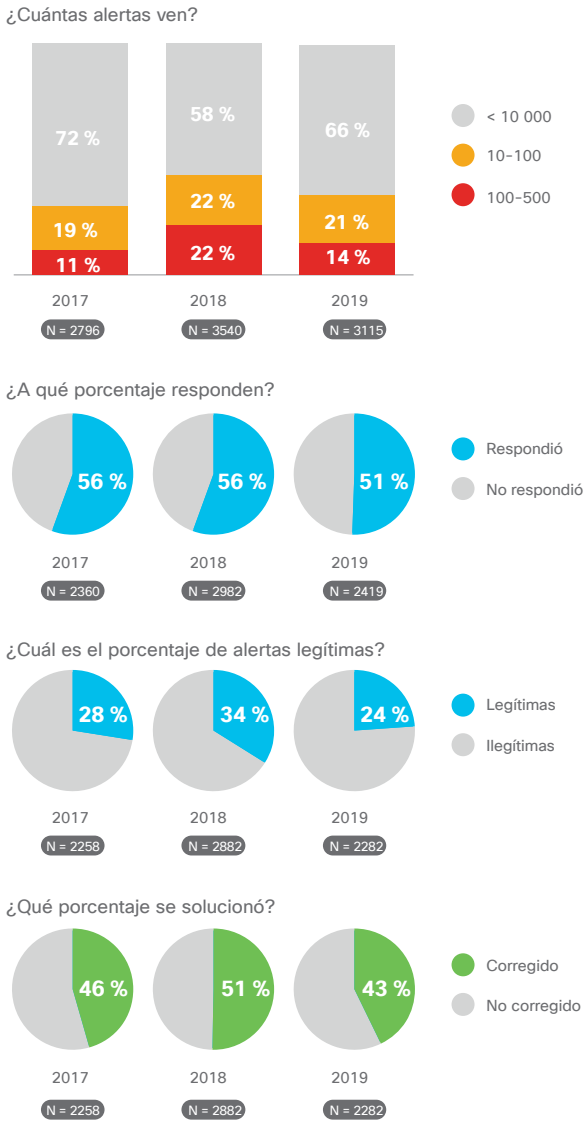
4. Solo el 24,1 % de las alertas investigadas resultaron ser legítimas en comparación con el 34 % en 2018. Esto demuestra que la precisión de las herramientas usadas para determinar qué alertas deben investigarse no funciona bien.
5. Existen noticias aún peores cuando analizamos la remediación de las alertas: hay un descenso drástico de la encuesta de 2018 en el número de alertas legítimas remediadas: del 50,5 % al 42,8 % este año.

Dicho de otro modo e ilustrado en la Figura 7: si pertenecen a una de las organizaciones que enfrentan un máximo de 10 000 alertas por día, solo quedan 1 000 alertas legítimas desatendidas todos los días. Y esto es solo la mitad (50,7 %) de las investigadas. El caso nunca ha sido más fuerte para que las herramientas de respuesta ante amenazas de seguridad puedan introducir amplios conjuntos de datos, visualizar los datos masivos y proporcionar un medio para actuar rápidamente.

Gestión de la medición

Esta caída en la remediación es crucial, dado que muchos avanzan hacia la remediación como un indicador clave de la eficacia en materia de seguridad. La cantidad de encuestados que emplean un tiempo de detección medio como métrica disminuyó del 61 % (2018) al 51 % (2019) en promedio. El enfoque del tiempo de reparación también cayó del 57 % (2018) al 40 % (2019). El mayor cambio se dio en los encuestados que se centran en el ***tiempo de remediación*** (48%) como indicador, que aumentó respecto del 30 % en 2018. Esto muestra un nuevo enfoque sobre la remediación como KPI del profesional de seguridad para medir el estado de la seguridad. *Cuando se contrasta con el aumento en el número de alertas legítimas no remediadas, la disminución en la inversión en aprendizaje automático y el lento aumento o la tasa constante en la cantidad de capacitaciones, parece que nos encontramos ante la necesidad de más innovación en la gestión de alertas.*

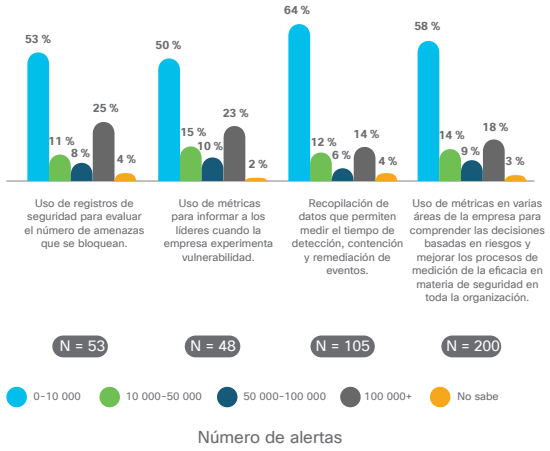
Figura 7 Comparación de resultados de la encuesta respecto de la cantidad de alertas detectadas, el porcentaje de respuesta, el porcentaje de respuesta de alertas legítimas y el porcentaje de incidentes remediados.



Fuente: Reporte de referencia de CISO de Cisco de 2019

Los datos de la encuesta además revelaron que el 64 % de quienes recopilan datos que permiten medir el tiempo de detección observó 10 000 o menos alertas diarias; el grupo más alto en esta matriz (consulte la Figura 8).

Figura 8 ¿Cómo miden las empresas la eficacia en materia de seguridad en comparación con el número de alertas?
Porcentaje de encuestados: N = 3259



Fuente: Reporte de referencia de CISO de Cisco de 2019

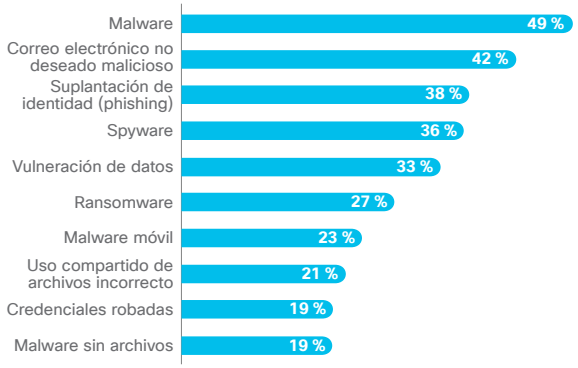
Preparación y respuesta frente a las vulnerabilidades: cuando llama lo desconocido

Ataques de los últimos años

Por primera vez este año, preguntamos específicamente acerca de los tipos de ataques que experimentaron los CISO y la lista de ataques comunes. Si bien algunos han visto variantes muy específicas de malware, como WannaCry (11 %), o categorías de amenazas, como el malware limpiador (15 %), los ataques más citados son el malware y sus variantes, por ejemplo, el ransomware.

"Hoy en día el 90 % de nuestros incidentes todavía se relaciona con el malware, o la evolución del malware, como el ransomware y ataques similares. Y aún no sabemos con certeza cuál es el vector amenazante de estas amenazas persistentes y avanzadas."

Figura 9 ¿Qué tipos de incidentes/ataques de seguridad han encontrado en el último año?
Porcentaje de encuestados: N = 2909



Fuente: Reporte de referencia de CISO de Cisco de 2019

Como se muestra en la Figura 9, dos de los tres tipos principales son problemas con la seguridad del correo electrónico; el vector de amenazas #1. Independientemente de si invierten en protección, cambian a Microsoft Office 365 o tratan de protegerse mejor contra las vulnerabilidades del correo electrónico empresarial (BEC) con DMARC, el correo electrónico sigue siendo un área de enfoque. Que 2 de los primeros 10 tipos sean problemas de amenazas internas (uso compartido de archivos y credenciales robadas) muestra que debe observarse qué sucede dentro y fuera de la empresa, teniendo en cuenta que algunos delincuentes pueden iniciar sesión en lugar de irrumpir. Esto impulsa la necesidad de una mejor autenticación de varios factos (MFA). En ningún ámbito se hace más patente esta necesidad de equilibrio en la seguridad (contratación de personas adecuadas) que en el

respaldo de operaciones empresariales perfectas (no se deben perjudicar las personas contratadas con una experiencia de autenticación de usuario anticuada).

Y así como la preocupación respecto de otras áreas sigue siendo alta pero manejable (como el traspaso a la nube), la preocupación por el comportamiento de los usuarios (si hacen clic en enlaces maliciosos en el correo electrónico o en sitios web) sigue siendo alta y ahora es la principal preocupación de los CISO. Al preguntarles sobre el reto de la defensa en varias partes de la infraestructura, la mayor preocupación fue el comportamiento de los usuarios. Esta percepción de la vulnerabilidad se ha mantenido estable durante los últimos tres años entre el 56 % y el 57 % de los encuestados.

También preguntamos cuáles de estos tipos de ataques dio lugar a cierto nivel de vulnerabilidad (pérdida de datos) y obtuvimos la siguiente prioridad de respuestas:

1. Malware (20 %)
2. Vulneración de datos (19 %)
3. Spyware (14 %)
4. Suplantación de identidad (13 %)
5. Ransomware (13 %)
6. Correo electrónico no deseado malicioso (13 %)

Curiosamente, las percepciones de riesgo variaron entre los roles relacionadas con la seguridad. Por ejemplo, los responsables de cumplimiento y riesgo consideraron que la vulnerabilidad más importante son los "ataques dirigidos"; estos ejecutivos son conscientes de las calamitosas consecuencias que un ataque fatal podría tener en la continuidad del negocio.

Para obtener más información sobre lo que las vulnerabilidades ponen en peligro en la estabilidad organizativa, lea el Informe de amenazas de Cisco de 2019.

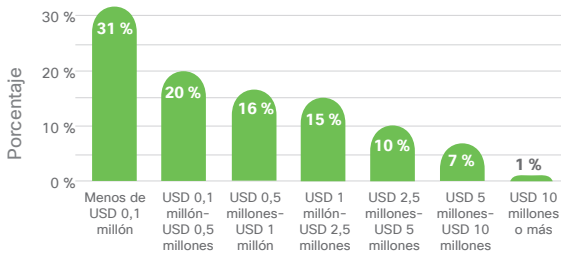
Costo de una vulnerabilidad: algo más que dinero

Todos somos conscientes de las posibles consecuencias de una vulnerabilidad: pérdidas financieras (vea la Figura 10), retroceso o ruina de la marca y reputación, pérdida de confianza de los accionistas, pérdida de datos valiosos, sanciones por incumplimiento reglamentario, etc. Si observamos la comparación interanual de los datos, hay un claro giro hacia los problemas de percepción y opinión; no hubo modificaciones en la necesidad de mantener las operaciones en funcionamiento, pero la experiencia del cliente y la reputación de la marca surgieron como preocupaciones clave (Tabla 1).

Tabla 1 Principales inquietudes debidas a vulnerabilidades.

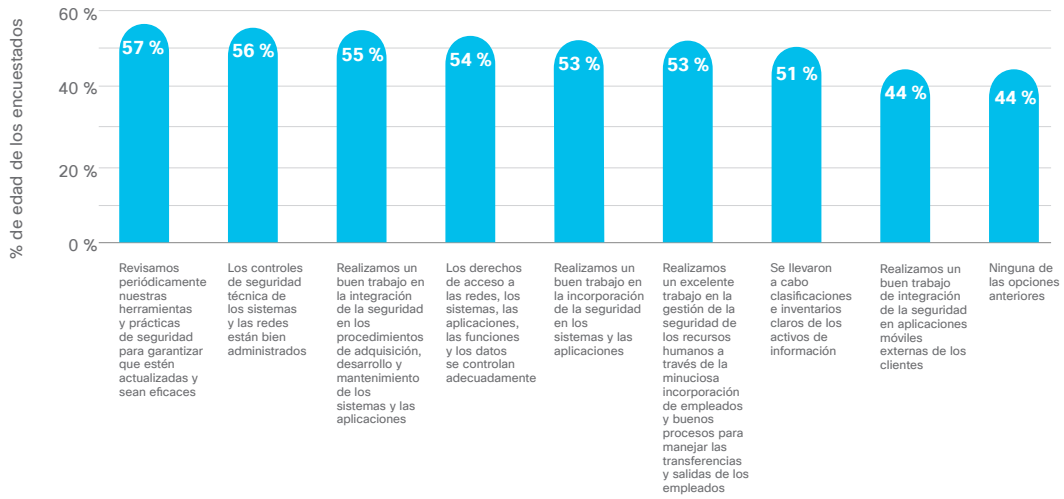
Inquietudes debidas a vulnerabilidades	Afirmó: 2018	Afirma: 2019	
Operaciones	38 %	36 %	Un cambio marginal descendente en la preocupación operativa se ve ensombrecido por las preocupaciones dirigidas al cliente.
Conservación de clientes	26 %	33 %	La continuación de opiniones negativas en torno a las vulnerabilidades de datos y la prevalencia del malware, como el ransomware, hacen que los consumidores sean cautelosos.
Reputación de la marca	27 %	32 %	Los nombres familiares se convierten en sinónimos de un gran ataque durante años; no mencionamos ninguno aquí, pero los clientes pronto confeccionarán una lista.

Figura 10 Pensando en la vulnerabilidad más impactante que sus organizaciones experimentaron en el último año, ¿cuál fue la repercusión financiera?
Porcentaje de encuestados: N = 2386



Fuente: Reporte de referencia de CISO de Cisco de 2019

Figura 11 ¿Qué prácticas se emplean para salvaguardar la organización?
Porcentaje de encuestados: N = 3223



Fuente: Reporte de referencia de CISO de Cisco de 2019

Cómo afrontar la amenaza de una vulnerabilidad

Les preguntamos a nuestros profesionales de seguridad hasta qué punto sus organizaciones adoptaron medidas para tener empleados, procesos y productos vigentes a fin de protegerse. Los resultados se muestran en la Figura 11.

Además, les preguntamos qué enfoques adoptan para mitigar los riesgos de seguridad. Los resultados se muestran en la Figura 12.

Y entre más datos, descubrimos que, si bien el 85 % de los encuestados tenía conocimientos sobre las políticas y prácticas de protección y seguridad de la infraestructura, solo el 74 % tenía información acerca de la continuidad de los negocios y la recuperación tras un desastre. Solo el 75 % de los encuestados tenía conocimientos de la respuesta ante incidentes. Esto es un problema. El 100 % de las personas que participan en la seguridad debe conocer la respuesta ante incidentes; de hecho, esto se puede ampliar a todos los empleados de la organización. Aquí es donde la capacitación es tan vital, pero su falta de protagonismo en los resultados de este año sigue destacándose.

Figura 12 Estados de seguridad: planteamientos para mitigar los riesgos de seguridad.
Porcentaje de encuestados: N = 3248

Fuente: Reporte de referencia de CISO de Cisco de 2019

Cómo lidiar con lo desconocido

El puente entre la detección de amenazas desconocidas y la adopción de medidas respecto de las adecuadas radica en el estado de seguridad eficaz. Estas son recomendaciones prácticas que hemos ideado en función de nuestros resultados de la encuesta para que tengan en cuenta:

- Basen la elaboración de presupuestos de seguridad en resultados de medición de la seguridad con estrategias prácticas acopladas a evaluaciones de seguros y riesgos cibernéticos a fin de guiar sus decisiones de adquisición, estrategia y gestión.
- La única forma de entender las necesidades de seguridad subyacentes de un caso de negocio es colaborar a través de los silos entre los grupos de TI, redes, seguridad y cumplimiento.
- Hay procesos comprobados que las organizaciones pueden emplear para reducir su exposición y el alcance de las vulnerabilidades. Preparen simulacros, empleen métodos de investigación rigurosos y conozcan los métodos más oportunos de recuperación.
- El aprendizaje automático, la inteligencia artificial y la automatización aumentan los esfuerzos de seguridad exponencialmente y el próximo año veremos más encuestados en la fase de implementación y práctica "completamente dependientes". Cisco emplea la tecnología de aprendizaje automático en distintos productos de seguridad, como Advanced Malware Protection, Umbrella, Stealthwatch y Cisco Threat Response.
- Construya un centro de operaciones de seguridad (SOC) para gestionar la respuesta ante vulnerabilidades en las organizaciones de todos los tamaños.
- La seguridad en la nube puede ayudar con lo desconocido. El 91 % está de acuerdo en que el uso de la seguridad en la nube incrementa la visibilidad de la red. Cisco Umbrella es la seguridad en la nube que bloquea a los usuarios para que no se conecten a IP, URL y dominios maliciosos conocidos y sospechosos, tanto si están dentro como fuera de la red empresarial.
- Proteja los centros de datos y los ecosistemas de nubes múltiples con soluciones integradas, como la solución Cisco Secure Data Center que ofrece visibilidad, segmentación y detección de amenazas de Tetration, Stealthwatch y NGFW.
- Aborde el vector de amenazas número uno con la protección contra suplantación de identidad, filtrado de correo electrónico no deseado avanzado y vulnerabilidades del correo electrónico empresarial con DMARC; consulte Cisco Email Security.
- La seguridad para terminales ayuda a hacer frente a amenazas desconocidas en dispositivos de usuarios; pruebe Cisco Advanced Malware Protection para terminales, también disponible en nuestra web, correo electrónico, nube y soluciones de seguridad de la red, para crear un entorno de productos que trabajen juntos para una protección contra amenazas más eficaz y eficiente.
- Obtenga la detección rápida de amenazas, acceso sumamente seguro y la segmentación definida por software con la segmentación y visibilidad de red de Cisco que combina Cisco Stealthwatch Enterprise, Cisco Identity Services Engine y la tecnología Cisco TrustSec.
- El acceso de confianza es un componente crítico de la seguridad. Duo verifica si un usuario es confiable (confirma si un usuario es quien dice ser) con la mejor solución de autenticación multifactor (MFA) adaptable.

"Por momentos, averiguar cómo mantenerse al frente de los hackers maliciosos puede parecer una carrera armamentista, pero la manera en la que veo lo que sucederá, es que hay que seguir por donde vaya el negocio en términos de nuevas técnicas y tecnologías. Allí es donde se verán las brechas."

"A veces los CISO han utilizado el miedo para impulsar algunas de las inversiones del presupuesto. Lo que preferimos mirar es: ¿cuál es el riesgo para la empresa? Hay muchos niveles de riesgo aceptable, por lo que nos centramos en el sitio donde se encuentra el mayor riesgo para la empresa. Somos muy afortunados de que Cisco tome la seguridad muy en serio e invierta en la arquitectura fundamental para prepararnos mejor."

Marisa Chancellor
Directora Senior, Organización de Seguridad y Confianza, Cisco

Acerca de la encuesta de parámetros de Cisco

El estudio doble ciego, llevado a cabo por un socio de investigación independiente, cubre muchos sectores que incluyen el sector minorista, el transporte, la fabricación, los servicios financieros, el gobierno y la educación superior. Los participantes son empleados a tiempo completo que trabajan en empresas medianas (250 – 999 empleados), grandes (1 000 – 9 999 empleados) y corporaciones (más de 10 000 empleados).

Los encuestados cumplen una variedad de funciones que incluyen directores generales de seguridad de la información (CISO), directores generales de información (CIO) y otros cargos ejecutivos. Están bien informados sobre los procedimientos y las políticas de seguridad e implicados en la configuración de estrategias de seguridad. La mayoría tiene títulos de CISO, director/gerente de TI o CTO y el 99 % de los encuestados tiene un equipo en su organización dedicado a la ciberseguridad.

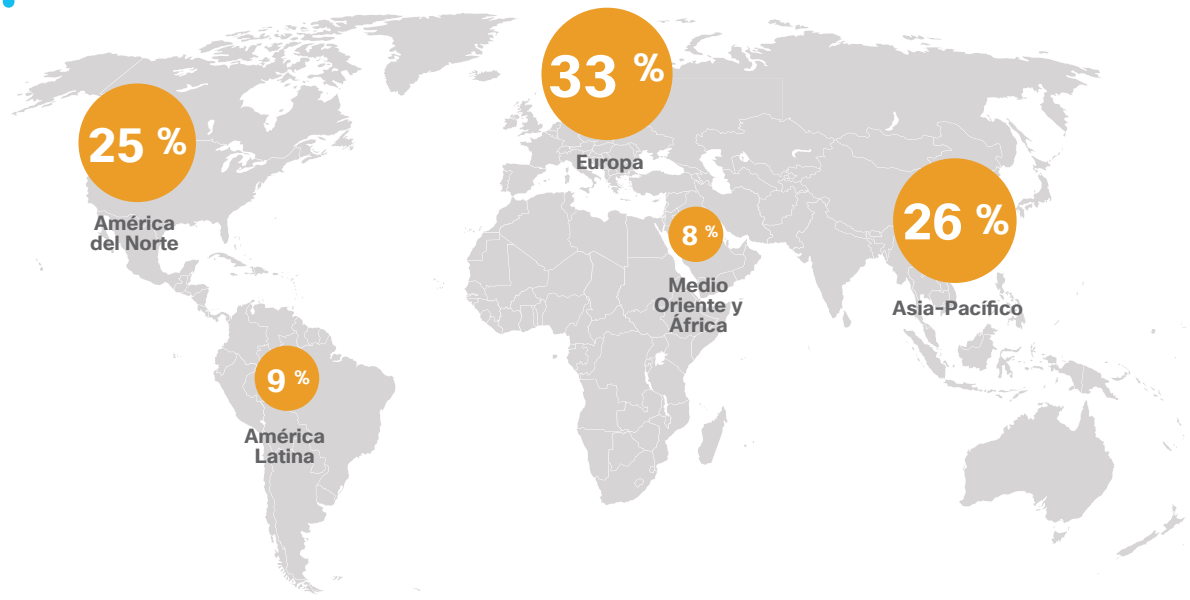
Los encuestados proceden de todos los continentes y 18 países, entre ellos, Estados Unidos, Canadá, Reino Unido, Francia, Alemania, Australia, Japón y China (Figura 13).

Encuestados calificados

Se utilizaron los siguientes criterios para calificar a los encuestados:

- Adultos (25 años o más) que superen las pruebas de empleo confidenciales/competitivas.
- Empleados a tiempo completo de una empresa con fines de lucro, gobierno o centro de educación superior con más de 250 empleados a tiempo completo y un departamento de TI formal.
- Participantes de la seguridad de TI más allá de la aprobación de presupuestos.
- Conocedores de las prácticas y políticas de seguridad.

Figura 13 Distribución de los encuestados por región redondeada al porcentaje más cercano.
Porcentaje de encuestados: N = 3259



Fuente: Reporte de referencia de CISO de Cisco de 2019

Serie de ciberseguridad de Cisco

A lo largo de la última década, Cisco ha publicado una gran cantidad de información crucial de seguridad e inteligencia de amenazas para profesionales de seguridad interesados en el estado de la ciberseguridad global. Estos informes exhaustivos proporcionan explicaciones detalladas de los panoramas de amenazas y las consecuencias para las organizaciones, así como mejores prácticas para defenderse frente a los efectos adversos de vulneraciones de datos.

En nuestro nuevo enfoque de liderazgo intelectual, la seguridad de Cisco realiza una serie de publicaciones basadas en investigaciones e impulsadas por datos bajo el banner Serie de ciberseguridad de Cisco. Hemos ampliado el número de títulos para incluir diversos informes para profesionales de seguridad con intereses diferentes. Invocando la amplitud y profundidad de conocimientos de los investigadores de amenazas e innovadores en el sector de seguridad, la recopilación de informes de la serie 2019 incluye el Reporte de referencia de privacidad de datos, el Reporte de amenazas, y el Reporte de referencia de CISO; y vendrán otros a lo largo del año.

Para más información y para acceder a todos los informes y las copias archivadas, visite www.cisco.com/mx/securityreports.

Sede central en América
Cisco Systems, Inc.
San José, CA

Sede central en Asia-Pacífico
Cisco Systems (USA), Pte. Ltd.
Singapur

Sede central en Europa
Cisco Systems International BV Ámsterdam,
Países Bajos

Cisco tiene más de 200 oficinas en todo el mundo. Las direcciones y los números de teléfono y fax están disponibles en el sitio web de Cisco en www.cisco.com/go/offices.

Publicado en marzo de 2019 CISO_01_0319_r1