Serie de informes sobre ciberseguridad de Cisco de 2020

Estudio comparativo sobre CISO

cisco Seguridad

Protección para el presente y el futuro

20 consideraciones de ciberseguridad para 2020

Incluye contenido exclusivo para España

Consulte la página 23

Índice

Introducción

A la vez que respaldan el crecimiento empresarial y la transformación digital, los líderes en seguridad se enfrentan a una multitud de desafíos. Lo sabemos porque nos lo ha dicho usted, en conversaciones corrientes además de como parte de nuestra encuesta comparativa anual. Algunos desafíos se centran en la seguridad, como la necesidad de una mejora de la visibilidad o automatización, o en el esfuerzo por conseguir una mayor simplicidad de la administración y respuesta. Algunos están relacionados con el éxito de su negocio, como el deseo de respaldar el crecimiento y la transformación, independientemente de qué aplicación en la nube se necesite o qué dispositivo móvil se esté utilizando. Otros desafíos se relacionan con inversiones actuales que sigan siendo relevantes en el futuro a medida que su organización cambie.

Y todo ello se suma a las demandas cotidianas del trabajo diario, como la detección y el bloqueo de amenazas avanzadas. Resulta difícil gestionar al mismo tiempo los agentes de amenazas sofisticados y la superficie de ataque en constante expansión. Los desafíos a los que se enfrenta van más allá de sacar mayor partido de un presupuesto limitado: abarcan el mantenimiento de la reputación de la marca, la confianza de la junta directiva y los accionistas y la contratación de personal experto para coordinar las tácticas, las técnicas y los procedimientos (TTP) ante un ciberataque, por nombrar algunos.

Tiene que ofrecer a los usuarios el acceso que necesitan, al tiempo que se enfrenta a estos desafíos de seguridad, complejidad y presupuesto. También ha de reducir la sobrecarga de tecnología, evitar brechas importantes, buscar las amenazas antes de que se infiltren en la red y exfiltren sus datos, gastar el presupuesto de seguridad de una manera más inteligente y convencer a más clientes.

Según el Foro Económico Mundial, los ciberataques se perciben como el segundo mayor riesgo global para los líderes empresariales de las economías avanzadas, solo superado por las crisis fiscales.[1]

Al realizar nuestra sexta encuesta anual a 2800 responsables de la toma de decisiones de TI de 13 países, hemos continuado nuestra tradición anual de profundizar en su mundo para recopilar estadísticas de referencia clave.[2] También hemos hablado largo y tendido con un grupo de CISO para analizar los resultados y elaborar una lista de 20 consideraciones para 2020. Este informe proporciona datos y puntos clave valiosos que puede compartir con otros miembros de su equipo directivo o de su junta directiva, para realizar recomendaciones concretas de cara a mejorar la postura relativa a la seguridad de su organización.
En España, hemos encuestado a una muestra de 200 especialistas en ciberseguridad de un total de 200 empresas.

Puesto que sabemos que no hay nada seguro excepto la incertidumbre de este sector, hemos diseñado las secciones de este informe como preguntas que podría estar haciéndose a medida que se prepara para el año que viene. Si estas cuestiones le repercuten, o si le generan preguntas en otros aspectos, nos encantaría que nos enviara su opinión a security-reports@cisco.external.com. Mientras tanto, esperamos que el informe le ayude a superar los desafíos de seguridad de este año.

Para ver todos los informes de nuestra serie de informes sobre ciberseguridad, vaya a: cisco.com/go/securityreports.

---

[1] "Esto es lo que los directores generales de todo el mundo consideran los mayores riesgos para la empresa", Foro Económico Mundial, 2019

[2] Los países encuestados son Alemania, Australia, Brasil, Canadá, China, España, Estados Unidos, Francia, India, Italia, Japón, México y Reino Unido.

20 consideraciones de ciberseguridad para 2020

1. ¿Quién ofrece soporte ejecutivo y un enfoque claro en su organización?

A lo largo de los años, en nuestra encuesta, hemos evaluado cuatro prácticas clave para fomentar una relación mutuamente ventajosa entre los ejecutivos y la organización de seguridad. Este ejercicio evalúa el apoyo descendente en relación con la seguridad, donde hemos encontrado una ligera tendencia a la baja con respecto al año pasado. Si analizamos estos resultados:

- El 89 % de los encuestados afirmó que su **dirección ejecutiva sigue considerando la seguridad una prioridad máxima;** sin embargo, este porcentaje ha disminuido ligeramente (un 7 %) durante los cuatro años anteriores. En España, el porcentaje es de un 79%, una disminución del 16% con respecto al año anterior. De este tema se ocupa de hecho el capítulo 21.
- El porcentaje de organizaciones que han **aclarado las funciones y responsabilidades relativas a la seguridad dentro del equipo ejecutivo** ha fluctuado en los últimos años y ha alcanzado el 89 % este año, 81% en el caso de España. Teniendo en cuenta la creciente visibilidad de la ciberseguridad y la extrema necesidad de líderes en seguridad en los niveles superiores, aclarar las funciones y responsabilidades ha de seguir siendo una prioridad.
- La incorporación de evaluaciones de riesgos cibernéticos en los procesos generales de evaluación de riesgos ha descendido un 5 % con respecto al año pasado, pero sigue siendo alta, con un 91 % de los encuestados que dicen que las utilizan. Mientras que en España es del 80%.
- Aunque haya descendido un 6 % con respecto al año pasado, el porcentaje de equipos ejecutivos que definen métricas claras para la evaluación de la eficacia de los programas de seguridad sigue siendo bastante alta, ya que el 90 % de nuestros encuestados lo hacen.

A lo largo de cuatro años, estas respuestas han descendido ligeramente, lo que puede indicar: 1) que el alcance de la responsabilidad en seguridad está cambiando, 2) que la comunicación con el equipo ejecutivo no es tan clara como antes, 3) que la dirección ejecutiva tiene otras prioridades empresariales, o 4) que los CISO y ejecutivos están reevaluando las métricas.

Aunque estos porcentajes han descendido, siguen siendo muy altos. Tal vez esto se deba a que la seguridad se ha operativizado, aunque requiere una mayor presencia en la mesa ejecutiva. **El hecho de que los porcentajes sigan siendo muy altos indica una relación sólida y continuada entre los ejecutivos y los profesionales de la seguridad.**

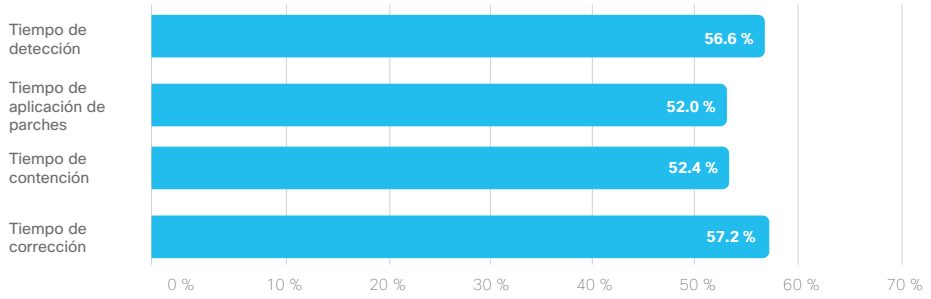
> Cada organización es diferente en términos de la composición ejecutiva y hay muchos estilos diferentes de liderazgo ejecutivo. La función de un CISO es mantener conversaciones y comprometerse con la empresa demostrando que una seguridad bien diseñada aportará valor a la misma.
>
> Mick Jenkins MBE, CISO de la Brunel University de Londres

2. ¿Cómo puede decidir qué métricas son las más importantes?

Como acabamos de señalar, un 90% mundialmente y solo un 80% en España, estaba de acuerdo en que los ejecutivos de su organización habían definido métricas claras para la evaluación de la eficacia de su programa de seguridad. La definición de métricas claras es una actividad fundamental en un marco de seguridad y no es tarea fácil que exista acuerdo entre varios ejecutivos y equipos de seguridad en cómo evaluar la mejora operativa y los resultados de seguridad. En el capítulo 21 abordamos las métricas usadas en España.

Los responsables de toma de decisiones de TI que han respondido a nuestra encuesta han puntuado **más alto el tiempo de detección como un indicador de rendimiento clave (KPI). Sin embargo, al rendir cuentas al equipo directivo o a la junta directiva, el tiempo de corrección es igual de importante,** ya que representa una suma de la repercusión total, que puede incluir: el tiempo de inactividad del sistema, los registros afectados, el coste de investigación, la pérdida de ingresos, la pérdida de clientes, la pérdida de oportunidades y los gastos extra (Figura 1). También puede ser una métrica representativa de la eficacia general de la organización de TI, ya que la corrección puede requerir mucho trabajo colaborativo entre departamentos.

Figura 1: Métricas utilizadas para informar internamente de una brecha de gran repercusión al equipo directivo o la junta directiva (N=2800). Los porcentajes se han redondeado.

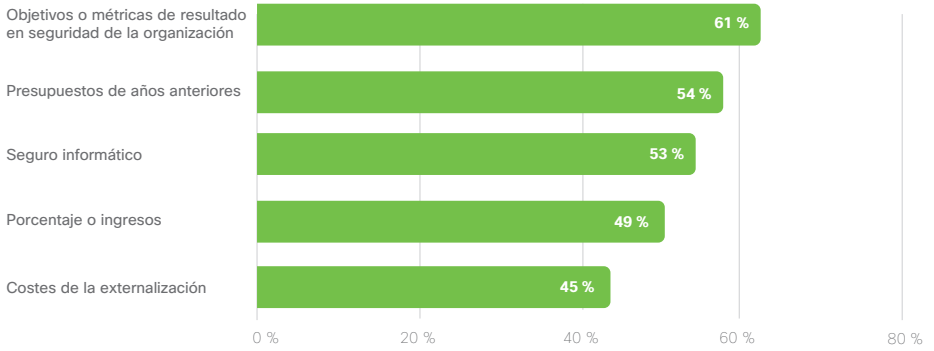


Fuente: Encuesta comparativa de CISO de 2020 de Cisco

3. ¿Cuáles son las consideraciones principales que impulsan el gasto con un presupuesto limitado?

Casi siempre hemos escuchado opiniones sobre que la mejor manera de asignar el gasto en seguridad es a través de objetivos y métricas basados en los resultados. El 61 % utiliza este método de planificación, lo que supone un aumento del 10 % con respecto al año anterior y una tendencia alentadora (Figura 2).

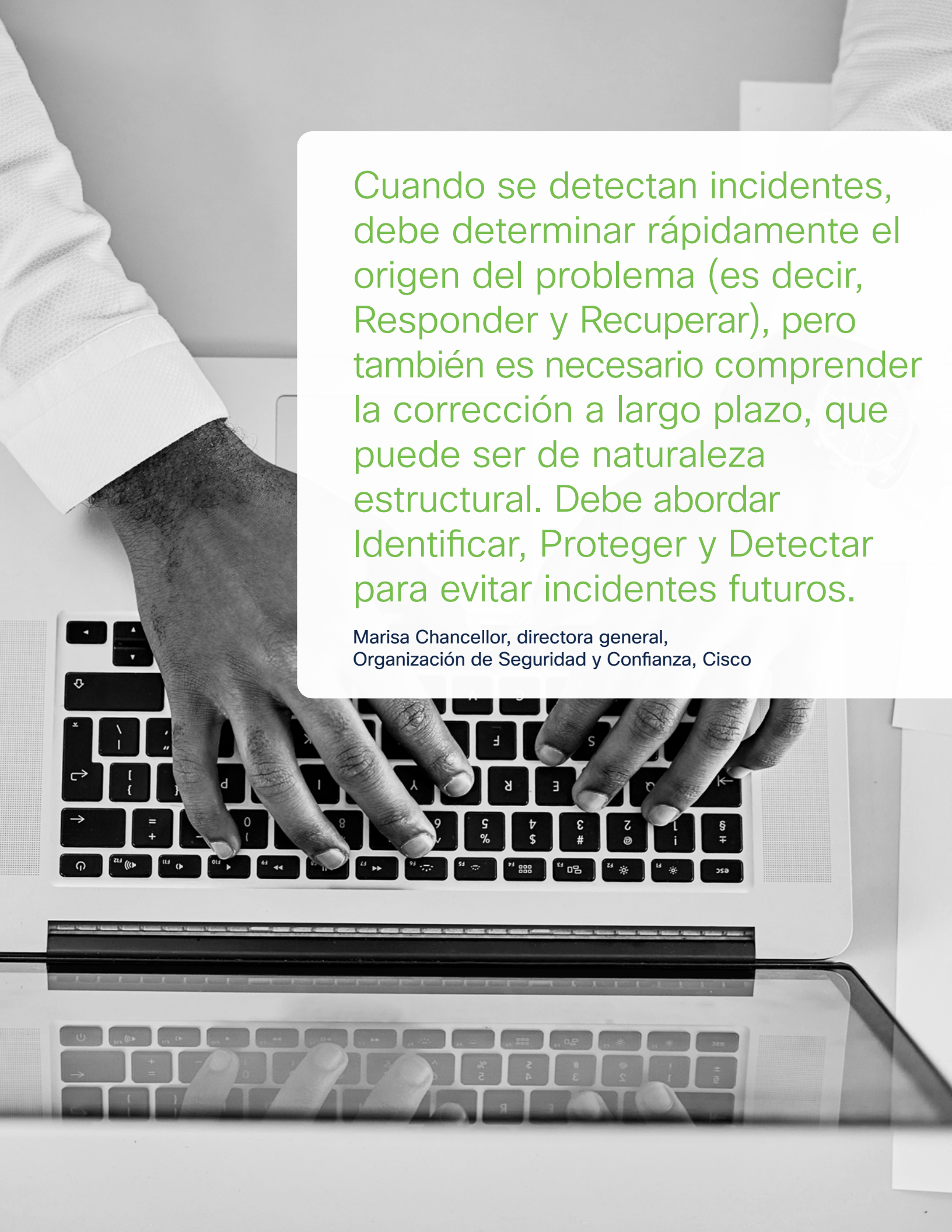
Figura 2: Qué utilizan las organizaciones para determinar o controlar el gasto en seguridad (N=2799). Los porcentajes se han redondeado.



Fuente: Encuesta comparativa de CISO de 2020 de Cisco

" Porcentaje de ingresos" y " Costes de la externalización" fueron los factores menos utilizados para determinar los presupuestos de seguridad. El 54 % del gasto base en el presupuesto de años anteriores. Aunque puede no parecer una manera precisa de cuantificar el gasto en seguridad, en especial cuando el coste medio de una brecha de datos a nivel global (3,92 millones de USD) rara vez se tiene en cuenta, si su presupuesto es el mismo año tras año o cuenta con suscripciones SaaS predecibles, es probable que el presupuesto que haya previsto varíe muy poco.[3]

[3] Informe de coste de una brecha de 2019, Ponemon Institute



Cuando se detectan incidentes, debe determinar rápidamente el origen del problema (es decir, Responder y Recuperar), pero también es necesario comprender la corrección a largo plazo, que puede ser de naturaleza estructural. Debe abordar Identificar, Proteger y Detectar para evitar incidentes futuros.

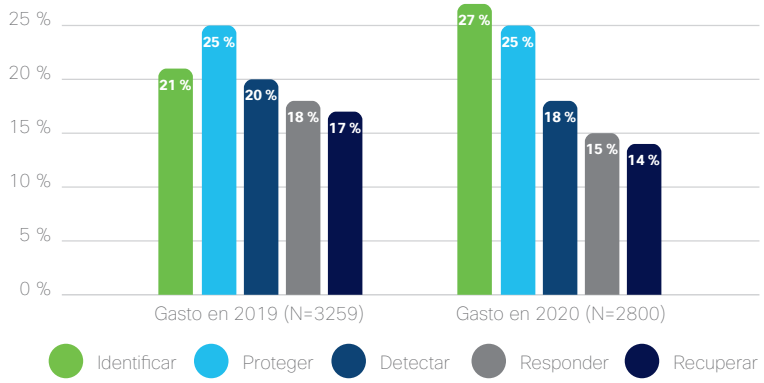
Marisa Chancellor, directora general,
Organización de Seguridad y Confianza, Cisco

4. ¿Cuál es el equilibrio adecuado del gasto en verificación de confianza y detección de amenazas?

Al analizar en qué se gasta el presupuesto de seguridad, hemos preguntado a nuestros encuestados en relación con cinco categorías (Identificar, Proteger, Detectar, Responder y Recuperar) que describen el ciclo de vida de la defensa de la ciberseguridad y la gestión de las brechas:

- **La categoría Identificar** registró un aumento de los gastos del 21 % al 27 % de 2019 a 2020
- **Proteger y Detectar** se mantuvieron básicamente en el mismo nivel, en un 25 % y un 18 % respectivamente
- **El gasto en las categorías Responder y Recuperar** disminuyó un poco en el mismo período de tiempo a un 15 % y un 14 % respectivamente

Figura 3: Gasto en seguridad por categoría del ciclo de vida. Los porcentajes se han redondeado.



Fuente: Encuesta comparativa de CISO de 2020 de Cisco

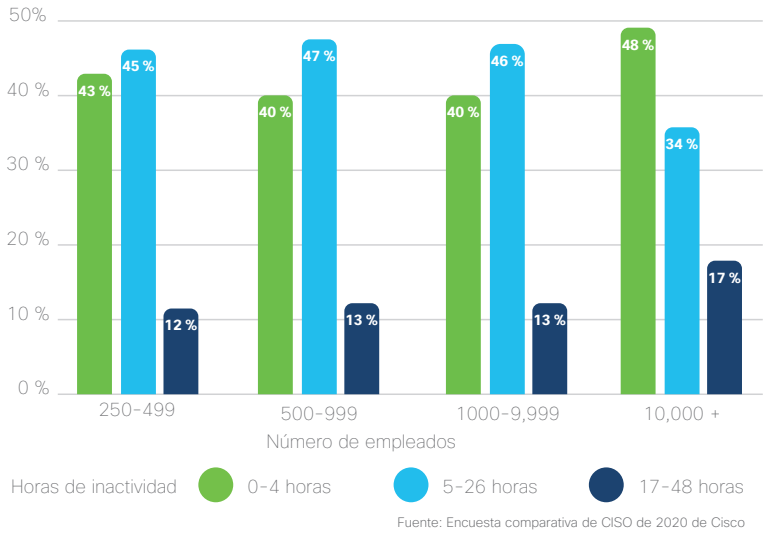
Esta tendencia muestra que **las organizaciones están gastando más en prevención que en ser reactivas** en su postura con respecto a la ciberseguridad. Las empresas siempre tratan de encontrar el equilibrio adecuado entre la proactividad y la capacidad de respuesta y resistencia, una balanza que se inclina de un sentido al otro cada año. El año pasado, las organizaciones pueden haber concentrado sus esfuerzos en los aspectos básicos (inventario de recursos, detección, etc.). Y, en teoría, si se gasta lo correcto en Identificar, Proteger y Detectar por adelantado, no se tendría que gastar tanto en Responder y Recuperar, ya que no son aspectos que se necesiten tan a menudo.

5. ¿Qué información le aporta la evaluación de la repercusión de las brechas de seguridad en su empresa?

En nuestra encuesta, hemos preguntado acerca de varios efectos de las brechas, incluidos el tiempo de inactividad, los registros y las finanzas.

¿En qué medida tienen que resistir las organizaciones el tiempo de inactividad debido a brechas importantes? Hemos comparado los diferentes tamaños de las organizaciones y los resultados han sido muy similares en todos los niveles. Las grandes empresas (10 000 empleados o más) tienen más probabilidades de sufrir un menor tiempo de inactividad (0-4 horas), ya que probablemente dispongan de más recursos para responder y recuperarse. Las organizaciones pequeñas y medianas han dominado el intervalo de tiempo de recuperación de 5-16 horas y los tiempos de inactividad catastróficos de 17-48 horas han sido igualmente bajos para las organizaciones de todos los tamaños (Figura 4).

Figura 4: En el caso de la brecha de seguridad más grave gestionada el año pasado, el número de horas durante las que los sistemas estuvieron inactivos correlacionaba con el tamaño de la organización (N=2265). Los porcentajes se han redondeado.

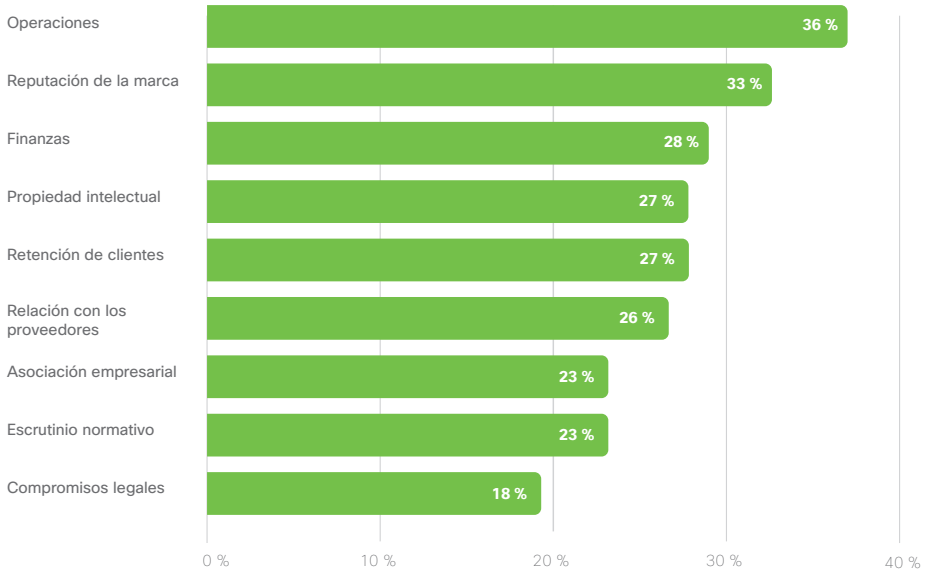


Fuente: Encuesta comparativa de CISO de 2020 de Cisco

Las organizaciones con más de 100 000 registros afectados por la brecha más grave han aumentado del 15 % el año pasado a más del 19 % este año.

Además, como muestra la Figura 5, una brecha importante puede afectar a nueve áreas clave de una organización. **Las áreas de negocio más afectadas han sido las operaciones y la reputación de la marca,** seguidas de las finanzas, la propiedad intelectual y la retención de clientes.

Figura 5: Porcentajes de encuestados que afirman que las áreas de negocio se han visto afectadas negativamente debido a una brecha. (N=2121). Los porcentajes se han redondeado.



Fuente: Encuesta comparativa de CISO de 2020 de Cisco

En años anteriores, observamos que el número de encuestados cuya **reputación de marca se ha visto afectada debido a brechas importantes ha aumentado del 26 % al 33 % en tres años**. El porcentaje de quienes han visto cómo sus operaciones se han visto afectadas se ha mantenido estable entre el 36-38 % de los encuestados. Y el porcentaje de quienes han visto cómo sus finanzas se han visto afectadas ha disminuido solo un punto porcentual por año durante los últimos tres años, por lo que también se mantiene relativamente estable. Puesto que la marca en general se ve afectada cada vez más, **es fundamental incluir la planificación de las comunicaciones de las crisis en su plan general de respuesta ante incidentes**.

6. ¿Por qué la divulgación voluntaria de las brechas se encuentra en su máximo histórico?

Con un 61 %, el porcentaje de encuestados que han afirmado haber revelado voluntariamente una brecha el año pasado es el más alto de los cuatro años anteriores. Esto demuestra que, en general, las organizaciones informan proactivamente de las brechas, tal vez como resultado de una nueva legislación, o quizás debido a una mayor conciencia social y al deseo de mantener la confianza del cliente.

La ventaja es que más del doble de las organizaciones que han sufrido una brecha que durase más de 17 horas ha revelado la brecha voluntariamente frente a quienes han revelado la brecha de manera involuntaria o debido a las exigencias que supone la elaboración de informes.

Más de la mitad de todas las brechas (51 %) pone a las organizaciones a la defensiva, pues tienen que gestionar el escrutinio público que acarrea una brecha. Sin embargo, si bien las exigencias gubernamentales para la elaboración de informes han aumentado, la divulgación involuntaria sigue siendo en gran medida la misma en algo más de una cuarta parte (27 %) de las brechas. **Además, el 61 % de los encuestados está descubriendo ahora que su credibilidad aumenta cuando revelan de manera voluntaria una brecha importante, preservando así la reputación de la marca.**

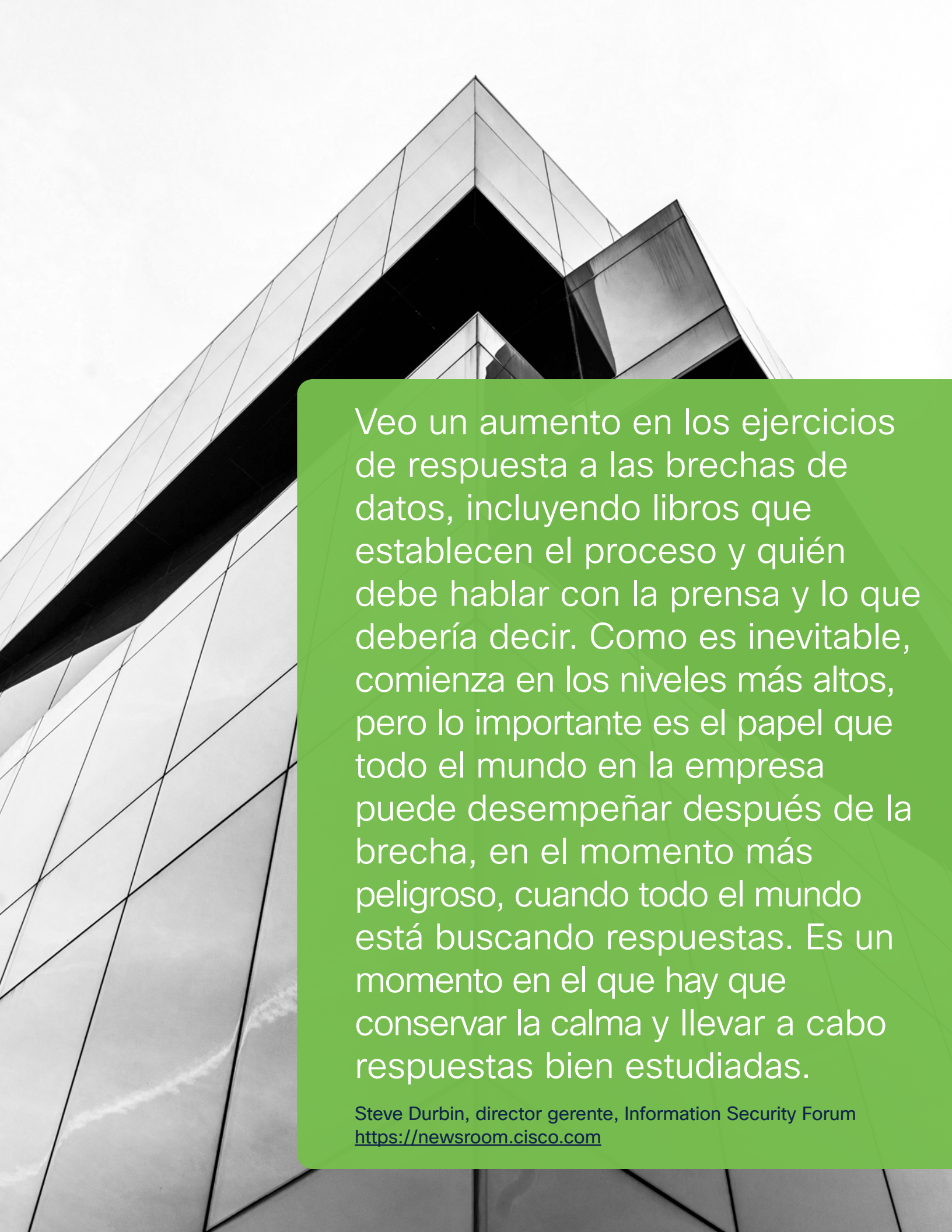
7. ¿Puede cuantificar las ventajas de la colaboración entre las redes y la seguridad?

La colaboración entre **equipos de redes y seguridad sigue siendo alta**, ya que más del 91 % de los encuestados informan que han sido muy o sumamente colaborativos en la encuesta de este año. La colaboración entre **los equipos de seguridad y terminales también se mantiene alta en un 87 %**. A pesar de haber descendido un par de puntos porcentuales en estas áreas, la tendencia general es que es menos probable que trabaje en silos.

8. ¿Qué motivos existen para la externalización además de la reducción de los costes?

En comparación con el informe del año pasado, la externalización ha aumentado de manera significativa, lo que posiblemente indique una tendencia histórica a medida que el mercado de proveedores se vuelve más y más difícil de gestionar internamente. Curiosamente, las organizaciones han informado de que esperan que su externalización disminuya en el futuro.

Nuestros encuestados externalizan por una serie de razones básicas, no solo por el coste. La rentabilidad está ligeramente por delante como la razón principal en un 55 %. Sin embargo, es seguida de cerca por los equipos de seguridad que necesitan respuestas más rápidas a los incidentes (53 %).



Veo un aumento en los ejercicios de respuesta a las brechas de datos, incluyendo libros que establecen el proceso y quién debe hablar con la prensa y lo que debería decir. Como es inevitable, comienza en los niveles más altos, pero lo importante es el papel que todo el mundo en la empresa puede desempeñar después de la brecha, en el momento más peligroso, cuando todo el mundo está buscando respuestas. Es un momento en el que hay que conservar la calma y llevar a cabo respuestas bien estudiadas.

Steve Durbin, director gerente, Information Security Forum
https://newsroom.cisco.com

9. ¿Le compensa la preparación?

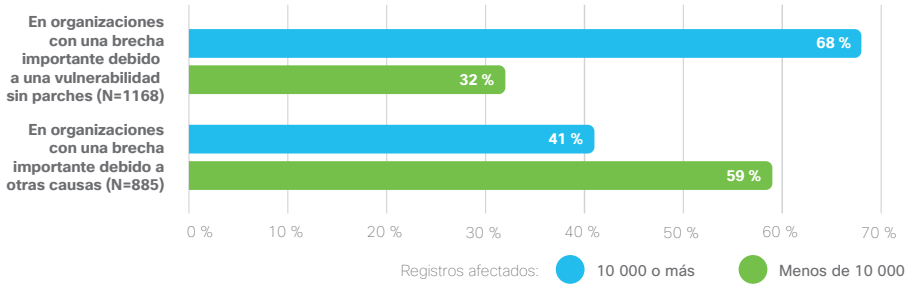
Al preguntar qué prácticas o políticas de seguridad se aplican en sus organizaciones, hemos hallado que **los encuestados que empleaban las estrategias enumeradas a continuación con mayor frecuencia contaban con costes menores debidos a las brechas importantes**. En otras palabras, si las siguientes seis prácticas se ajustan a su programa de seguridad, es más probable que sus brechas se mantengan por debajo de los 100 000 USD.

- Revisamos y mejoramos nuestras prácticas de seguridad de manera periódica, formal y estratégica a lo largo del tiempo
- Revisamos periódicamente la actividad de conexiones en la red para garantizar que las medidas de seguridad funcionen como es debido
- La seguridad está bien integrada en los objetivos y las capacidades empresariales de la organización
- Investigamos los incidentes de seguridad de forma rutinaria y sistemática
- Nuestras tecnologías de seguridad están bien integradas para que funcionen de un modo eficaz juntas
- Nuestras capacidades de detección y bloqueo de amenazas se mantienen al día.

10. ¿Hasta qué punto es fundamental la aplicación de parches en la defensa contra las brechas?

Una preocupación clave en 2020 es que el 46 % de las organizaciones (frente al 30 % del informe del año pasado) ha sufrido un incidente provocado por una vulnerabilidad sin parches. Además, **quienes padecieron una brecha importante debido a una vulnerabilidad sin parches el año pasado han sufrido mayores niveles de pérdida** de datos (Figura 6). Por ejemplo, el 68 % de las organizaciones que han padecido una brecha por una vulnerabilidad sin parches sufrieron pérdidas de 10 000 registros de datos o más el año pasado. De quienes afirmaron haber sufrido una brecha por otras causas, solo el 41 % perdió 10 000 registros o más en el mismo período de tiempo.

Figura 6: Se preguntó a los encuestados si habían sufrido un incidente de seguridad debido a una vulnerabilidad sin parches el año pasado, o debido a otras causas, en correlación con el número de registros de datos que se han perdido (N=2053). Los porcentajes se han redondeado.



Fuente: Encuesta comparativa de CISO de 2020 de Cisco

Se sabe a ciencia cierta que la aplicación de parches puede resultar complicada y causar interrupciones. Sin embargo, estos resultados muestran que existe una rentabilidad tangible de la inversión en la implementación de una política de base mínima para los parches lanzados más recientemente. **Las organizaciones deben mantener un inventario actualizado de todos los dispositivos de su entorno y realizar un análisis de riesgos de los parches que faltan. A continuación, cree un proceso de gestión de los cambios para aplicar el control de versiones y la documentación.**

11. ¿Qué provoca el tiempo de inactividad?

Como se ha indicado anteriormente, los encuestados han informado de un intervalo de horas de tiempo de inactividad. Cuando se les preguntó por la causa más frecuente del tiempo de inactividad, el malware y el correo no deseado malicioso aparecen en primer y segundo lugar. Curiosamente, la tercera causa difiere en función de la duración del tiempo de inactividad. En las brechas con un tiempo de inactividad de 0-4 horas, la suplantación de identidad es la tercera causa más frecuente. En el tiempo de inactividad que dura 4-24 horas, es el spyware. Por encima de las 24 horas, es el ransomware.

De manera significativa, el ransomware no discrimina: ha sido la amenaza más destructiva para las organizaciones grandes y pequeñas en términos de tiempo de inactividad. Las grandes cantidades de tiempo de inactividad resultante pueden deberse a la profundidad de investigación necesaria para evaluar el daño, intentar restaurar las copias de seguridad y corregir los vectores de entrada.

Para obtener más información sobre cómo lidiar con los diversos tipos de ataques, suscríbase a nuestro blog de inteligencia de amenazas de Talos.

12. ¿Hasta qué punto es complicado proteger a los empleados móviles?

Hemos solicitado a nuestros encuestados que nos informen del grado de dificultad de la protección de los diversos aspectos de su infraestructura. **Más de la mitad (52 %) nos ha comentado que los dispositivos móviles son ahora muy o sumamente complicados de defender.** Han superado al comportamiento del usuario, que fue el mayor desafío del informe del año pasado.

Con un marco de confianza cero, puede identificar y verificar a cada persona y dispositivo que intente acceder a su infraestructura. La confianza cero es un marco pragmático y con garantía de futuro que puede contribuir a ofrecer una seguridad eficaz en toda su arquitectura, pues abarca el personal, la carga de trabajo y el lugar de trabajo.

Un marco de confianza cero alcanza estas tres métricas de éxito, entre otras:

- El usuario es conocido y se ha autenticado
- El dispositivo se ha comprobado y es adecuado
- El usuario está limitado a dónde puede ir en su entorno

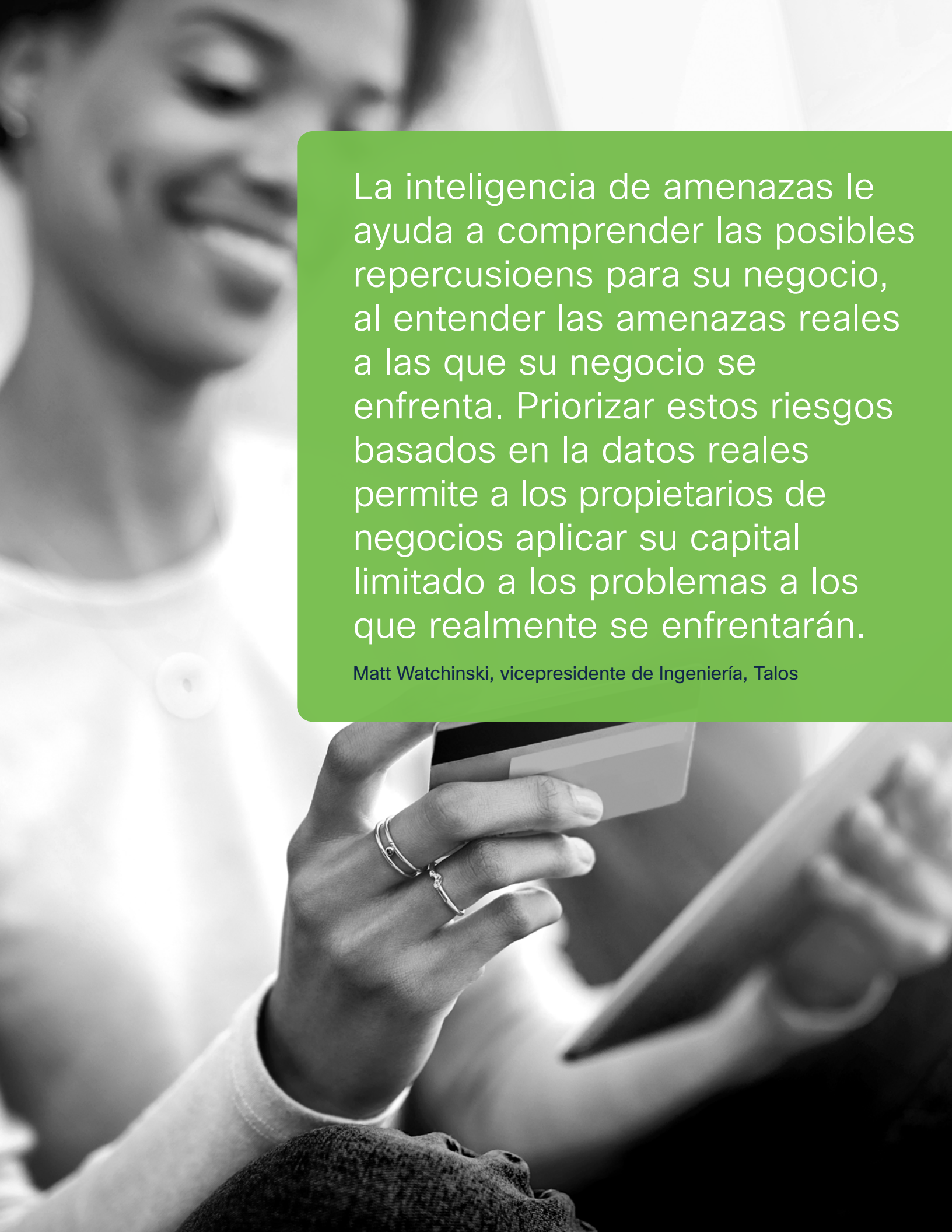
Contar con una confianza cero implementada elimina gran parte de las conjeturas en la protección de su infraestructura de todas las posibles amenazas, incluidos los dispositivos móviles.

13. ¿Cómo ampliaría la confianza cero para proteger las aplicaciones?

La seguridad de la carga de trabajo consiste en proteger todas las conexiones de los usuarios y los dispositivos a través de la red. Un marco de confianza cero puede identificar las dependencias dentro y alrededor de las bases de datos y las aplicaciones para aplicar la microsegmentación y contener el movimiento lateral.

El 41 % de nuestras organizaciones encuestadas considera que los centros de datos son muy o sumamente difíciles de defender y el 39 % afirma que se esfuerza realmente para proteger las aplicaciones. El aspecto más problemático son los datos almacenados en la nube pública, pues un 52 % considera que es muy o sumamente difícil de proteger.

Un marco de confianza cero le proporciona visibilidad de lo que se está ejecutando y lo que es fundamental mediante la identificación y la aplicación de políticas en toda la red. También le avisa en caso de la infracción de una política a través de la supervisión continua y la respuesta a los indicadores de riesgo.



La inteligencia de amenazas le ayuda a comprender las posibles repercusioens para su negocio, al entender las amenazas reales a las que su negocio se enfrenta. Priorizar estos riesgos basados en la datos reales permite a los propietarios de negocios aplicar su capital limitado a los problemas a los que realmente se enfrentarán.

Matt Watchinski, vicepresidente de Ingeniería, Talos

14. ¿Sigue siendo difícil defender la infraestructura de red?

La infraestructura de nube privada es un desafío de seguridad principal para las organizaciones. (El 50 % de las organizaciones la considera muy o sumamente difícil de defender). En lo que respecta a la infraestructura de red, el 41 % de las organizaciones la considera muy o sumamente difícil de defender.

En este punto es donde un marco de confianza cero aporta valor. Incluye el mantenimiento del control de acceso definido por software sobre todas las conexiones que se dan dentro de las aplicaciones y en un entorno multinube basado en el usuario, el dispositivo y el contexto de la aplicación, no en la ubicación. Este modelo le permite mitigar, detectar y responder a los riesgos en toda su infraestructura, independientemente de la distribución o la ubicación. A continuación, se muestran las etapas del marco definido para desarrollar la madurez de la seguridad de confianza cero.

Desarrollo de un modelo de madurez de la seguridad de confianza cero

En Cisco, empleamos cinco pasos de transformación para que nuestros clientes los adopten como estructura para implementar un **marco de confianza cero** en su organización:

Etapa 1: ¿Tiene una estrategia clara en relación con la gestión de acceso e identidades (IAM) que concuerde con las necesidades de su negocio que haya dado lugar a una implementación e integración completas de una solución de autenticación de varios factores (MFA) compatible con las políticas basadas en riesgos?

Etapa 2: ¿Tiene un inventario de recursos actualizado que distinga entre los dispositivos administrados y no administrados y que los someta a una comprobación higiénica como parte de una función integrada de TI y seguridad?

Etapa 3: ¿Tiene una política de dispositivos de confianza que solicite a los usuarios que actualicen sus dispositivos contra las vulnerabilidades evaluada (dentro de un proceso gestionado) e informes sobre dispositivos que no se ajusten a la política?

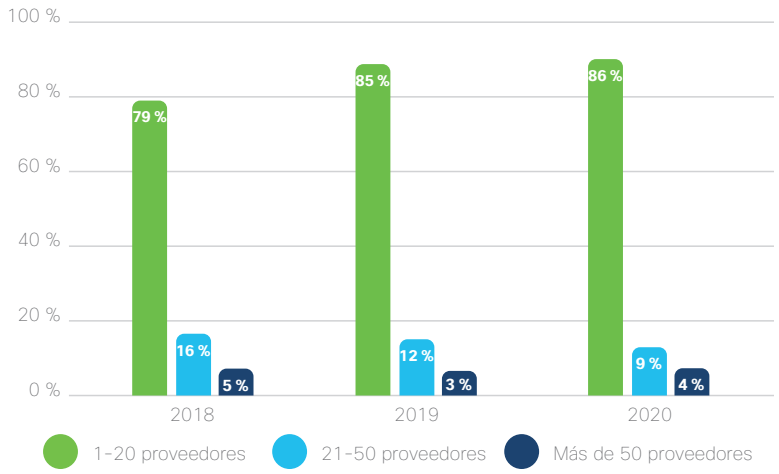
Etapa 4: ¿Controla el acceso de los usuarios a través de una política gestionada de forma centralizada que identifique y actúe ante las excepciones?

Etapa 5: ¿Tiene una estrategia de confianza cero en consonancia con el negocio y respaldada por una arquitectura y un conjunto de procesos que permita a los usuarios acceder sin problemas a las aplicaciones locales y en la nube?

15. ¿Puede medir el efecto de la consolidación de proveedores?

La tendencia a reducir la complejidad a través de la consolidación de proveedores continúa y se mantiene estable, pues el **86 % de las organizaciones utiliza entre 1 y 20 proveedores, en España el 91%, y el 13 %, el 8% en España, utiliza más de 20** (Figura 7).

Figura 7: Número de distintos proveedores de seguridad (es decir, marcas, fabricantes) utilizados en los entornos de seguridad de los encuestados (N=2800). Los porcentajes se han redondeado.



Fuente: Encuesta comparativa de CISO de 2020 de Cisco

Desde 2017, se han producido algunos cambios en la forma en que las organizaciones consideran que están haciendo frente a una estrategia de varios proveedores. **El 28 % considera ahora que la gestión de un entorno de varios proveedores es muy complicada, lo que ha aumentado un 8 % desde 2017. El 53 % considera ahora que es algo complicada.** Menos organizaciones (del 26 % al 17 %) consideran que resulta sencillo gestionar un entorno de varios proveedores. La mayoría de las organizaciones se enmarca ahora en las categorías de " considerarla complicada" (81 %). Esto puede significar que tiene menos proveedores que administrar o que ha comenzado a usar herramientas como motores de análisis para mejorar los resultados de varias herramientas dispares.

También hemos analizado las tendencias entre las alertas en un entorno de varios proveedores y la repercusión que tienen en el agotamiento debido a la ciberseguridad (que analizamos con algo más de profundidad en el siguiente tema). **Definido como renunciar virtualmente a la defensa proactiva contra los agentes maliciosos, el 42 % de los encuestados sufren agotamiento debido a la ciberseguridad, un 34% en España.**

Nuestros datos han revelado que, en el caso de las organizaciones que sufren de agotamiento, estas son mucho más propensas a considerar que un entorno de varios proveedores es complicado. Además de tener que responder a demasiadas alertas y combatir la complejidad del proveedor, hemos hallado que sufrir una brecha de mayor repercusión (en términos del número de horas de tiempo de inactividad) también aumenta el agotamiento. Sin embargo, puesto que más del 96 % de los encuestados que sufren agotamiento afirma que la gestión de un entorno de varios proveedores es complicada, **la complejidad parece ser una de las principales causas del desgaste**.

No quiero dedicar tiempo a integrar productos de seguridad. Solo quiero implementar la seguridad. Le digo a mi equipo que quiero ver tres cosas en lo referente a un nuevo producto:

- Asegurarnos de que funciona
- Asegurarnos de que tenga visibilidad completa Cero incertidumbre
- Asegurarnos de que esté integrado con el resto de nuestro ecosistema de seguridad

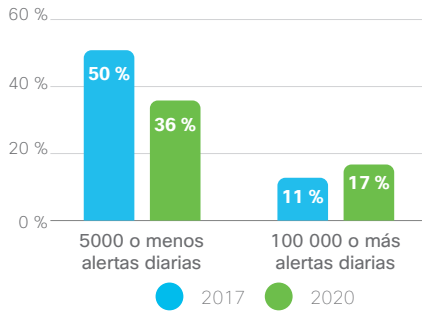
Steve Martino, SVP, director de seguridad e información en Cisco

16. ¿Cuáles son las causas de su desgaste y agotamiento debido a la ciberseguridad?

En la sección anterior, hemos comenzado a observar una relación entre los entornos de varios proveedores y el creciente agotamiento. Ahora, analizaremos el volumen medio de alertas de seguridad diarias que recibe una organización.

El número total de alertas diarias que se manejan ha aumentado en los últimos años. En 2017, el 50 % de las organizaciones recibía 5000 alertas diarias o menos; ahora solo el 36 % se enmarca en esta categoría. Además, la cantidad de organizaciones que reciben 100 000 alertas diarias o más ha crecido del 11 % en 2017 al 17 % en 2020 (Figura 8).

Figura 8: Número de alertas recibidas de las que se han informado (N=2800). Los porcentajes se han redondeado.



Fuente: Encuesta comparativa de CISO de 2020 de Cisco

Tal vez debido a este aumento en el volumen y los recursos de procesamiento necesarios, la investigación de las alertas se encuentra en su nivel más bajo en más de cuatro años, con algo menos del 48 %. (El porcentaje en 2017 era un 56 % y ha ido disminuyendo cada año desde entonces). La tasa de incidentes legítimos, del 26 %, se mantiene constante año tras año e indica que muchas investigaciones están generando falsos positivos.

Eso sí, el número de amenazas legítimas que se corrigen ha mejorado desde el informe del año pasado y ahora hemos vuelto a los niveles de 2017, con un 50 %. Sin embargo, este porcentaje sigue significando que la mitad de todos los incidentes reales se quedan desatendidos.

En particular, el abrumador número de alertas está afectando al agotamiento debido a la ciberseguridad. **Entre quienes afirman sufrir de agotamiento, el 93 % recibe más de 5000 alertas al día.**

Para hacer frente al ruido y el volumen cada vez mayores de las alertas, apostamos por un enfoque que tenga la automatización en su núcleo. La automatización permite que las políticas se apliquen de manera más coherente, rápida y eficiente. Cuando se determina que un dispositivo está infectado o es vulnerable, se pone automáticamente en cuarentena o se deniega el acceso sin necesidad de que un administrador realice ninguna acción.

17. ¿Qué ventajas en materia de seguridad se asocian con la infraestructura de alojamiento en la nube?

Durante nuestra investigación, hemos descubierto que una eficacia, eficiencia y visibilidad mayores son algunos de los principales factores que impulsan a las organizaciones a trasladar su seguridad (88 %) e infraestructura (89 %) a la nube. Y no es de extrañar que el **86 % afirme que el uso de la seguridad en la nube ha aumentado la visibilidad de sus redes**. En 2020, hemos seguido observando que más del 83 % de las organizaciones administraba más del 20 % de su infraestructura de TI en la nube (ya sea de manera interna o externa).

> Los clientes dependen cada vez más de los proveedores para profundizar en los incidentes, pues estos ofrecen análisis avanzados e informes de diagnóstico detallados. Esto requiere que los proveedores de IR aporten combinaciones muy especializadas de productos y procesos para reducir el tiempo medio de contención (MTTC) y el tiempo medio de corrección (MTTR) de un incidente activo.
>
> Guía comercial de servicios digitales de informática forense y respuesta ante incidentes, Gartner, diciembre de 2019[4]

[4] Brian Reed, Toby Bussa, Guía comercial de servicios digitales de informática forense y respuesta ante incidentes, Gartner, 11 de diciembre de 2019

18. ¿Qué desafíos cree que depara el futuro?

Aunque presente una oleada de cambios en la infraestructura que pueden ser difíciles de implementar, la transformación digital continúa siendo una oportunidad para que los líderes en seguridad y TI innoven y obtengan una ventaja frente a la competencia.

Los profesionales de seguridad están adoptando tecnologías y enfoques avanzados, desde la inteligencia artificial y el aprendizaje automático hasta la implementación segura de DevOps y microsegmentación. Y, como todos sabemos, los entornos multinube siguen siendo los entornos predominantes.

Dada la naturaleza dinámica de este entorno, los profesionales de la seguridad no solo deben dominar los conceptos básicos, sino también mantenerse al día con las tecnologías más recientes que tengan a su disposición. Podría decirse que algunas de estas tecnologías más recientes deberían convertirse en un elemento básico en su ecosistema de seguridad, aunque no lo sean en la actualidad.

Por ejemplo, observamos que en esta era de ubicuidad digital, **solo el 27 % de las organizaciones utilizan actualmente la autenticación de varios factores (MFA)**. Este número es bajo para una tecnología de confianza cero tan valiosa. Los encuestados de los siguientes países han mostrado las tasas de adopción más altas de la MFA en este orden: Estados Unidos, China, Italia, India, Alemania y Reino Unido. Los sectores con las tasas de adopción más altas (en este orden) son el desarrollo de software, los servicios financieros, los organismos gubernamentales, el comercio minorista, la fabricación y las telecomunicaciones.

Con respecto a la transformación digital, además de la adopción de la nube, la automatización es la gran ganadora. Muchos profesionales de la seguridad aprovechan la automatización para resolver su problema de escasez de competencias a medida que adoptan soluciones con mayores capacidades de aprendizaje automático e inteligencia artificial.

Como se ilustra en la Figura 9, **la mayoría (77 %) de nuestros encuestados planean aumentar la automatización para simplificar y acelerar los tiempos de respuesta en sus ecosistemas de seguridad.** Al planear la automatización, debe definir estratégicamente dónde será más eficaz la automatización y proporcionar el mayor retorno de la inversión dentro de su organización.

Figura 9: Encuestados con planes para aumentar el uso de la automatización en todo el ecosistema de seguridad de su organización durante el próximo año (N=2800). Los porcentajes se han redondeado.

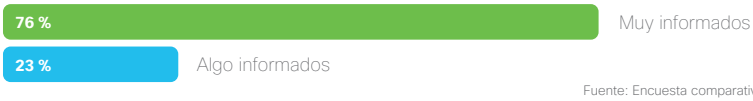
Fuente: Encuesta comparativa de CISO de 2020 de Cisco

19. ¿Cuánta atención debe poner a la respuesta ante incidentes?

El panorama de las amenazas ha evolucionado a un entorno complejo y desafiante para las organizaciones de todo el mundo. La escasez de talento, combinada con el aumento de los incidentes, ha llevado a una postura en materia de seguridad generalmente débil en la mayoría de las organizaciones. Relajarse y esperar a que surja una alerta sin prevención alguna puede conllevar grandes multas, un mayor escrutinio, la pérdida de la propiedad intelectual, riesgos para la privacidad de los datos y la pérdida de acuerdos comerciales. La prevención, mediante el aumento de la visibilidad, la búsqueda de amenazas y la definición de un marco de confianza cero, se ha convertido en un proceso fundamental para proteger su infraestructura.

En nuestra encuesta a los responsables de la toma de decisiones de TI, **el 76 % se consideraba muy bien informado acerca de la respuesta ante incidentes y el 23 % afirmaba que estaba algo informado, lo que suma un total de un 99 %**. Esa es la buena noticia. Sin embargo, como hemos descubierto en nuestra encuesta, la complejidad de la seguridad está generando agotamiento debido a la ciberseguridad, que podría ejercer una carga excesiva en sus recursos, que son difíciles de obtener. En este punto es donde la externalización puede ser de ayuda.

Figura 10: Porcentajes de encuestados que están muy bien o algo informados acerca de la respuesta ante incidentes, que suman un total de un 99 %. N=2800. Los porcentajes se han redondeado.



Fuente: Encuesta comparativa de CISO de 2020 de Cisco

Hemos descubierto que el 34 % externaliza los servicios de respuesta ante incidentes y que el 36 % utiliza servicios externos/de terceros para analizar los sistemas en riesgo, lo que significa un aumento con respecto al año pasado. El uso de un servicio de respuesta ante incidentes se ha convertido en un enfoque eficaz para proteger los recursos, mitigar el riesgo y mantener el cumplimiento. Puede contribuir a que su organización se proteja contra lo desconocido gracias a una planificación proactiva y a la experiencia para coordinar y llevar a cabo una respuesta.

¿Desea obtener información acerca de cómo usted o su personal pueden mejorar su trayectoria profesional en el campo de la ciberseguridad?

Visite: Certificados de seguridad de Cisco.

20. ¿Qué puede hacer en este momento para impulsar mejoras en su postura relativa a la seguridad?

Se enfrenta a adversarios activos que son muy pacientes y tienen amplios recursos económicos. También tiene que lidiar con desafíos constantes que nunca parecen desaparecer, como mantener un inventario preciso de usuarios, aplicaciones y dispositivos. Tiene que administrar el riesgo empresarial, el riesgo de seguridad y, al mismo tiempo, permitir a los equipos moverse rápido. Sin embargo, las decisiones empresariales se siguen tomando sin tener en cuenta la seguridad. Y, cuando se añaden nuevas normativas, mandatos de la junta directiva, presupuestos ajustados, gestión de riesgos y una puerta giratoria del personal de seguridad, es una rueda que nunca se detiene.

Los desafíos que supone la defensa de su organización se están acelerando y no van a dejar de hacerlo. Es hora de trabajar de manera más inteligente, optimizar la defensa y centrarse en la prevención, así como en la detección y corrección de amenazas. En este informe, hemos proporcionado 20 áreas que puede tener en cuenta como ayuda para dirigir su organización con mayor seguridad. Con ellas, hemos aportado recomendaciones que se pueden resumir de la siguiente manera:

- Emplee una defensa por capas, que debe incluir MFA, segmentación de red y protección de terminales
- Obtenga los más altos niveles de visibilidad para reforzar la administración de datos, reducir el riesgo y aumentar el cumplimiento
- Apuntale las defensas, actualice sus dispositivos y aplíqueles parches, y céntrese en la higiene cibernética mediante simulacros y formación
- Mejore la madurez de su seguridad mediante la creación de un marco de confianza cero (Figura 13).

Figura 11: Una estrategia de confianza cero puede proteger al personal, la carga de trabajo y el lugar de trabajo.

Proteja a su personal
Acceso seguro para los usuarios y los dispositivos que se conectan a las aplicaciones

Proteja su carga de trabajo
Proteja todas las conexiones de sus aplicaciones en todos los entornos

Proteja su lugar de trabajo
Conéctese de forma segura a través de su red

En Cisco, creemos que es hora de que el sector de la seguridad evolucione. Las soluciones de seguridad deben funcionar como un equipo. Los equipos se comunican en tiempo real, aprenden unos de otros y responden como una unidad coordinada. La seguridad de los terminales debe coordinarse con la seguridad de la red y la seguridad de la nube y necesita una MFA que cubra la identidad y el acceso. **Creemos que la mejor manera de proteger realmente su empresa se logra a través de un enfoque de plataforma que garantice que todas las brechas tengan cobertura de seguridad.**

21. La ciberseguridad baja en la escala de prioridades de los directivos españoles.

Al igual que en el resto del mundo, también en España se ha registrado una disminución de la importancia que tiene la seguridad informática para los dirigentes de las empresas.

Mientras que en 2019 el 95% de los expertos españoles estimaban que los dirigentes españoles consideraban la seguridad informática una prioridad muy importante de la empresa, en 2020 este porcentaje se ha reducido en un 16%. Una disminución claramente inferior con respecto al 7% de la tendencia mundial.

Figura A: La dirección ejecutiva de mi empresa, en España, considera la seguridad una prioridad muy importante.

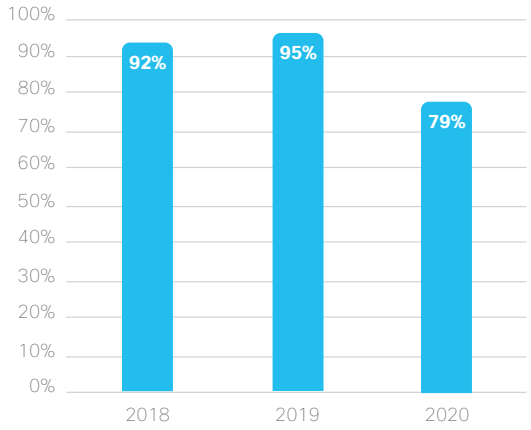
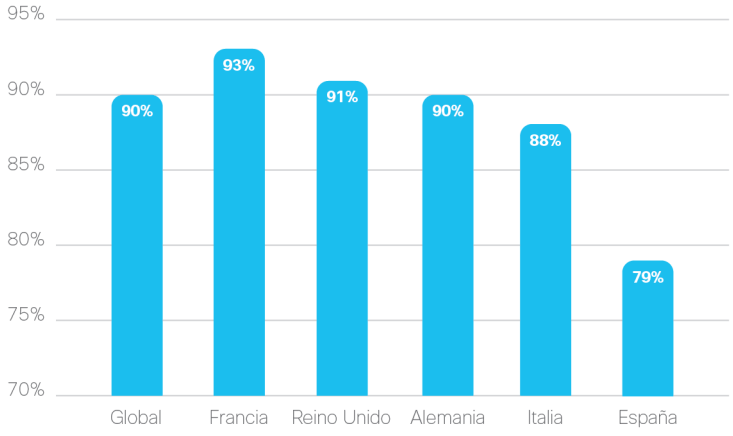


Figure. (N=600) Los porcentajes se han redondeado

La particularidad de España es que parece que es el país europeo donde se da menos importancia a la seguridad informática en el nivel de la dirección.

Figura B: La dirección ejecutiva de mi empresa, en España, considera la seguridad una prioridad muy importante.



Espana=n.200. Los porcentajes se han redondeado

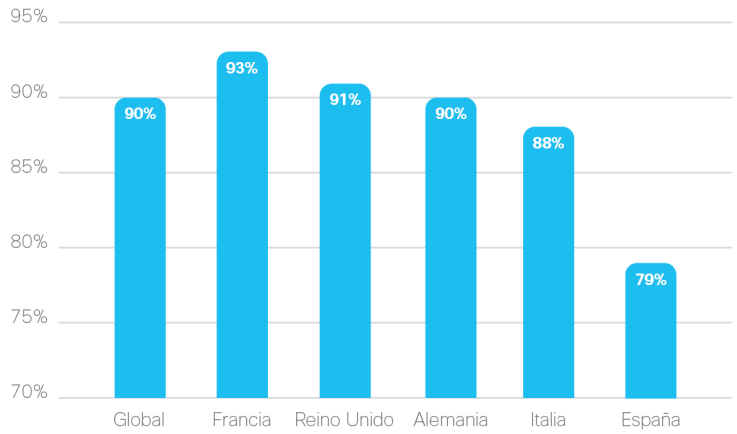
Esta situación implica dos aspectos:

1. En España, como práctica rutinaria, los expertos del sector no incluyen mayoritariamente el proceso de evaluación de riesgos cibernéticos dentro de los procesos normales de evaluación de riesgos.
    a. Solo el 80% de las empresas españolas lo considera un proceso integrado de forma natural en los procesos empresariales de evaluación de riesgos frente al 90% de las empresas de todo el mundo y el 89% de las empresas europeas.

2. Los consejos directivos españoles no han establecido métricas de evaluación claras de la efectividad de un programa de seguridad informática. De hecho, solo el 77% de las empresas españolas cuenta con parámetros precisos para evaluar la eficacia de un programa de seguridad informática frente al 90% de las empresas de todo el mundo.

¿Cuál es por lo tanto el criterio adoptado en España para determinar la eficacia de un programa de seguridad informática?

Figura C: Mi empresa usa el " tiempo de detección" para determinar el rendimiento de seguridad.



Espana=n.200. Los porcentajes se han redondeado

El tiempo de corrección (implementación de parches) para el 54% de las empresas españolas. Sin embargo, el criterio para el 65% de las empresas de todo el mundo es el " tiempo de detección" . En el gráfico se puede ver la posición de España respecto a este indicador.

Considerar la seguridad informática como un elemento que no afecta a los objetivos de la empresa significa perder una ocasión de crecimiento y evolución. Una oportunidad que sí han aprovechado empresas españolas como Indra o Ibermutuamur.

> “La ciberseguridad es fundamental para proteger los datos vitales de la empresa y es fundamental para generar confianza y por lo tanto, negocio. Es muy importante que la dirección de las compañías tome la ciberseguridad como una prioridad”
>
> Eutimio Fernandez, Director de Ciber-seguridad en Cisco España.

Protección para el presente y el futuro

Nuestra visión es proteger a nuestros clientes de las amenazas de hoy y de mañana para que puedan centrarse en su misión principal y dejarnos la seguridad a nosotros.

Presentamos la plataforma de seguridad de Cisco – SecureX – creada por el equipo de seguridad más fuerte del planeta, ofreciendo la protección que necesita para la forma en que funciona su negocio.

- Comenzamos con las **mejores soluciones** para proteger la red, el terminal, las aplicaciones y la nube.
- Utilizamos la **verificación de confianza** para garantizar que solo las personas adecuadas obtengan acceso a su red
- Respaldamos cada producto con la **inteligencia de amenazas** de Talos líder en el sector para bloquear más amenazas y mantener las organizaciones más seguras.
- Ofrecemos **respuestas automatizadas a amenazas avanzadas** y **simplificamos las operaciones con una gestión integrada de las amenazas y la seguridad** en toda nuestra cartera
- **Diseñamos nuestras soluciones de modo que funcionen con otras tecnologías que tenga implementadas** para ofrecer respuestas de seguridad integradas, incluso fuera de Cisco.

SecureX ofrece visibilidad, acciones automatizadas y una postura de seguridad mejorada. Las aplicaciones personalizadas y entregadas en la nube también se han creado sobre la **plataforma SecureX** para simplificar la seguridad. Conectamos la cartera de seguridad integrada de Cisco y los productos de terceros desde el entorno del cliente a una interfaz coherente. Y la innovación a nivel de plataforma de Cisco ofrece los análisis más integrados del planeta. Todos trabajando juntos:

- SecureX une a los equipos de operaciones de seguridad, red y TI con flujos de trabajo colaborativos para mejorar la productividad
- Cisco Threat Response simplifica las investigaciones de amenazas y su corrección para mejorar la eficiencia de SecOps
- Los análisis simplifican la detección de amenazas desconocidas para mejorar las decisiones de políticas, los tiempos de respuesta y la eficacia de la respuesta a las amenazas

Gracias a nuestra inteligencia de amenazas líder en el sector y a nuestra cartera integrada, Cisco le ofrece las herramientas, la escalabilidad y las capacidades para seguir el ritmo a las amenazas, cada vez más complejas y mayores. Dar prioridad a la seguridad por encima de todo lo demás le permite innovar mientras protege sus activos. Para nosotros, la seguridad es lo más importante en todo lo que hacemos. Solo con Cisco conseguirá una seguridad de red eficaz para enfrentarse a las amenazas del mañana. Obtenga más información sobre nuestro enfoque de plataforma en cisco.com/go/security.

Información sobre la serie de informes sobre ciberseguridad de Cisco

Durante la última década, Cisco ha publicado una amplia cantidad de información sobre inteligencia de amenazas y seguridad para los profesionales de seguridad que están interesados en el estado de la ciberseguridad global. Estos completos informes han ofrecido cuentas detalladas de los panoramas de amenazas y sus implicaciones organizativas, además de prácticas recomendadas para defenderse de los efectos negativos de las brechas de datos.

La seguridad de Cisco publica una serie de publicaciones basadas en datos e investigación con el título Serie de ciberseguridad de Cisco. Hemos ampliado el número de títulos con el fin de incluir diferentes informes para profesionales de seguridad con intereses distintos. Hacemos un llamamiento a la amplitud y el alcance de la experiencia de los innovadores e investigadores de amenazas del sector de la seguridad, ya que los informes de la serie de cada año incluyen el estudio comparativo de privacidad de los datos, el informe sobre amenazas y el estudio comparativo de CISO, además de otros documentos publicados a lo largo del año.

Para obtener más información y acceder a todos los informes y copias archivadas, visite www.cisco.com/go/securityreports.


Privacidad de los datos 2019


Informe sobre amenazas 2019


Referencia de CISO 2019


Correo electrónico: cuidado al hacer clic


Estándares mínimos de seguridad

Búsqueda de amenazas


Encuesta de privacidad a consumidores

Amenazas del año 2019


Privacidad de los datos 2020


Referencia de CISO 2020

Sede central en América
de Cisco Systems, Inc.
San José (California)

Sede central en Asia-Pacífico
de Cisco Systems (EE. UU.), Pte. Ltd.
Singapur

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

Cisco tiene más de 200 oficinas en todo el mundo. Las direcciones, números de teléfono y fax se encuentran en la web de Cisco en www.cisco.com/go/offices.

CISO_02_0220

Publicado en febrero de 2020

cisco Seguridad

Seguridad