CISCO
SECURE

Estudio de resultados en materia de seguridad

Volumen 2

Maximización de las cinco principales prácticas de seguridad

Contenido

(Re)Presentación de los fabulosos cinco

El estudio de resultados en materia de seguridad de Cisco de 2021 procuró medir lo más importante en la administración de la ciberseguridad. Con ese fin, examinamos 25 prácticas de seguridad generales y probamos cómo cada una se correlaciona con el logro de 11 resultados en el nivel del programa. Puede ver las correlaciones de estos resultados de las prácticas mediante una visualización interactiva en el sitio web del Estudio de resultados en materia de seguridad de 2021 de Cisco, o descargar el informe completo.

En las pruebas, descubrimos que cinco de las 25 prácticas se destacaban del resto en cuanto a contribución total al éxito del programa de seguridad en todos los resultados medidos.

En las páginas que siguen, nos centramos en estos "fabulosos cinco" impulsores del éxito del programa de seguridad para identificar estrategias para maximizar su eficacia.

Los "fabulosos cinco" son:

Actualización tecnológica proactiva:	la organización cuenta con una estrategia de actualización tecnológica proactiva para estar al día con las mejores tecnologías de seguridad y TI disponibles.
Tecnologías de seguridad bien integradas:	nuestras tecnologías de seguridad están bien integradas y funcionan eficazmente en conjunto.
Respuesta oportuna ante incidentes:	nuestras capacidades de respuesta ante incidentes permiten una investigación y corrección oportunas y eficaces de los eventos de seguridad.
Rápida recuperación tras desastres:	las capacidades de recuperación minimizan el impacto y garantizan la recuperabilidad de las funciones empresariales afectadas por incidentes de seguridad.
Detección precisa de amenazas:	nuestras capacidades de detección de amenazas brindan un reconocimiento preciso de los posibles eventos de seguridad sin puntos ciegos significativos.

La amplia eficacia de estas prácticas plantea la pregunta: "¿Por qué?" ¿Qué los hace tan clave para desbloquear el éxito? ¿Qué factores los hacen más o menos eficaces? ¿Cómo deben las empresas implementar estas prácticas para maximizar los resultados? Estos son los tipos de preguntas que queremos explorar en esta iteración del Estudio de resultados en materia de seguridad.

En las páginas que siguen, nos centramos en estos "fabulosos cinco" impulsores del éxito del programa de seguridad para identificar estrategias para maximizar su eficacia. Lo hacemos a través de una encuesta doble ciego realizada de forma independiente a más de 5100 profesionales de TI y seguridad en todo el mundo. Analizamos los datos, extraemos hallazgos sobresalientes y compartimos conclusiones para ayudar a desbloquear nuevos niveles de logro de seguridad para su organización.

Hallazgos clave

Le preguntamos a más de 5100 profesionales de TI y seguridad sobre los enfoques de sus organizaciones para actualizar e integrar la arquitectura de seguridad, detectar y responder a las amenazas, y mantenerse resilient cuando ocurre un desastre. Como puede imaginar, compartieron una amplia gama de perspectivas, dificultades, estrategias y éxitos. Analizamos cada respuesta de varias maneras, y extrajimos conclusiones clave como las que se presentan a continuación.

Actualizar e integrar la arquitectura

- La TI moderna y bien integrada contribuye al éxito general del programa más que cualquier otro control o práctica de seguridad.
- Las arquitecturas más nuevas basadas en la nube son mucho más fáciles de actualizar periódicamente para seguir el ritmo de los negocios.
- Las organizaciones que obtienen servicios principalmente de un único proveedor duplican sus posibilidades de crear una pila tecnológica integrada.
- Las tecnologías de seguridad integrada son siete veces más propensas a alcanzar altos niveles de automatización de procesos.

Detectar y responder a las amenazas cibernéticas

- Los programas de SecOps basados en tecnología, personas y procesos fuertes ven un aumento del rendimiento 3.5 veces mayor que aquellos con recursos más débiles.
- Los equipos de respuesta y detección subcontratados se perciben como superiores, pero los equipos internos muestran un tiempo medio de respuesta más rápido (6 días frente a 13 días).
- Los equipos que utilizan ampliamente la inteligencia de amenazas tienen el doble de probabilidades de reportar capacidades sólidas de detección y respuesta.
- La automatización supera el doble del rendimiento de las personas menos experimentadas y hace que los equipos fuertes estén casi seguros (95 %) para lograr el éxito de SecOps.

Mantenerse resiliente cuando ocurre un desastre

- Las organizaciones con supervisión en el nivel de la junta directiva de la continuidad del negocio y la recuperación tras desastres son las más propensas (11 % por encima del promedio) a reportar que cuentan con programas sólidos.
- La probabilidad de mantener la capacidad de recuperación empresarial no mejora hasta que la continuidad del negocio y las capacidades de recuperación tras desastres abarcan al menos el 80 % de los sistemas críticos.
- Las organizaciones que prueban periódicamente sus capacidades de continuidad del negocio y recuperación tras desastres de varias maneras tienen 2,5 veces más probabilidades de mantener la capacidad de recuperación empresarial.
- Las organizaciones que realizan la práctica estándar de ingeniería del caos tienen el doble de probabilidades de alcanzar altos niveles de recuperabilidad.

Acerca de la encuesta

Muestreo	Encuestados	Análisis
Cisco contrató a una empresa de investigación mediante encuestas, YouGov, para realizar una encuesta totalmente anónima a mediados de 2021 que utilizó una técnica de muestreo aleatorio estratificado.	Respondieron 5123 profesionales activos de TI, seguridad y privacidad de 27 países. Puede encontrar ejemplos de datos demográficos en el apéndice.	Cyentia Institute realizó un análisis independiente de los datos de la encuesta para Cisco y generó todos los resultados que se presentan en este estudio.

5,123 profesionales activos de TI, seguridad y privacidad de **27** países respondieron

"Necesitamos saber que estamos haciendo todo lo posible para mantener las cosas seguras. Sabemos lo avanzados que están los atacantes, que se vuelven más avanzados y tienen nuevas técnicas todos los días. Queremos proteger nuestros dispositivos, usuarios y empresas, por lo que queremos reducir la superficie de ataque ante posibles vulneraciones a la seguridad"

Eric J. Mandela, director asistente de infraestructura tecnológica en Allied Beverage Group

Más información

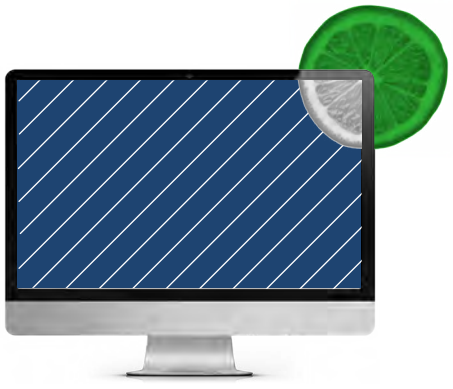
Estrategias para la actualización de tecnología proactiva

En nuestro estudio anterior, descubrimos que un enfoque proactivo para actualizar y mantener las mejores tecnologías de TI y seguridad contribuyó más a un programa de ciberseguridad exitoso que cualquier otra práctica. Esto no es poca cosa, teniendo en cuenta que las 25 prácticas que probamos se consideran "procedimientos recomendados" por derecho propio. Por lo tanto, queríamos profundizar en lo que hace que este procedimiento sea tan eficaz en este estudio de seguimiento.

A medida que profundizamos en las estrategias de actualización tecnológica, hagamos una rápida prueba de la actualización de la infraestructura existente. Les preguntamos a los encuestados qué proporción de sus tecnologías de seguridad activas están desactualizadas. En promedio, el 39 % de las tecnologías de seguridad utilizadas por las organizaciones se consideran desactualizadas. Casi el 13 % de los encuestados afirma que al menos 8 de cada 10 herramientas de seguridad que utilizan muestran su edad.

Este hecho por sí solo puede ayudar a explicar muchos de los beneficios que vemos de una estrategia de actualización tecnológica proactiva. Aparentemente, las tecnologías más nuevas incorporan funcionalidades avanzadas contra una horda cada vez mayor de ciberamenazas. Pero hay más que eso, así que sigamos analizando las preguntas que les hicimos sobre los datos.

En promedio, el 39 % de las tecnologías de seguridad utilizadas por las organizaciones se consideran desactualizadas.



¿Las características de la infraestructura afectan las iniciativas de actualización?

En el estudio original, especulamos que arquitecturas más modernas basadas en la nube podrían ser más eficaces porque son más fáciles de administrar y tienen medidas de seguridad nativas incorporadas. Como paso para probar esa hipótesis, les pedimos a los encuestados que describieran en general la infraestructura de su tecnología mediante la elección de un conjunto de descriptores a escala, que incluyen:

- En la nube vs. en las instalaciones
- Moderno vs. obsoleto
- Consolidado vs. distribuido

¿Estos diferentes rasgos arquitectónicos contribuyen a la eficacia de las capacidades de actualización tecnológica? Mucho, según la Figura 1. Las organizaciones con arquitecturas modernas, consolidadas y basadas en la nube tienen más del doble de probabilidades de reportar capacidades de actualización tecnológica sólidas que aquellas que usan tecnologías obsoletas, distribuidas y en las instalaciones. Sin embargo, antes de omitir ese gráfico en la próxima reunión de estrategia de migración a la nube, tenga en cuenta que las organizaciones con entornos predominantemente en las instalaciones aún funcionan muy por encima de la media, siempre que hayan modernizado la TI.

Claro, ser nativo de la nube hace que sea más fácil liberarse de su estrategia de actualización tecnológica, pero estar desactualizado es el problema más urgente aquí. Si mantener actualizada la infraestructura antigua se convierte en una ardua batalla, puede avanzar más si migra a una nueva arquitectura que si continúa modernizando la antigua. Eso no siempre es posible o rentable con una infraestructura crítica o heredada, por supuesto, pero aún se aplica el principio general.

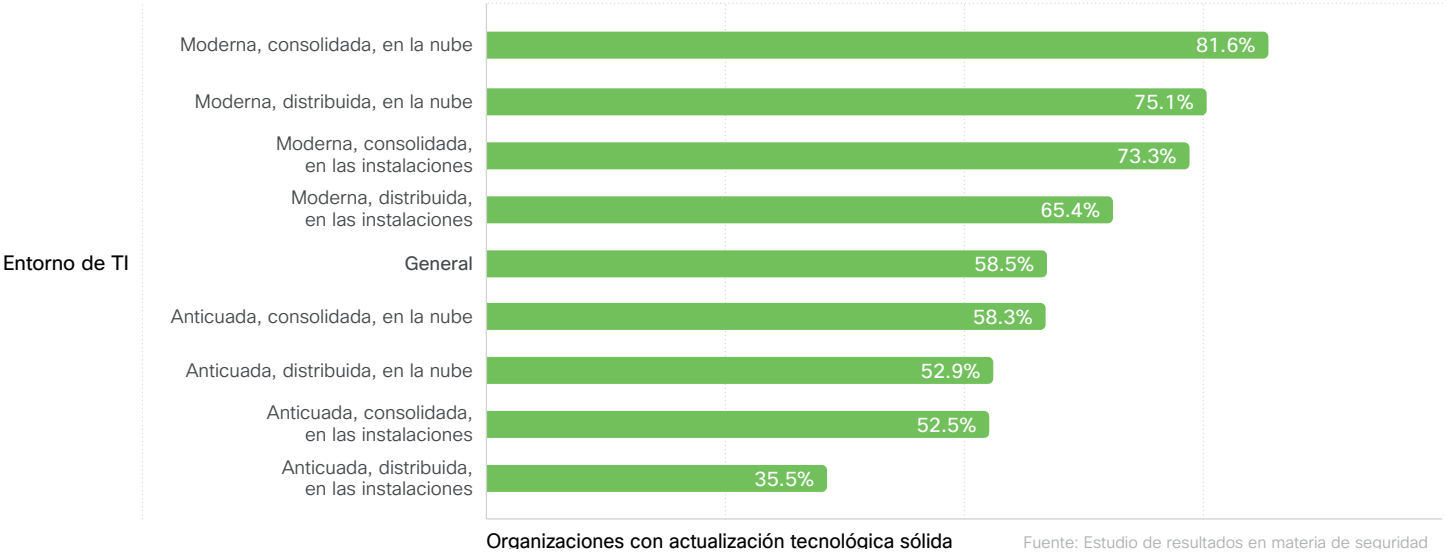
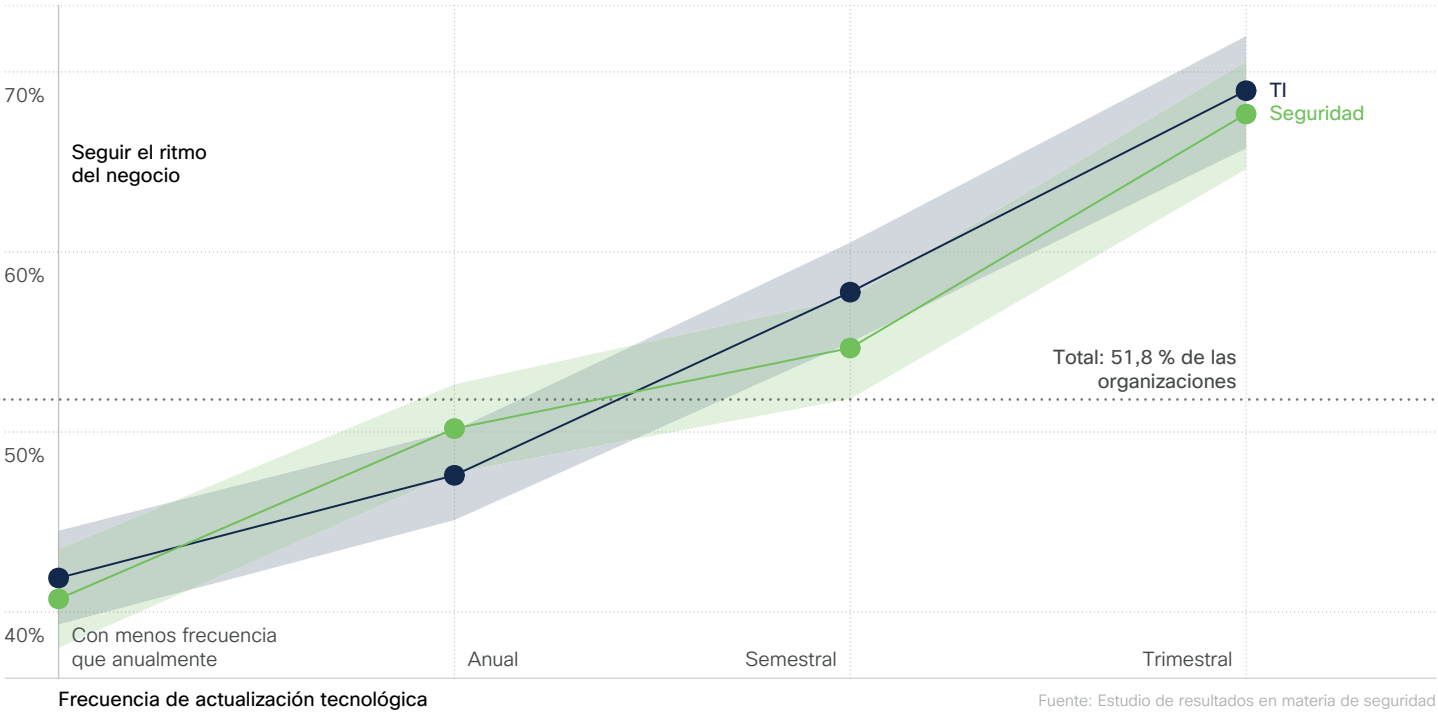


Figura 1: Efecto de los rasgos de la arquitectura de TI en el rendimiento de la actualización tecnológica

81.6% de las organizaciones con arquitecturas basadas en la nube reportan sólidas capacidades de actualización tecnológica.

¿Las actualizaciones frecuentes ayudan a que la seguridad esté al día con los negocios?

Según el Estudio de resultados en materia de seguridad de 2021, el resultado más estrechamente relacionado con una estrategia de actualización tecnológica proactiva fue permitir que el programa de seguridad cumpliera con las demandas y el crecimiento del negocio. De hecho, esa fue la combinación práctica-resultado más sólida en todo el estudio.



Fuente: Estudio de resultados en materia de seguridad

Figura 2: Efecto de la frecuencia de actualización técnica en la capacidad del programa de seguridad para mantenerse al día con los negocios

Le preguntamos a las organizaciones sobre la frecuencia de sus actualizaciones de seguridad y TI, y comparamos esas respuestas con la capacidad establecida de su programa de seguridad para estar al día con el negocio. ¿Existe una relación entre esas dos variables?

Sí, de hecho; descubrimos una mejora constante en este resultado clave a medida que aumentaba la cadencia de actualizaciones. **En general, las organizaciones que actualizan las tecnologías de seguridad y TI trimestralmente tienen un 30 % más de probabilidades de mantenerse exitosamente al día con el negocio que aquellas que solo actualizan cada algunos años.** Suena como un buen póster de motivación para los equipos de TI estresados: Manténgase actualizado y continúe.

1 En el informe, etiquetaremos las cifras con el valor "general" de una práctica o resultado en particular. Este valor representa el valor promedio entre todos los encuestados que respondieron a ese conjunto particular de preguntas. Se proporciona como referencia y debe usarlo como guía para comprender quién está mejor que el promedio y quién no está a la altura. También mostramos incertidumbre a través de barras de error o áreas sombreadas en algunos gráficos. Cuando esas áreas se superponen a la línea "General", significa que no podemos deducir que un aspecto particular de un programa de seguridad tenga algún efecto en el resultado o la práctica que estamos examinando.

¿Qué (o quién) debe impulsar los esfuerzos de actualización tecnológica?

Hemos establecido que las actualizaciones frecuentes contribuyen a habilitar el negocio, pero ¿qué (o quién) debe impulsar el proceso para realizar esas actualizaciones? Les pedimos a los encuestados que seleccionaran los principales impulsores de su organización para actualizar las tecnologías de seguridad, y sus respuestas se dividieron en tres grandes categorías:

- **Impulsado por el proveedor:** el programa lo determina un proveedor de SaaS o es parte de una iniciativa de consolidación de proveedores más grande (impulsor más común)
- **Proactivo:** en un programa predeterminado o cuando nuevas características o casos de uso justifican una actualización (la segunda más común)
- **Reactivo:** en respuesta a un incidente, cuando la tecnología queda obsoleta, o para satisfacer los requisitos de cumplimiento (menos común)

Estos factores son interesantes en sí mismos, pero lo que realmente queremos saber es si esos motivos se correlacionan con un enfoque más sólido de actualización tecnológica. La respuesta se encuentra en la Figura 3, que básicamente afirma que las iniciativas de actualización tecnológica son más exitosas cuando las manejan los proveedores (o al menos participan activamente en su implementación). **Menos de la mitad de las personas con un enfoque reactivo informan sólidas capacidades de actualización, en comparación con casi dos tercios de las que se sincronizan con los ciclos de actualización del proveedor.**

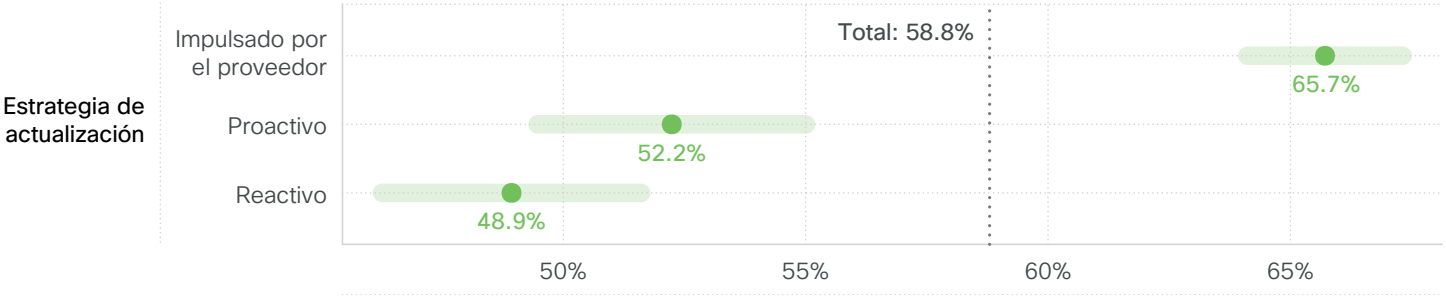


Figura 3: Efecto de los controladores principales para las actualizaciones en el rendimiento de la actualización de tecnología de seguridad

Lo entendemos: todo parece sospechoso si proviene de un proveedor de productos de seguridad y TI. Pero, sinceramente, no tuvimos ninguna influencia en este hallazgo. La encuesta fue realizada por una empresa de investigación independiente y de buena reputación, los encuestados no tenían idea de que Cisco patrocinó la encuesta y el respetado Instituto Cyentia analizó los datos para obtener lo que se ve en la Figura 3. Y, en buena medida, seremos muy cautelosos al interpretar estos resultados. Sospechamos que gran parte de las mejoras atribuidas a los enfoques impulsados por los proveedores en relación con las arquitecturas de nube / SaaS son más compatibles con las actualizaciones frecuentes. También notaremos que esto puede deberse menos a que los proveedores sean excelentes y más a evitar los obstáculos internos y los enredos políticos que tienden a impedir los programas de actualización técnica.

En palabras de Rob Base y DJ EZ Rock, "se necesitan dos para que todo salga bien. Se necesitan dos para estar fuera de la vista."¡Quién iba a saber que eran arquitectos de seguridad! Haga que su estrategia de actualización quede fuera de la vista aprovechando la inercia de sus partners de solución tecnológica para impulsar los resultados de la misión.

65.7% de las organizaciones se sincronizan con los ciclos de actualización del proveedor

¿Actualizar por capacidad o compatibilidad?

La sección anterior abordó qué situaciones impulsan a las organizaciones a actualizar las tecnologías, y ahora veremos por qué eligen una solución sobre otra. En la Figura 4, se transmite lo que los encuestados nos dijeron sobre sus criterios de selección. La integración clara con la tecnología existente es la clara preferencia, seguida de soluciones que ofrecen las mejores funcionalidades o que satisfacen necesidades particulares. Quizás sorprendentemente, minimizar costos ocupa el último lugar.

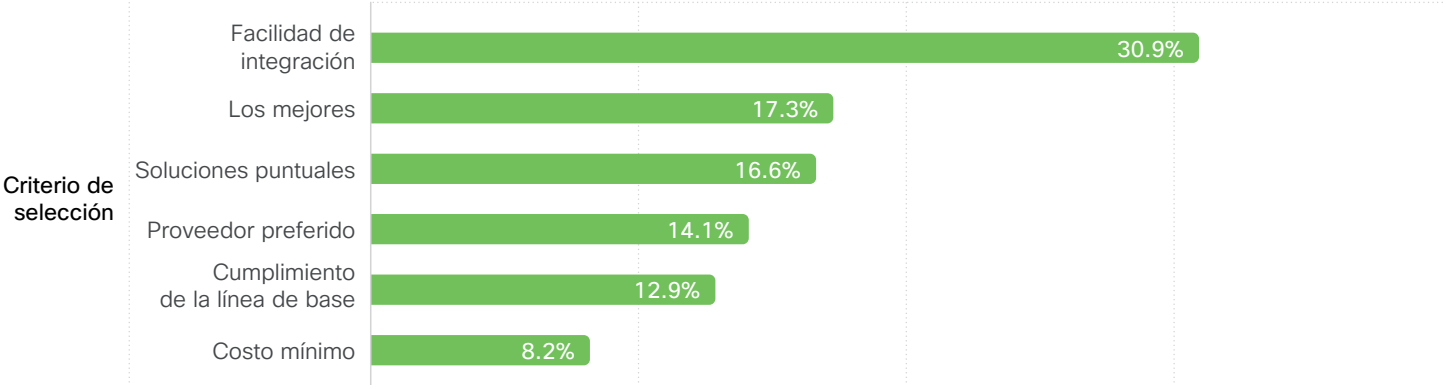


Figura 4: Efecto de los criterios de selección de productos de seguridad en el rendimiento de la actualización de tecnología de seguridad

- Eso está muy bien, pero, ¿importa algo de esto en cuanto al desarrollo de un programa de seguridad exitoso? Para responder a esto, agrupamos los criterios de selección de la figura 4 en tres categorías:
-

- **Mínimo:** solución de costo mínimo; Cumplimiento de la línea de base
- **Integración:** se integra con la tecnología existente; Uso de proveedores preferidos
- **Capacidad:** la mejor; Soluciones puntuales

Luego probamos estas categorías con una puntuación agregada creada para cada organización en función de su nivel de logro en los 11 resultados de seguridad. El valor absoluto de la puntuación no tiene un significado particular, pero proporciona un punto de comparación para las diferentes estrategias de actualización técnica. Como se muestra en la figura 5, **la priorización de la integración y las funcionalidades impulsan los resultados más que la selección de productos basados en la minimización de costos o el cumplimiento de los requisitos de cumplimiento de la línea de base. Pero un enfoque basado en la integración es el único que supera significativamente el promedio.**

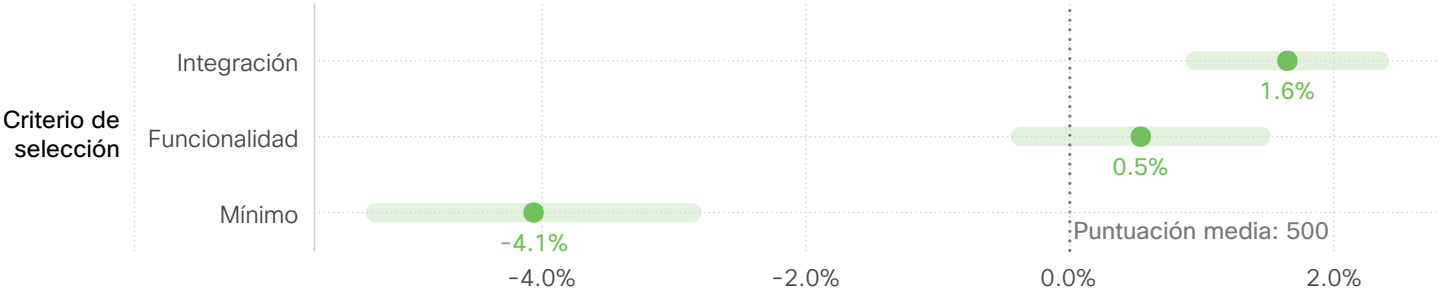


Figura 5: Efecto del criterio de selección de tecnología en la puntuación general de resultados de seguridad

Tenga en cuenta que las diferencias aquí son bastante pequeñas en cuanto al éxito general del programa. Y es probable que lo que realmente estamos viendo aquí sea una ventana a las prioridades y prácticas más amplias del programa de seguridad. Pero esto sugiere que vale la pena considerar cuestiones más sencillas, como por qué elegimos un producto sobre otro. Y si tiene dificultades para clasificar las funciones al actualizar las soluciones de seguridad, tome esto como una justificación razonable para impulsar la compatibilidad y la capacidad en lugar de minimizar el costo.

¿Cuál es la puntuación de los resultados de seguridad?

Les preguntamos a los encuestados sobre el nivel de éxito de su organización en 12 resultados de programas de seguridad diferentes. La primera edición del Estudio de resultados en materia de seguridad analizó estos detalles, y verá que algunos de ellos también se evalúan individualmente en este estudio. Pero también queríamos crear una puntuación agregada que capturara el nivel de logro de cada organización en los 12 resultados como una medida del rendimiento general del programa de seguridad. Nos referimos a eso como la "puntuación de resultados de seguridad", y verá que se hace referencia en este reporte varias veces.

Para obtener la puntuación, utilizamos una técnica de estadísticas sofisticada llamada "Teoría de respuesta al elemento". Esta técnica nos permite puntuar a las organizaciones según su desempeño en todos los resultados y, al mismo tiempo, tener en cuenta el hecho de que algunos resultados pueden ser más difíciles de lograr que otros. Esta técnica comprobada es la forma en que se crean las puntuaciones de las pruebas estandarizadas. El valor absoluto de la puntuación no tiene un significado particular, pero proporciona un punto de comparación entre los programas.

“Los CISO deben ser personas influyentes y educadores. Si queremos ser lo más eficaces posible, debemos estar a la vanguardia de las decisiones estratégicas que se toman en nuestras organizaciones. Pero mientras intentamos convencer a la gente de que la seguridad es importante, que necesitamos las inversiones adecuadas para hacerlo bien y que debemos participar en todos los aspectos del negocio, también debemos educar. La mayoría de los ejecutivos no tiene experiencia en seguridad, por lo que debemos informarles en cada paso sobre los tipos de riesgos que presentamos con cada decisión que tomamos.”

Helen Patton, Aasesora de CISO en Cisco @CisoHelen

Logro de tecnologías de seguridad bien integradas

Según nuestro último estudio de resultados de seguridad, las tecnologías de seguridad bien integradas que funcionan eficazmente con una infraestructura de TI más amplia contribuyen a la probabilidad de éxito de todos los resultados del programa. Hicimos una serie de preguntas diseñadas para profundizar en los factores detrás de esta hazaña encomiable, comenzando con las intenciones detrás de las integraciones de tecnología de seguridad.

Según los encuestados, el motivo más común para integrar tecnologías de seguridad es mejorar la eficiencia del monitoreo y la auditoría. Eso también resuena en nosotros, ya que estamos familiarizados con el dolor y la frustración de tener que revisar numerosas consolas o tableros para reconstruir algo de lo que sucede en la red. La colaboración y la automatización más sencillas también fueron factores de impulso comunes para la integración de tecnologías de seguridad (hablaremos sobre este último más adelante).

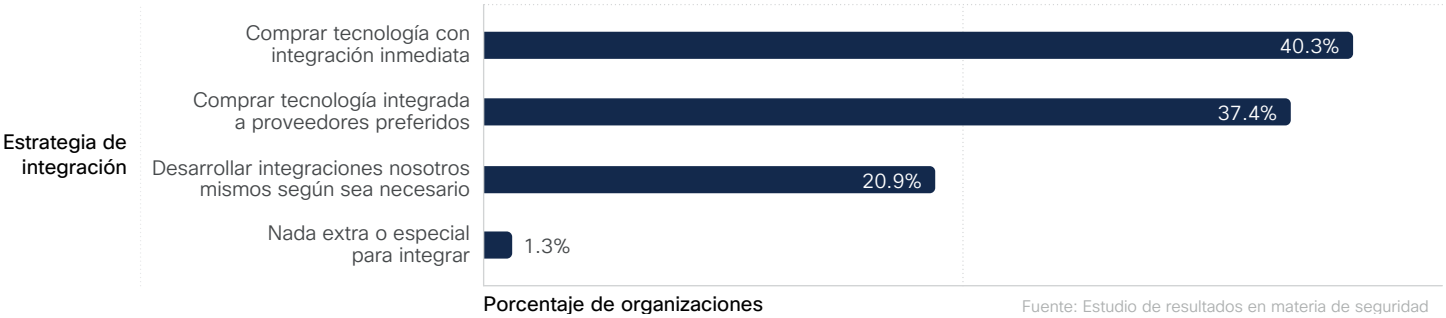
Probamos estas motivaciones con los niveles de integración de tecnología y los resultados del programa, pero la correlación no fue tan sólida. ¿Quizás “qué” o “cómo” es más importante que “por qué” al integrar tecnologías de seguridad? Analicemos un poco más este tema en las siguientes preguntas.

Según los encuestados, el motivo más común para integrar tecnologías de seguridad es mejorar la eficiencia del monitoreo y la auditoría.

¿Comprar o desarrollar para una tecnología bien integrada?

Gracias al estudio anterior, sabemos que la integración de tecnologías de seguridad genera resultados, pero ¿cuál es la mejor manera de lograr una pila tecnológica altamente integrada? ¿Adquirirla de esa manera? ¿Creada a medida? ¿Simplemente dejarla que surja? Veamos si podemos averiguarlo.

Le preguntamos a las organizaciones sobre su enfoque típico para la integración de la tecnología de seguridad, y las respuestas se incluyen en la Figura 6. **En general, más de tres cuartas partes de las organizaciones preferirían comprar soluciones integradas en lugar de crearlas** De esas organizaciones, casi el 40 % elige tecnologías que vienen con integraciones listas para usar en su infraestructura existente. Y cerca del 37 % va más allá y prefiere obtener soluciones de un único proveedor para que estén bien integradas de forma nativa o sean parte de una plataforma más grande. Poco más del 20 % está dispuesto a desarrollar la integración, siempre que el producto satisfaga sus necesidades. Pocos adoptan un enfoque de laissez-faire.



Fuente: Estudio de resultados en materia de seguridad

Figura 6: Enfoques comunes para la integración de tecnología de seguridad entre todas las organizaciones

En general, más de **3/4** de las organizaciones preferirían comprar soluciones integradas que construirlas.

En la Figura 7, se evalúa si alguno de estos enfoques de integración hace la diferencia. Aquí vemos nuevamente un tema que apunta a los beneficios de colaborar con proveedores para mantener la tecnología moderna y bien integrada. **Como se ve en el gráfico, seguir con un proveedor preferido tiene el doble de probabilidades de lograr tecnologías de seguridad bien integradas que un enfoque de no intervención (~ 69 % frente a ~ 29 %).** Además, según nuestra investigación, este hallazgo sigue siendo uniforme en todos los tamaños de organizaciones, si bien las pequeñas y medianas empresas tienen más beneficios por utilizar un proveedor preferido que las grandes empresas.

Y sí, sabemos que es otro hallazgo sospechosamente conveniente que proviene de una empresa con un amplio portafolio de seguridad integrado. Claro, nos complace ver que este resultado respalda la estrategia de Cisco... pero recordemos que este fue un estudio doble ciego y no manipulamos ese resultado en absoluto.

No es sorprendente que las organizaciones que no hicieron nada más para integrar tecnologías de seguridad se convirtieran en una profecía autocumplida. **Sin embargo, esperamos que algunos se sorprendan al saber que prácticamente no hay diferencia entre los que compran productos con integraciones listas para usar y los que crean integraciones por su cuenta. Poco menos de la mitad (~ 49 %) de las organizaciones que utilizan cada uno de estos enfoques informan niveles sólidos de integración.**

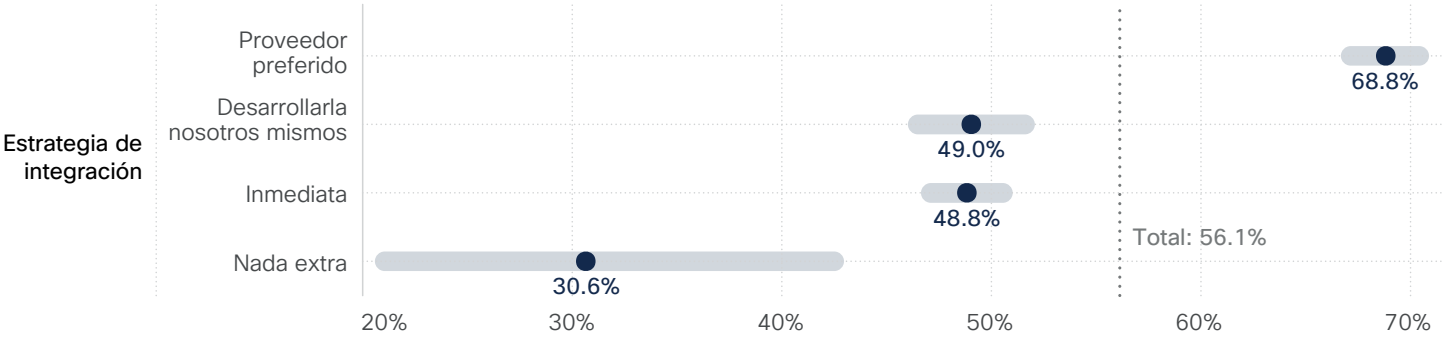


Figura 7: Efecto de los enfoques comunes de integración en el nivel de integración de la tecnología de seguridad

Con nubes, con posibilidades de integración

Muchas organizaciones nos preguntaron si debían comenzar (o ampliar) sus esfuerzos de integración de tecnología de seguridad en entornos en la nube o en las instalaciones. Si ese es su caso, tenemos algunos datos que podrían ayudar en esa evaluación. La buena noticia es que muchos encuestados informan buenos resultados tanto en entornos en las instalaciones como en la nube. Dicho esto, parece mucho más fácil lograr una sólida integración tecnológica en la nube.

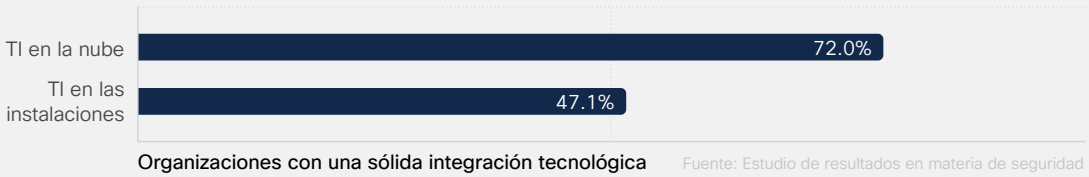


Figura 8: Efecto de la nube frente a los entornos en las instalaciones en el nivel de integración de la tecnología de seguridad

¿La integración ayuda a la automatización?

Volviendo al inicio de esta sección, la automatización no es la motivación más común para la integración tecnológica. Pero el 44 % de las organizaciones lo identificó como un incentivo. Dejando los motivos a un lado, ¿hay evidencia de que las tecnologías bien integradas realmente permiten una mejor automatización de los procesos de seguridad? La evidencia presentada en la Figura 9

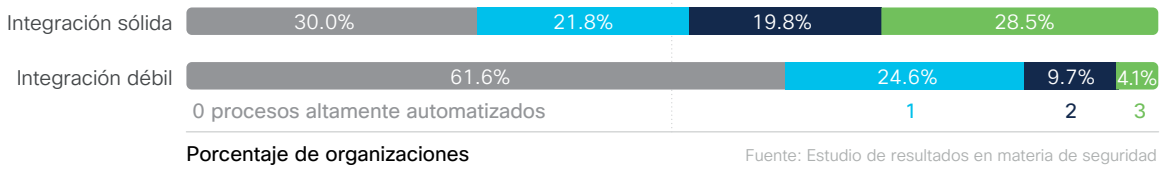


Figura 9: Efecto de la integración tecnológica en el alcance de la automatización de procesos de seguridad

Las dos barras horizontales en la Figura 9 distinguen a las organizaciones en función de su nivel de integración de tecnología de seguridad (fuerte frente a débil). Los segmentos de color representan la cantidad de procesos de seguridad principales (monitoreo de eventos, análisis de incidentes y respuesta a incidentes) admitidos por una automatización madura. La proporción de organizaciones sin automatización es más del doble que entre las organizaciones con integración débil. **Por el contrario, aquellos con tecnologías de seguridad bien integradas eran siete veces más propensos a alcanzar altos niveles de automatización para estos tres procesos (4,1 % frente a 28,5 %).** ¡Eso suena como una motivación convincente!

¿Qué funciones deben integrarse?

A continuación, preguntamos a los encuestados sobre su nivel de integración entre tecnologías que admiten las cinco funciones principales del Marco de Ciberseguridad (CSF) de NIST. Respondieron en una escala que va desde muy fragmentada (tecnologías aisladas que funcionan principalmente de forma aislada) hasta altamente integrada (tecnologías coordinadas que funcionan como una unidad funcional). Luego creamos un modelo para determinar el efecto en la puntuación de los resultados de seguridad generales para cada organización.

Los resultados en la Figura 10 son bastante consistentes en las cinco funciones. **Trabajar para desfragmentar e integrar cualquiera de las áreas funcionales de CSF de NIST corresponde a un aumento en el éxito del programa de seguridad (+ 11 % a 15 %).** Por lo tanto, la respuesta a nuestra pregunta principal es "todas". Pero una función altamente integrada de "identificación" ofrece el mayor impulso si se está preguntando por dónde comenzar.

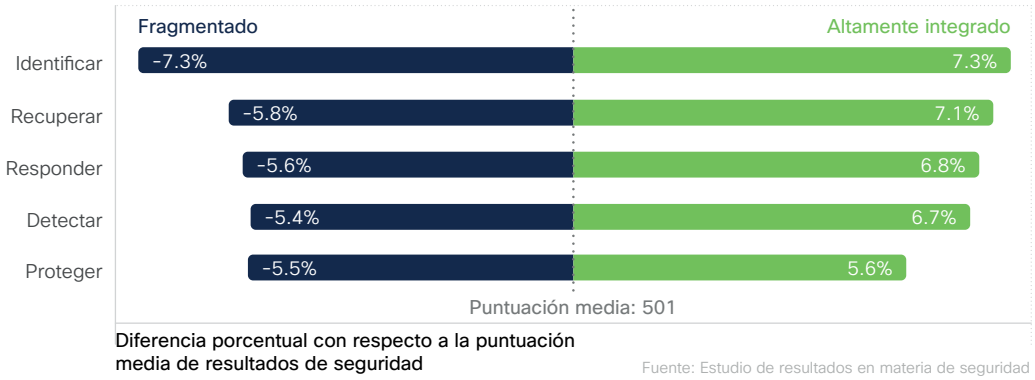


Figura 10: Efecto de la integración de funciones de CSF de NIST en la puntuación de resultados de seguridad general

No podemos evitar ver una conexión entre este hecho y lo que aprendimos en la sección anterior sobre el monitoreo, la auditoría y la colaboración como el motor más fuerte para la integración de la tecnología. Juntos, parecen defender la importancia fundamental de una buena visibilidad en toda la empresa. Ciertamente tiene sentido que un enfoque fragmentado para "desarrollar una comprensión de la organización para administrar el riesgo de ciberseguridad de los sistemas, las personas, los activos, los datos y las capacidades" (lenguaje CSF) no termine bien. Verán este tema reforzado a medida que avancemos en la sección Detección de amenazas y respuesta a incidentes.

Acerca de la integración, la identificación y la información

Además del gráfico que acabamos de analizar, los datos de este estudio apuntan constantemente a la relación crucial entre integración, identificación e información. Si no puede identificar un activo o una amenaza, no sabrá que está allí y, por lo tanto, no se preocupará lo suficiente como para establecer una defensa informada hasta que sea demasiado tarde.

La Figura 11 ilustra bien este concepto. Comparamos el nivel de integración informado de cada organización dentro de la función "Identificar" de CSF de NIST con su capacidad para detectar con precisión las amenazas de manera oportuna. Las organizaciones con sistemas altamente integrados para identificar recursos y riesgos críticos contaban con capacidades de detección de amenazas mucho más sólidas (más del 41 %). Por lo tanto, en un sentido real, la fragmentación de la lucha y los adversarios van de la mano.

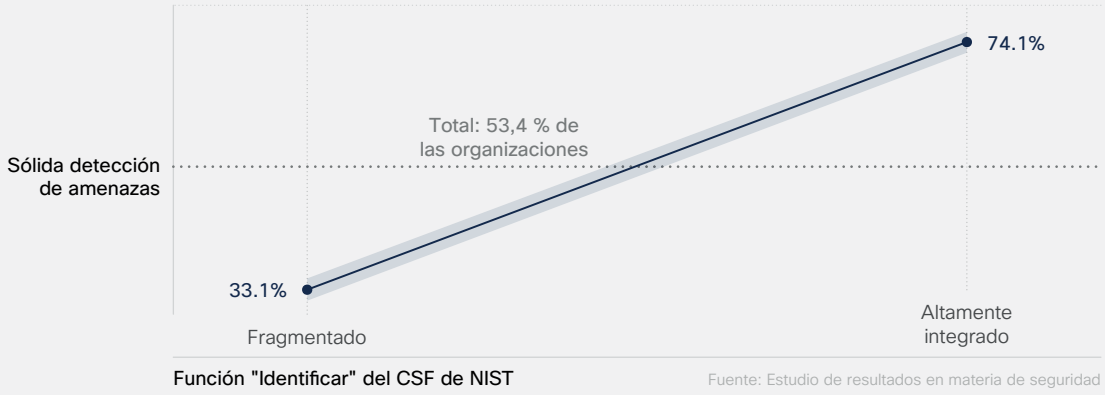


Figura 11: Efecto de la integración de la función Identificar de CSF de NIST en las capacidades de detección de amenazas

+41% de organizaciones con sistemas altamente integrados para identificar los activos y riesgos críticos tenían capacidades de detección.

“La automatización permite que nuestros ingenieros reaccionen a las amenazas emergentes de manera oportuna. Ahora podemos centrarnos en transmitir los conceptos de seguridad correctamente en lugar de actualizar continuamente las reglas y monitorear la red las 24 horas, los 7 días de la semana. Cisco se mete en las malezas y extrae la información que necesitamos para poder hacer un mejor trabajo en cuanto a la protección y el mantenimiento de nuestra infraestructura. Nos ha proporcionado la combinación perfecta de máquinas e inteligencia humana.”

Steve Erzberger, director de tecnología de Frankfurter Bankgesellschaft (Schweiz), AG

Más información

Desarrollo de capacidades de detección de amenazas y respuesta a incidentes

Esta sección abarca dos áreas separadas de práctica de seguridad que hicieron los fabulosos cinco por derecho propio. Pero debido a que la detección de amenazas y la respuesta a incidentes (IR) a menudo comparten personas, procesos y tecnologías en el marco de las operaciones de seguridad (SecOps), planteamos un conjunto de preguntas comunes entre ellas. Por lo tanto, tiene sentido analizarlos dentro de la misma sección para este estudio.

Casi todas (aproximadamente el 92%) de las organizaciones con personas, procesos y tecnología sólidos logran anticipar amenazas con capacidades de detección y respuesta.

¿Priorizar a las personas, los procesos o la tecnología?

Hablando de personas, procesos y tecnología, comencemos nuestra investigación allí. Las funciones de seguridad a menudo se describen como una combinación de los tres elementos, particularmente en el dominio de la detección de amenazas y la respuesta a incidentes. Pero, ¿hay alguna parte de esta trinidad de seguridad que sea más crítica que las demás? Usted sabe a dónde va esto; vayamos al análisis.

A partir del final de la figura 12, vemos que solo alrededor de una cuarta parte de los programas que carecen de solidez en todas las facetas de la tríada de p-p-t expresa confianza en su SecOps. Obtener fortaleza en cualquier área (personas, procesos o tecnología) aumenta ese porcentaje entre un 60 % y un 64 %, según el área. Las personas fuertes parecen conceder una ligera ventaja, pero los intervalos de confianza superpuestos advierten sobre hacer mucho hincapié en ese hecho. La conclusión importante es que cualquiera de estos ofrece un buen punto de partida para desarrollar mejores capacidades de detección y respuesta.

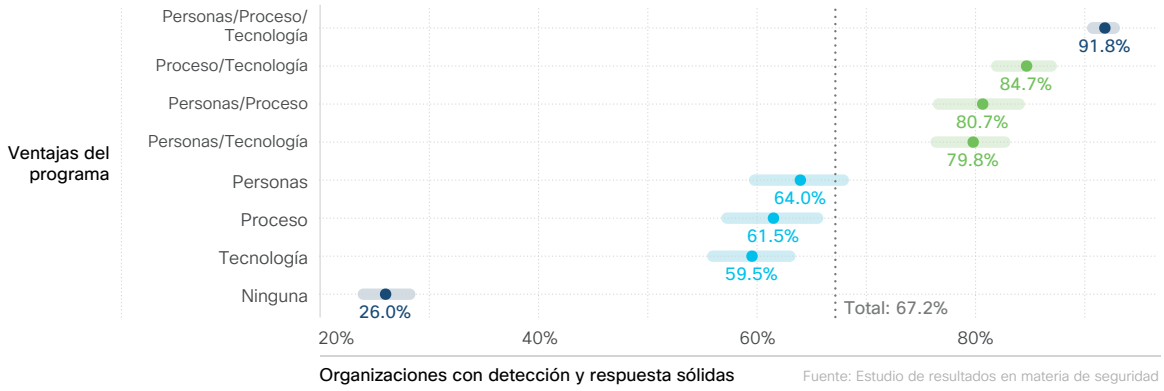


Figura 12: Efecto de las personas, los procesos y la tecnología fuertes en la detección de amenazas y las capacidades de respuesta a incidentes

Continuando con la Figura 12, hacer dos cosas bien pone a los programas de SecOps por encima del promedio y mejora las capacidades entre un 15 % y un 20 % con respecto a los que hacen bien una cosa. Una vez más, realmente no importa qué pares de personas, procesos o tecnología elija. Solo necesita fortaleza en cualquiera de los dos. Es bueno saber que hay cierta libertad de elección para adaptar el plan de SecOps de su organización, ¿no?

Y eso nos lleva a los programas de elite en la Figura 12 que logran alcanzar la trifecta SecOps. **Casi todas (alrededor del 92 %) de las organizaciones con personal, procesos y tecnología fuertes logran capacidades avanzadas de detección y respuesta ante amenazas. ¡Es un aumento de rendimiento 3,5 veces mayor en comparación con los programas de SecOps que no funcionan correctamente!** Por lo tanto, comience donde sea que pueda avanzar más, pero no se detenga hasta llegar a la cima de p-p-t

¿Zero Trust y SASE permiten mejores SecOps?

Comprendemos que los descriptores abstractos, como “tecnología fuerte”, dificultan la obtención de conclusiones concretas de los hallazgos anteriores. Es por eso que planteamos un par de preguntas de seguimiento sobre arquitecturas específicas. Les preguntamos a los encuestados sobre su adopción del perímetro de servicio de acceso seguro (SASE) y Zero Trust para comprender mejor cómo esos enfoques afectan la detección de amenazas y las capacidades de respuesta a incidentes (y, por lo tanto, los resultados del programa de seguridad).

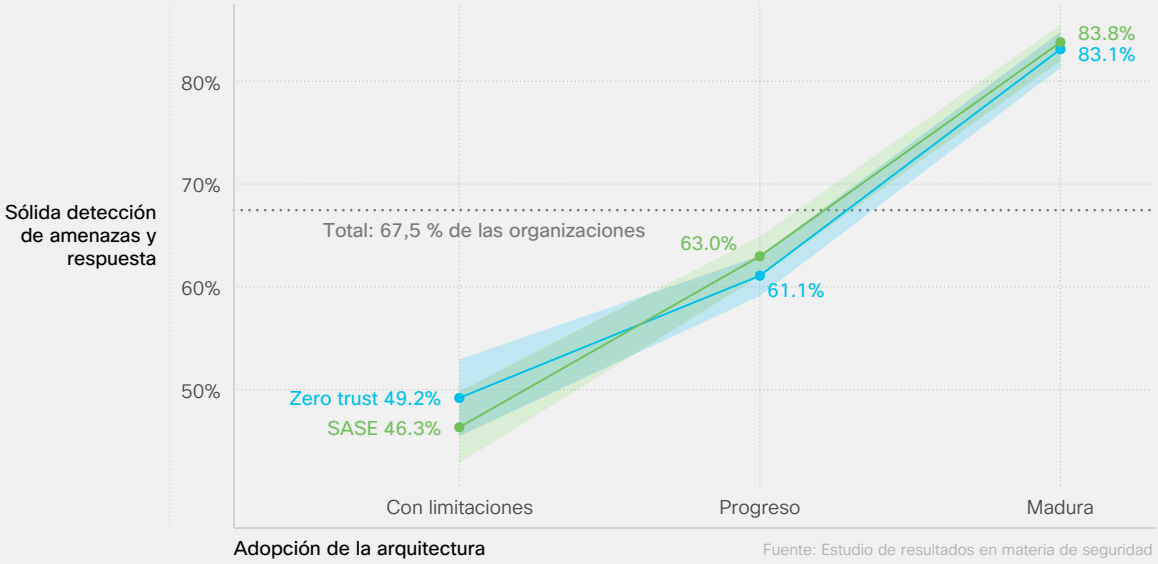


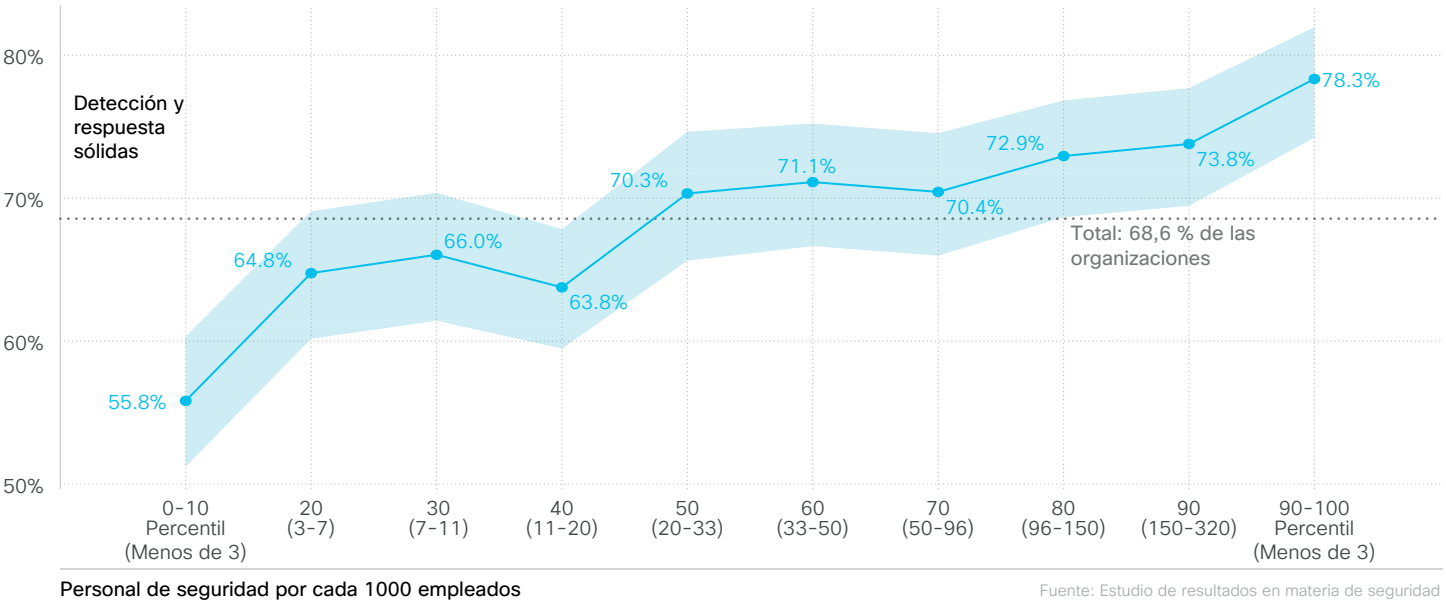
Figura 13: Efecto de arquitecturas de Zero Trust (izquierda) y SASE (derecha) en las capacidades de detección de amenazas y respuesta a incidentes

Las organizaciones que afirman tener implementaciones maduras de Zero Trust o SASE tienen aproximadamente un 35 % más de probabilidades de reportar SecOps fuertes que aquellas con implementaciones incipientes. Estos resultados corroboran la evidencia que compartimos anteriormente sobre los muchos beneficios que las arquitecturas modernas pueden aportar a los programas de ciberseguridad.

¿Más cabezas significan menos dolores de cabeza?

De la última pregunta, sabemos que las buenas personas son importantes para desarrollar capacidades sólidas de detección de amenazas y respuesta a incidentes. Pero, ¿es mejor centrarse en agregar más personas o aumentar las habilidades de las personas que tiene? Obviamente, eso no tiene por qué ser mutuamente excluyente, pero la pregunta sigue siendo: ¿vemos alguna evidencia de que la cantidad o la calidad es más importante cuando se trata de desarrollar equipos SecOps exitosos?

Para responder a esto, primero calculamos la relación entre el personal de SecOps y el total de empleados de todas las organizaciones. Luego, comparamos esa relación con la fortaleza reportada de las capacidades de detección y respuesta. En la Figura 14, se muestra el resultado de esos cálculos y, si bien no se responde completamente a la cuestión de la cantidad o la calidad, se ofrecen algunas conclusiones.



Fuente: Estudio de resultados en materia de seguridad

Figura 14: Efecto de la proporción del personal de seguridad en la detección de amenazas y las capacidades de respuesta ante incidentes

El primero de ellos es que las proporciones de personal de seguridad se correlacionan con una mejor detección y respuesta ante amenazas. Las organizaciones con la proporción más alta tienen un 20 % más de probabilidades de reportar capacidades más sólidas que las organizaciones con la proporción más baja. PERO, ¿ve cómo la línea de puntos que marca el promedio general atraviesa gran parte del intervalo de confianza sombreado en la Figura 14? Eso básicamente significa que las organizaciones que no están en los extremos de la escala de personal (la mayoría de ellas) tienen las mismas probabilidades de reportar programas sólidos de SecOps.

¿Qué significa todo eso en realidad? Bien, podemos decir con confianza que las organizaciones con grandes equipos de seguridad son significativamente más propensas a lograr capacidades sólidas de detección y respuesta que aquellas con personal mínimo. Pero el personal solo no hará que todos sus dolores de cabeza de SecOps desaparezcan ni garantizará el éxito. Además, incluso las diferencias entre la proporción de personal más baja y la más alta no tienen en cuenta el aumento del rendimiento asociado con tener recursos humanos fuertes que mencionamos la sección anterior. **Por lo tanto, podemos deducir que la calidad es igual de importante (quizás incluso más) que la cantidad a la hora de crear equipos fuertes de detección y respuesta ante amenazas.**

Los equipos de seguridad continúan enfrentando una grave escasez de personal.

Con recursos reducidos y amenazas cada vez mayores, muchos profesionales de ciberseguridad están experimentando un estrés y un agotamiento extremos. ¿Qué medidas proactivas podemos tomar para ayudar a su bienestar? En este eBook, pedimos a los líderes y profesionales del sector que compartan sus conocimientos e historias sobre el manejo de la salud mental.

Personal de SecOps: ¿suyo, mío o nuestro?

Entonces, el éxito de SecOps no se trata solo del personal, sino que los modelos de dotación de personal afectan los resultados. En igualdad de condiciones, ¿es mejor subcontratar, contratar o compartir responsabilidades de detección y respuesta ante amenazas? Veamos cómo los datos responden a esa pregunta, pero tenga en cuenta que en cierto modo habla por los dos lados en este caso.

Les preguntamos a los encuestados sobre sus modelos de dotación de personal y luego lo comparamos con la calificación de sus capacidades de detección y respuesta. Como se muestra en la figura 15, las organizaciones con equipos predominantemente contratados o subcontratados eran mucho más propensas (más del 20 % a 30 %, respectivamente) a reportar programas sólidos de SecOps que aquellas con un modelo de dotación de personal mixto. Dado que la mayoría de las organizaciones afirmó que usaba algún tipo de modelo mixto, pensamos que valdría la pena ver esto desde una perspectiva diferente antes de condenarlas a todas al fracaso solo porque la encuesta (parece indicar) indica este resultado.

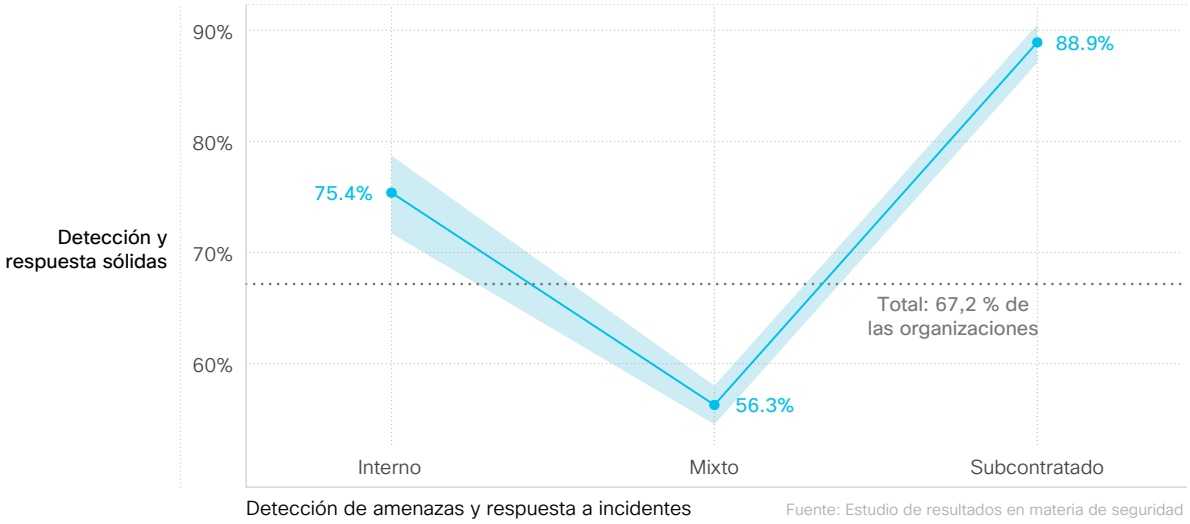


Figura 15: Efecto de los modelos de dotación de personal sobre la detección percibida de amenazas y las capacidades de respuesta a incidentes

Las organizaciones con equipos predominantemente internos o subcontratados tienen

20 to 30%

más probabilidades que aquellas con un modelo de dotación de personal mixto para informar sólidos programas SecOps.

Además de pedir a los encuestados que calificaran la fortaleza percibida de las capacidades de detección y respuesta, también intentamos obtener métricas más objetivas para la comparación. Uno de ellos es el tiempo medio de respuesta (MTTR), o el tiempo promedio para corregir o contener un incidente de seguridad. En nuestro análisis de antecedentes fuera de este reporte, estas métricas tienden a coincidir direccionalmente con las evaluaciones subjetivas. Pero las dos perspectivas se contradecían en este caso, como se ve en la figura 16.

Figura 16: Efecto de los modelos de dotación de personal en el tiempo promedio para responder a incidentes de seguridad

Según la versión de la Figura 16, las organizaciones con equipos internos de detección y respuesta a amenazas disfrutan de un MTTR que es menos de la mitad que el de los modelos subcontratados (aproximadamente 6 días frente a 13 días). **Las personas con modelos de dotación de personal híbridos se ubican en el medio (aproximadamente 8 días), con MTTR que no son tan rápidos como los equipos internos, pero mucho más rápido que sus contrapartes en su mayoría subcontratadas.**

Obviamente, tenemos un poco de dilema aquí. Qué medida (perspectiva vs. métrica) es la correcta y, lo que es más importante, cuál debe escuchar al tomar decisiones de abastecimiento. Vamos a ser intencionalmente dudosos aquí y decir "ambos" y "ninguno" (bueno, no nos culpen por seguir el ejemplo conflictivo de los datos aquí).

Por supuesto, la corrección tiene muchos elementos y dependencias. La organización puede depender de un proveedor para emitir un parche/corrección de errores para resolver completamente una vulnerabilidad. Ese parche luego debe probarse en el laboratorio en su entorno antes de implementarse en producción. Baste decir que hay muchas partes móviles involucradas.

En verdad, es difícil saber con certeza qué está sucediendo aquí. Quizás intentar recopilar métricas a través de una encuesta sea engañoso. Tal vez las calificaciones de MTTR y de capacidad son lo suficientemente diferentes como para que sea posible tener un programa de detección y respuesta "sólido" en general, pero tasas de corrección más lentas. Quizás esos programas son más lentos porque son más exhaustivos. Tal vez la coordinación con el personal subcontratado solo lleve más tiempo. Tal vez haya una sensación de confianza porque "estamos pagando a los expertos para que hagan esto y ellos lo tienen cubierto". Tal vez estamos viendo una versión de SecOps del efecto Dunning-Kruger. Probablemente sea todo esto y más. Y debido a eso, sugerimos utilizar esta sección para generar debates en lugar de tomar decisiones.

2 Utilizamos la media geométrica en este gráfico, ya que es más representativa de un valor "típico". El MTTR informado generalmente fue de menos de 2 a 3 semanas, pero ocasionalmente los encuestados reportaron meses (o años). El uso de la media geométrica logra representar mejor el valor "típico" sin verse sesgado por esos valores extremadamente altos.

¿Es inteligente usar la inteligencia?

Hablando del efecto Dunning-Kruger, es una configuración perfecta para esta sección. Les preguntamos a los encuestados sobre el uso de la inteligencia de amenazas cibernéticas en su programa SecOps. La mayoría de las organizaciones (85 %) afirma que utiliza la inteligencia en algún nivel, pero menos de un tercio (31 %) afirma que la utiliza ampliamente. ¿Esa inteligencia conduce a una mejor y más rápida detección y respuesta ante amenazas? Bien, veamos la Figura 17.

Curiosamente, la mayoría de las organizaciones que no utilizan inteligencia de amenazas parece pensar que les está yendo bastante bien. Aquí me viene a la mente el viejo dicho de "la ignorancia es una bendición", especialmente porque sumergirse un dedo del pie en las aguas de la inteligencia aparentemente disipa esas nociones (84 % a 46 % de confianza). Las organizaciones que hacen un uso extensivo de la inteligencia de amenazas tienen casi el doble de probabilidades de reportar capacidades sólidas de detección y respuesta en comparación con las que menos la usan. Y en un ejemplo en el que las métricas y las calificaciones de la capacidad coinciden, las que aprovechan más la inteligencia alcanzan un MTTR que es aproximadamente la mitad que el de los usuarios que no utilizan la inteligencia.

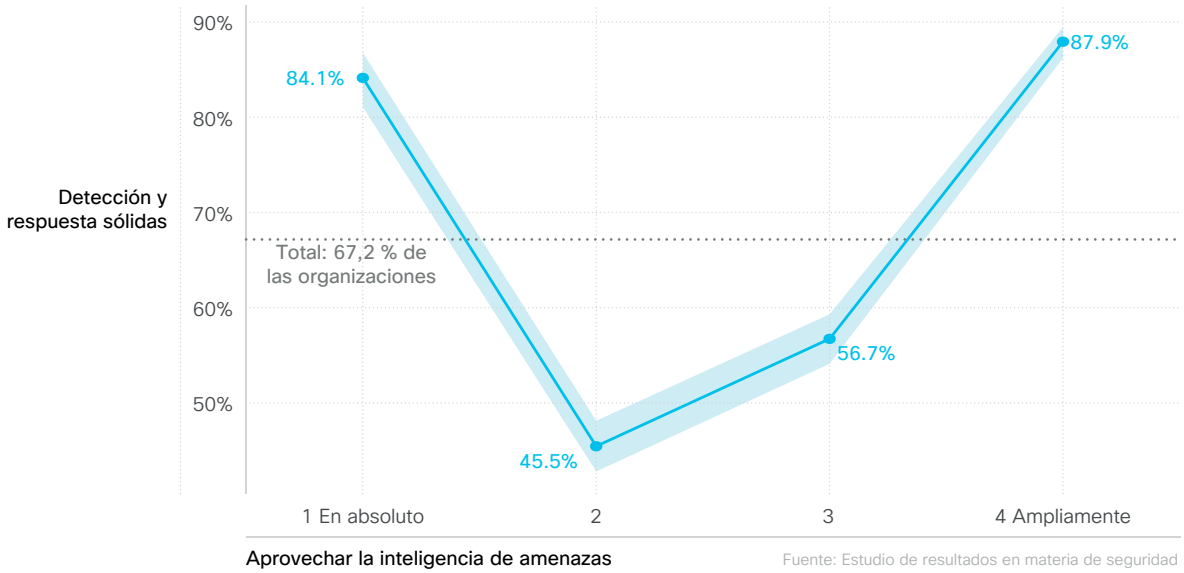


Figura 17: Efecto del uso de la inteligencia cibernética en las capacidades de detección de amenazas y respuesta a incidentes

El psicólogo y autor de best-sellers Daniel Kahneman dijo una vez: "Estamos ciegos a nuestra propia ceguera. Tenemos muy poca idea de lo poco que sabemos". En la figura 17, se sugiere que una vez que las organizaciones conocen un poco las amenazas en su contra, se dan cuenta de que hay muchas cosas que no saben. Con un uso más extenso de la inteligencia de amenazas, se comienza a recuperar esa confianza, excepto que ahora no tan ciegamente.

Las organizaciones que hacen un uso extensivo de la inteligencia de amenazas tienen **2X** casi la misma probabilidad de reportar una detección sólida y capacidades de respuesta

¿Es la automatización un sustituto de las personas?

Después de leer este título, es posible que haya asumido que era una pregunta retórica. No tan rápido. A riesgo de provocar la indignación de toda la comunidad de seguridad, vamos a ponernos a prueba (datos) para sugerir que la automatización puede, de hecho, reemplazar a las personas. PERO, siga leyendo antes de decidir eliminar este reporte y agregarnos a su lista de contactos bloqueados. <deep breath>

En la Figura 18, se incorporan elementos que ha visto antes en gráficos separados: personal de seguridad y automatización. Las dos líneas comparan dos tipos diferentes de programas de SecOps. La primera (línea naranja) representa a las organizaciones que NO cuentan con recursos humanos fuertes, mientras que las que sí disfrutan de ese lujo están representadas por la línea azul. En ambos casos, moverse de izquierda a derecha muestra el efecto del aumento de los niveles de automatización en la detección de amenazas y las capacidades de IR.

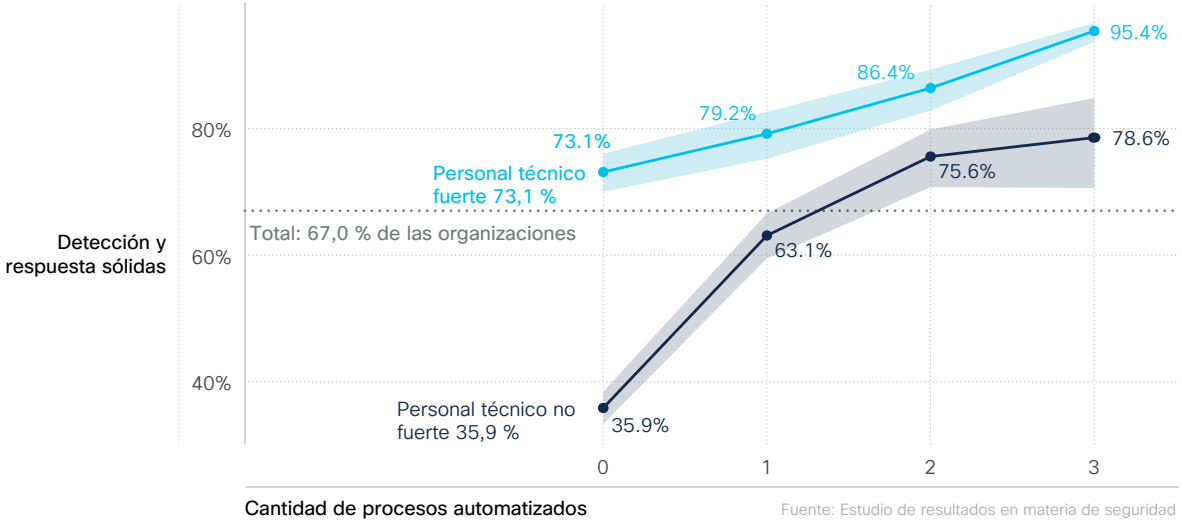


Figura 18: Efecto de la dotación de personal y la automatización en las capacidades de detección de amenazas y respuesta a incidentes

Comencemos con lo que no tienen. Solo alrededor de un tercio de las organizaciones que carecen de personal de seguridad fuerte y no automatizan ningún proceso importante reporta capacidades sólidas de detección y respuesta. Eso salta mucho cuando una de las tres áreas de proceso que investigamos (monitoreo de amenazas, análisis de eventos, respuesta a incidentes) está automatizada. Automatizar dos de estos aumenta aún más el valor y automatizar los tres supera el doble del rendimiento del personal con menos experiencia. **Más de tres cuartas partes de los programas de SecOps que no cuentan con recursos de personal fuertes aún pueden lograr capacidades sólidas a través de altos niveles de automatización.**

Ahora observe o siga con el dedo el recorrido desde el punto más a la derecha en la línea naranja hasta el primer punto de la línea azul. ¿Captó la implicación? **Un programa de SecOps con un personal más débil que emplea tasas de automatización avanzadas casi iguales que uno con un personal fuerte y una automatización deficiente.** O dicho de otra manera, una automatización sólida puede sustituir a un personal fuerte. Vea, ¡no le mentiríamos!

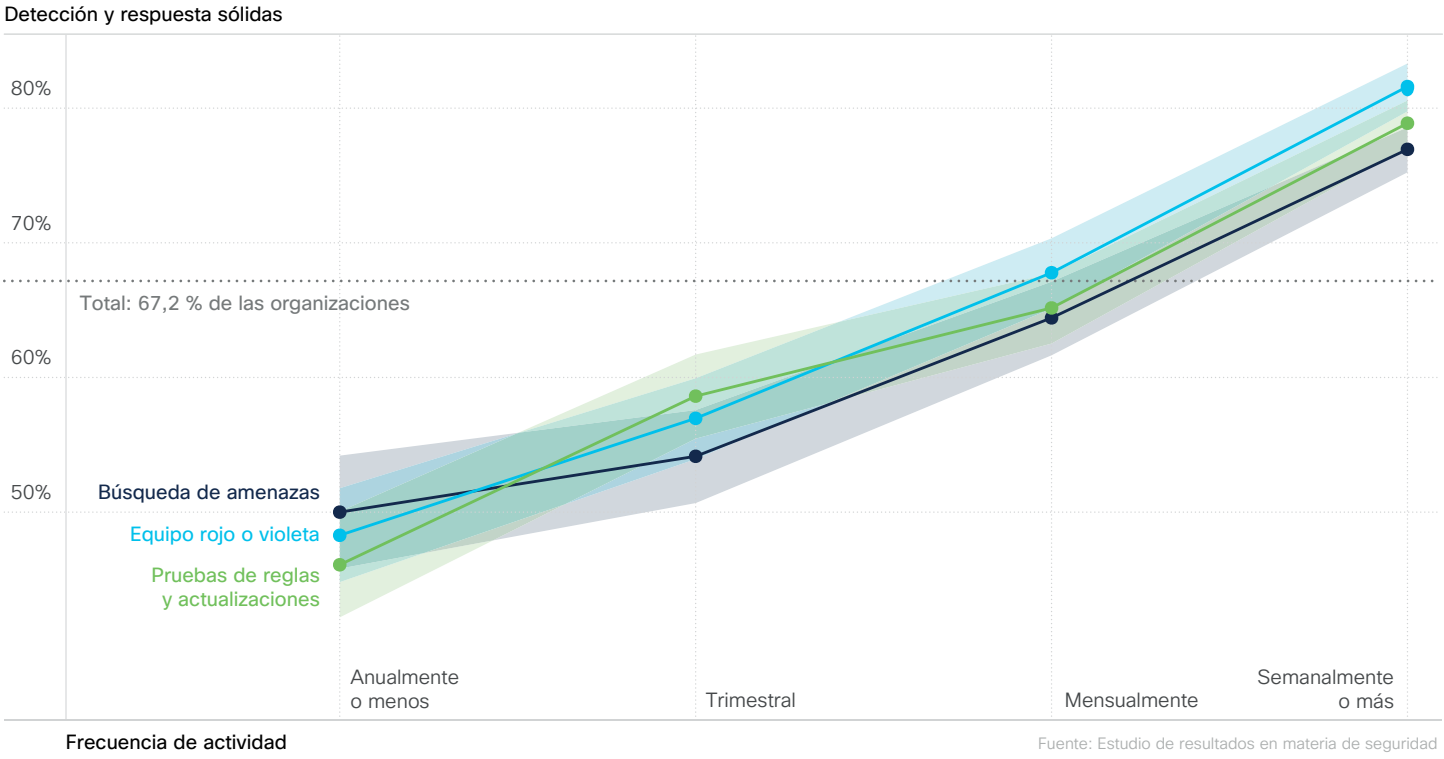
Pero el hombre contra la máquina no es realmente el punto principal o la lección más importante de la Figura 18. Seguir la línea azul a través de los sucesivos niveles de automatización proporciona una justificación muy convincente para alcanzar ambos objetivos. **Los programas de seguridad que logran armar un equipo fuerte Y automatizan los principales procesos de detección y respuesta ante amenazas tienen casi garantizado (más del 95 %) el éxito de SecOps.** Por lo tanto, no utilice la automatización como sustituto de una fuerza laboral con talento. Utilícela para aumentar su talento y permitirles centrarse en actividades de alta prioridad.

¿Con qué frecuencia debemos ajustar, hackear y detectar?

Uno podría nombrar cualquier cantidad de actividades recurrentes que podrían mejorar los programas de detección y respuesta ante amenazas. En una encuesta informal en la que abordamos este tema, se recomendaron tres más que ningún otro:

- Prueba y actualización de reglas de detección y casos de uso
- Búsqueda proactiva de señales de actividad maliciosa
- Participación en ejercicios de equipo rojo o violeta

Les preguntamos a los encuestados con qué frecuencia sus organizaciones realizan cada una de esas actividades y luego lo comparamos con la solidez de las capacidades de detección y respuesta ante amenazas. La tendencia resultante que se muestra en la Figura 19 no podría ser más clara.



Fuente: Estudio de resultados en materia de seguridad

Figura 19: Efecto de la frecuencia de actividad en las capacidades de detección de amenazas y respuesta a incidentes

El ajuste de reglas, la formación de equipos rojo/violeta y la detección de amenazas siguen una trayectoria similar. Cuanto más finalice, más se beneficiarán con los programas de SecOps. Las organizaciones que las realizan al menos una vez por semana ven un aumento de rendimiento de aproximadamente el 30 % en comparación con las que lo hacen anualmente o menos. Entonces, ¿con qué frecuencia debe hacerlo su organización? La respuesta simple es “cuanto más frecuente, mejor”.

Organizaciones que realizan estas actividades al menos una vez a la semana ven un **30%** aumento en el rendimiento.

"La seguridad cambia todo el tiempo y debemos seguir estas tendencias de seguridad. [Anteriormente], perdíamos mucho tiempo en la resolución de incidentes y problemas de seguridad. Ahora que hemos simplificado nuestro proceso y ahorrado tiempo durante las investigaciones, podemos seguir las nuevas tendencias de seguridad e integrar nuevas soluciones de seguridad para proporcionar una infraestructura más segura para nuestra red educativa."

Bahruz Ibrahimov, ingeniero sénior de seguridad de la información en AzEduNet

Más información

Garantizar una pronta recuperación ante desastres y recuperabilidad

Es interesante ver cómo lo más importante de diferentes aspectos de la ciberseguridad se filtra y fluye con el tiempo. Después de pasar a un segundo plano respecto de las vulneraciones de datos y el espionaje cibernético durante varios años, el tema de la continuidad del negocios y la recuperación tras desastres (BCDR) vuelve a ser un tema central. Y hay buenas razones para ello. El ransomware desenfrenado, las interrupciones de los principales proveedores de hosting, etc. han forzado cambios importantes en las estrategias para garantizar la recuperabilidad ante las amenazas incesantes.

El estudio de resultados en materia de seguridad de 2021 clasificó la pronta recuperación tras desastres como el cuarto factor más importante para desarrollar programas de ciberseguridad exitosos. Mostró correlaciones significativas con los 11 resultados excepto uno (cultura de seguridad). Con esto en mente, analicemos las estrategias para maximizar la eficacia de esta práctica y garantizar la recuperabilidad.

Ransomware desenfrenado, interrupciones de importantes proveedores de hosting, etc., han obligado cambios importantes en las estrategias para garantizar la resiliencia frente a amenazas incesantes.

¿La recuperación tras desastres debe tener supervisión en el nivel de la junta directiva?

Teníamos curiosidad por saber quién tenía la supervisión final de las capacidades de recuperación tras desastres. Resulta que la responsabilidad se detiene de manera bastante uniforme con el CIO, el CISO y otros miembros no pertenecientes a TI de la alta gerencia, y aproximadamente un cuarto de los procesos de BDCR de las organizaciones reporta a cada uno. La visibilidad en el nivel de la junta directiva es un poco menos común que esas, pero aún está presente en el 18 % de las organizaciones en nuestra encuesta.

Cuando comparamos estas respuestas con la evaluación de cada encuestado sobre la continuidad de su negocio y las capacidades de recuperación tras desastres, se hizo evidente que la cuestión de la supervisión no es solo una curiosidad. **Según la Figura 20, las organizaciones con supervisión de BCDR en el nivel de la junta directiva son las más propensas (11 % por encima del promedio) a reportar que tienen programas sólidos.** Las funciones de continuidad del negocio y recuperación tras desastres que se completaron con el CIO exhiben las tasas más bajas que son significativamente inferiores al promedio.

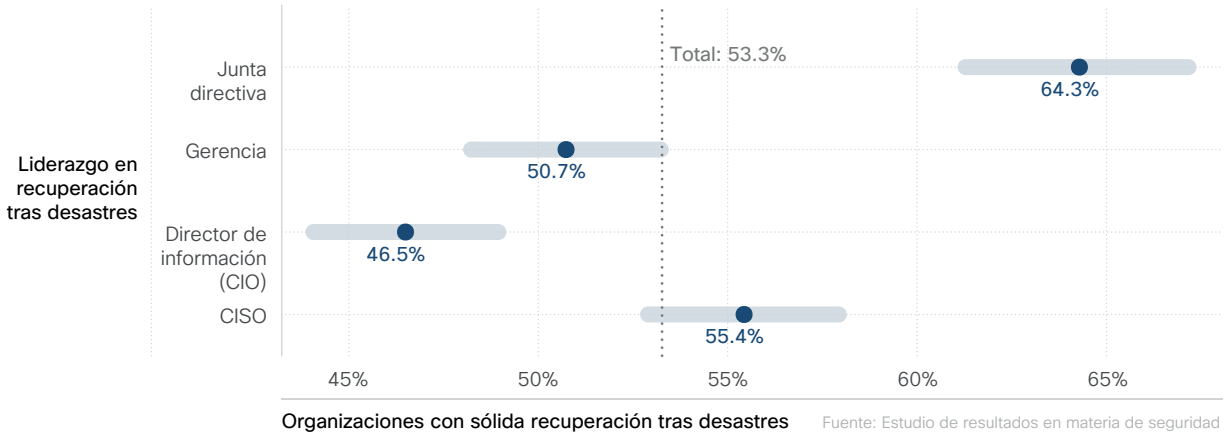


Figura 20: Efecto de la supervisión de la organización de alto nivel en las capacidades de recuperación tras desastres

Hay muchas explicaciones posibles para los resultados que se muestran en la Figura 20. Sospechamos que las organizaciones que responden a la junta sobre asuntos de recuperación tras desastres probablemente hayan aumentado las preocupaciones sobre el riesgo operativo y la recuperabilidad. Esas preocupaciones probablemente se traduzcan en una supervisión más estricta, un soporte más sólido y mayores presupuestos. Por lo tanto, si su organización tiene dificultades para mejorar las capacidades de recuperación tras desastres, podría tener sentido desarrollarlas de arriba hacia abajo y no de abajo hacia arriba.

¿Qué sucede con la operación diaria de recuperación tras desastres?

Además de la supervisión final, también preguntamos quién es responsable de ejecutar los aspectos más tácticos de la recuperación tras desastres. Las operaciones que residen en equipos de ciberseguridad o de continuidad del negocio especializados tienden a reportar el mejor rendimiento. Los programas ejecutados por TI generalmente se ubicaron por debajo de estos. Curiosamente, la visibilidad en el nivel de la junta directiva parece actuar como una marea creciente que eleva todos los botes. Las tasas de éxito fueron estadísticamente iguales, independientemente de dónde cayeran las responsabilidades diarias, siempre que la supervisión final fuera en la sala de la junta.

¿Es importante el alcance de la recuperación tras desastres?

Probablemente no se sorprenda al saber que el desastre no se produce convenientemente solo cuando o donde esté preparado para ello. Los desastres de ciberseguridad no son diferentes, por lo que la sabiduría convencional en el campo es prepararse para todas las eventualidades lo mejor posible. Eso es más fácil decirlo que hacerlo, por supuesto.

Para dar fe de ello, menos de tres de cada diez organizaciones afirman que sus funciones de recuperación tras desastres abarcan al menos el 80 % de los sistemas críticos. La mitad se encuentra en la zona del 50 % al 79 %, y un poco menos del 20 % admite tasas de cobertura inferiores. A primera vista, eso no parece tan malo. Después de todo, la mayoría de las organizaciones tiene la mayor parte de sus sistemas críticos cubiertos. Lamentablemente, este hecho ignora la tendencia inoportuna que tienen los desastres a ocurrir en lugares inesperados. Nuestros datos sugieren que esto sucede más a menudo de lo que nos gustaría admitir.

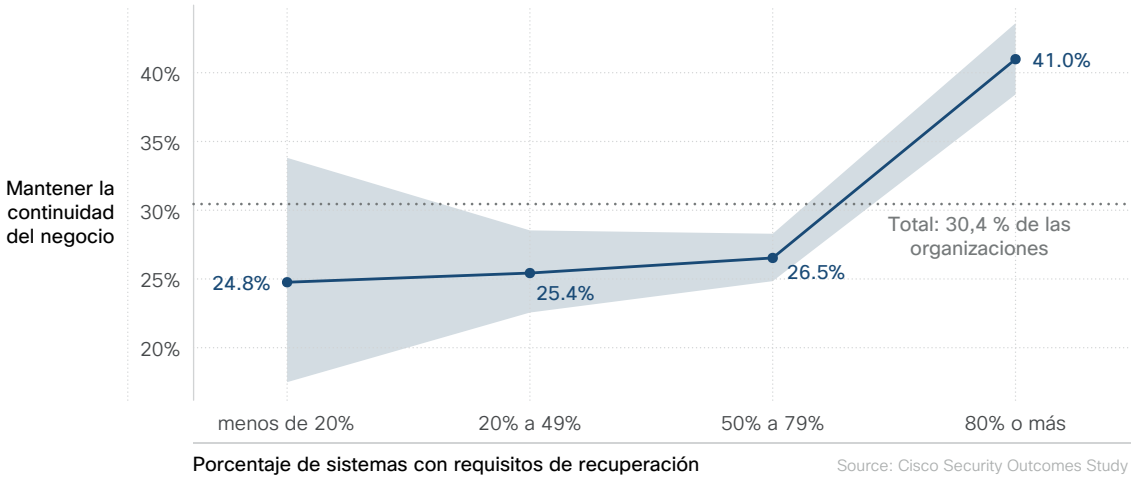


Figura 21: Efecto de la cobertura de activos críticos en las capacidades de recuperación tras desastres

En la Figura 21, se mide un nuevo resultado agregado para este estudio con el objetivo de medir la capacidad de la organización para mantener la continuidad del negocio a través de eventos desestabilizadores. Resulta que es uno de los tres resultados con los que la mayoría de los encuestados tiene dificultades. Eso hace que sea aún más importante encontrar formas eficaces de mejorar la probabilidad de éxito.

Hay un mensaje importante en la figura 21 sobre el mantenimiento de la continuidad del negocio. **A saber, prácticamente no hay mejora en la probabilidad de lograr este resultado hasta que las capacidades de BCDR cubran al menos el 80 % de los sistemas críticos.** Esto casi con certeza se remonta a la asombrosa tendencia de los desastres a atacar donde no estamos preparados. La lección aquí es que no podemos esperar que las inversiones en continuidad del negocio y recuperación tras desastres produzcan resultados inmediatos o equivalentes. Probablemente no sea un mensaje de bienvenida, pero, una vez más, el desastre nunca es un mensaje de bienvenida.

¿La práctica contribuye a una recuperación tras desastres perfecta?

Aplaudimos esta pregunta y le daremos la respuesta de inmediato. No, lamentablemente no. Pero sí hace que sea mucho mejor que si no se practica nada. ¿Cuánto mejor? Siga leyendo...

Un conocido adagio militar dice: "Ningún plan sobrevive al primer contacto con el enemigo". Resulta que se aplica bastante bien en el campo de batalla cibernético, y hay muchas maneras diferentes de probar las capacidades de BCDR, incluidos los recorridos del plan, los ejercicios con situaciones hipotéticas, las pruebas en vivo, las pruebas paralelas y las pruebas de producción completa. Les preguntamos a los encuestados con qué frecuencia sus organizaciones participan en tales ejercicios, y lo comparamos con su probabilidad de mantener la continuidad del negocio.

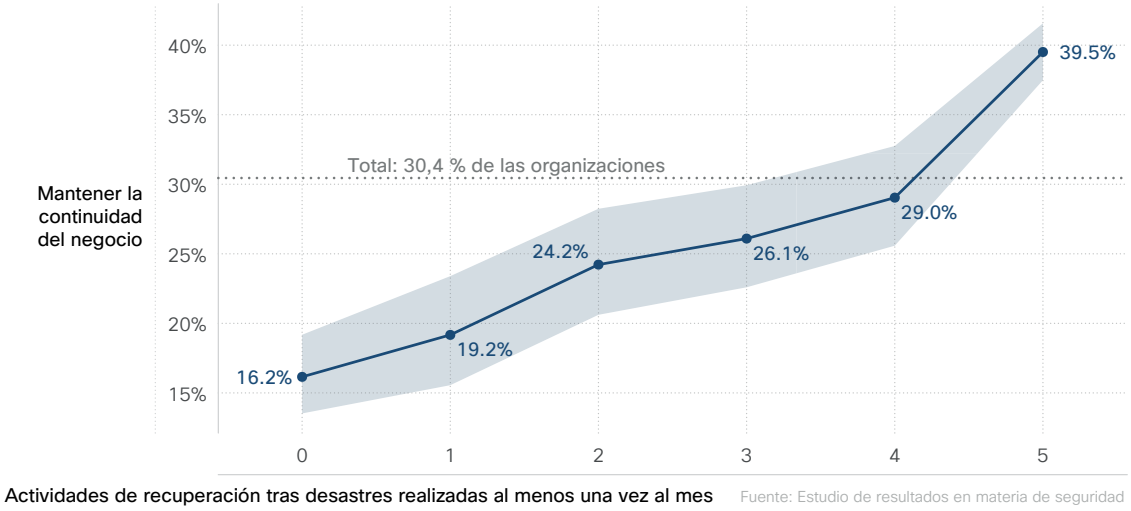


Figura 22: Efecto de las actividades de prueba en las capacidades de recuperación tras desastres

Ninguna de estas prácticas se situó muy por encima de las demás en términos de eficacia, pero todas contribuyeron colectivamente a mejorar la capacidad de recuperación. **Las organizaciones que participaban regularmente en los cinco tipos de pruebas de recuperación tras desastres eran casi 2,5 veces más propensas a mantener con éxito la continuidad del negocio que aquellas que no lo hacían.** ¿La conclusión? No deje la recuperabilidad al azar. Haga una prueba de esfuerzo de sus capacidades de continuidad del negocio y recuperación tras desastres con regularidad desde varios ángulos diferentes.

Organizations regularly engaged in all five types of disaster recovery testing are **2.5X** more likely to successfully maintain business continuity

¿Debemos desatar al mono del caos?

Sobre el tema de las pruebas de esfuerzo de su plan de recuperación tras desastres, maximicemos el "esfuerzo". Estamos hablando de la ingeniería del caos, mediante la cual los sistemas se interrumpen periódicamente (intencionalmente) para probar su capacidad de soportar condiciones y eventos inesperados. ¿Es posible que agregar una llave inglesa a sus sistemas de seguridad y TI ayude a que su organización sea más resistente? Bien, ha venido al lugar correcto para averiguarlo.

Les preguntamos a los encuestados sobre el grado en que sus organizaciones se dedican a la ingeniería del caos y descubrimos que era más común de lo que esperábamos. Cabe destacar que notamos una relación entre esta práctica y la integración tecnológica. Según la Figura 23, más de la mitad de las organizaciones para las que la ingeniería del caos es una práctica estándar reportan tecnologías altamente integradas que respaldan sus capacidades de recuperación. No está claro si la integración requiere o permite la ingeniería del caos. Como con tantas cosas en este campo, probablemente sea un poco de ambas. Esté atento a esta disciplina emergente, especialmente si es responsable de BCDR en un entorno de TI complejo y altamente integrado.

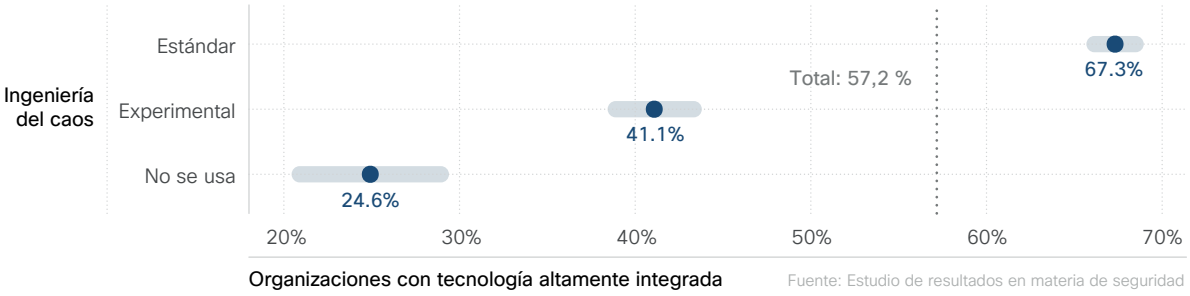


Figura 23: relación entre la ingeniería del caos y el nivel de integración de TI

La comparación del alcance de la ingeniería del caos con el resultado de mantener la recuperabilidad empresarial en la Figura 24 ofrece una razón de peso para invitar al mono del caos a su red. **Las organizaciones que hacen de la ingeniería del caos una práctica estándar tienen el doble de probabilidades de alcanzar altos niveles de éxito para este resultado que las organizaciones que no la utilizan.** Si ese resultado lo sorprende, no está solo. La buena noticia es que puede sorprender al mono antes de que él lo vuelva a sorprender a usted poniéndolo a trabajar para usted a través de la práctica de la ingeniería del caos.

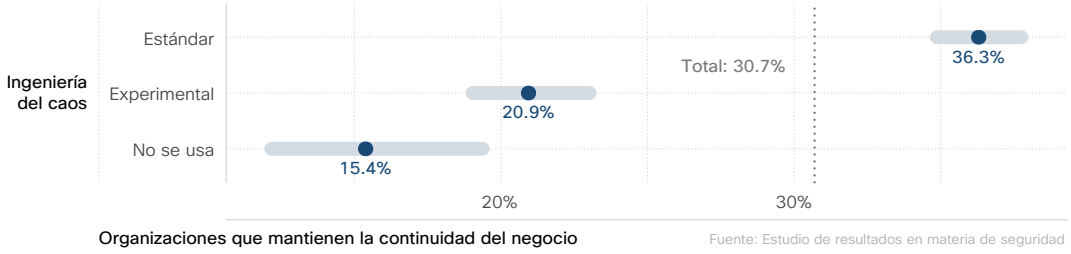


Figura 24: Efecto de la ingeniería del caos en el mantenimiento de la recuperabilidad empresarial

Conclusión y recomendaciones

Comenzamos con prácticas de seguridad identificadas como altamente eficaces en un estudio anterior, recopilamos más información a través de una nueva encuesta para saber qué las hace más eficaces y compartimos esas lecciones con usted. Esperamos que finalice este reporte con varios consejos prácticos sobre cómo hacer que su programa de ciberseguridad sea más exitoso.

Pero nunca está de más reflexionar sobre los resultados de un estudio como este y escuchar lo que otros obtuvieron de ellos. Le pedimos a nuestro experimentado equipo asesor de CISO que evaluara cada una de las áreas de práctica examinadas. Hemos incluido sus principales recomendaciones a continuación. Puede encontrar información adicional y conclusiones en nuestra serie de blogs #SecurityOutcomes.

Aumento en la actualización proactiva

"El problema de la deuda de seguridad es importante. Para el CISO, el camino a seguir es desarrollar una estrategia de "compra, retención, venta". Reconozca lo que tiene, defina una arquitectura adaptable, reduzca el riesgo de dependencia e implemente un ciclo de revisión para futuros ciclos de actualización".

Richard Archdeacon, Asesor de CISO, Cisco

Tecnología bien integrada

"Sabemos que la TI moderna y bien integrada contribuye al éxito general de los programas de seguridad, por lo que estas son algunas medidas que puede tomar para mejorar su entorno: busque soluciones de seguridad basadas en la nube, investigue las oportunidades de automatización y garantice que los requisitos de compra incluyan capacidades de integración de la tecnología".

Helen Patton, Asesor de CISO, Cisco @CisoHelen

Aumento en la respuesta oportuna

"El personal fuerte brinda una ventaja a los equipos de IR. Este es un buen punto de partida, pero debe realizarse junto con otros elementos. Cuando las empresas combinan personas, procesos y tecnología fuertes, logran capacidades avanzadas de detección y respuesta ante amenazas".

Dave Lewis, Asesor de CISO, Cisco @gattaca

Detección precisa de amenazas

"Elija las personas mejor capacitadas para sus equipos de SecOps, porque eso importa más que la cantidad de personal. Si no puede obtener el nivel de experiencia que necesita, la automatización puede ayudarlo a reducir la brecha con su personal junior y obtener resultados tan sólidos como si tuviera personal sénior".

Wendy Nather, Asesor de CISO, Cisco @wendynather

Aumento en la rápida recuperación

"Los resultados de este informe destacan el valor de la continuidad del negocio y las funcionalidades de recuperación tras desastres, pero no las ejecutan aisladas de otras funciones de seguridad. La priorización y la clasificación de riesgos de los recursos deben compartirse con otras funciones de administración de riesgos. De manera similar, integre estrechamente la administración de recursos y la gestión de amenazas para garantizar que todos los equipos trabajen con el mismo cuaderno de estrategias".

Wolfgang Goerlich, Asesor de CISO, Cisco @jwgoerlich

Acerca de Cisco Secure

Cisco ocupa una posición como líder mundial en tecnología que potencia la Internet desde hace mucho tiempo, y ha desarrollado un portafolio abierto e integrado de soluciones de ciberseguridad en el camino. Creemos que las soluciones de seguridad deben diseñarse para que funcionen juntas. Deben aprender una de otra. Deben escuchar y responder como una unidad coordinada. Cuando esto sucede, la seguridad se vuelve más sistemática y eficaz. Nuestros clientes han confiado en nosotros durante años como el proveedor más grande del mundo de infraestructura de TI y servicios de red y el negocio de ciberseguridad empresarial más grande del mundo.

Cisco Secure se basa en el principio de una mejor seguridad, no más. Ofrece un enfoque de seguridad optimizado y centrado en el cliente que garantiza que sea fácil de implementar, administrar y usar, y que todo funcione en conjunto. Nos motiva que las personas y nuestros clientes sean en el centro de dedicación de lo que hacemos. Comprendemos que los clientes desean superar la complejidad y el ruido, y tener confianza en su seguridad; centrándose en los resultados. Esto requiere simplificación, sin caer en el simplismo. Nuestra plataforma nativa de la nube es un gran avance en cuanto a esto.

Damos a los integrantes del área de seguridad la fiabilidad y la confianza de saber que están protegidos de las amenazas, ahora y en el futuro, con la plataforma Cisco SecureX. Ayudamos al 100 % de las empresas de Fortune 100 a proteger el trabajo, donde sea que tenga lugar, con la plataforma más amplia e integrada. Obtenga más información sobre cómo simplificamos las experiencias, aceleramos el éxito y protegemos el futuro en cisco.com/go/secure.

Apéndice: datos demográficos de muestra de la encuesta

En este apéndice, hemos incluido datos demográficos de muestra de las 5123 respuestas calificadas a esta encuesta. Esperamos que esto ayude a quienes intentan determinar la representatividad de estos hallazgos.

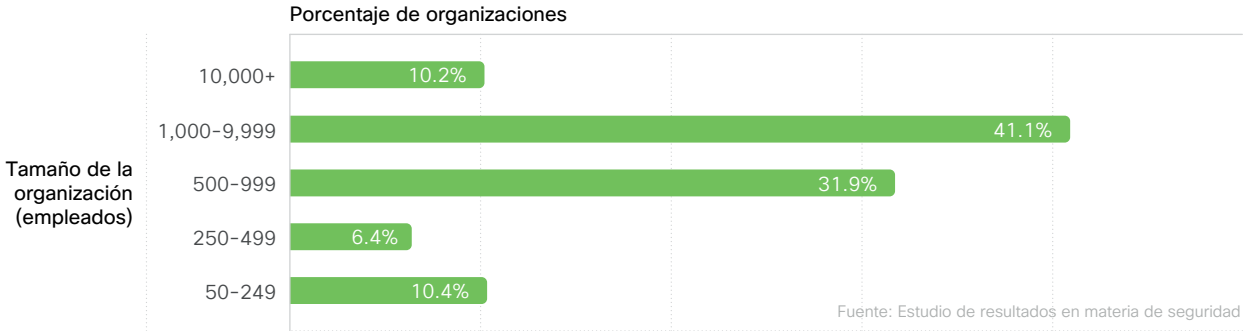


Figura A1: Cantidad de empleados para las organizaciones participantes

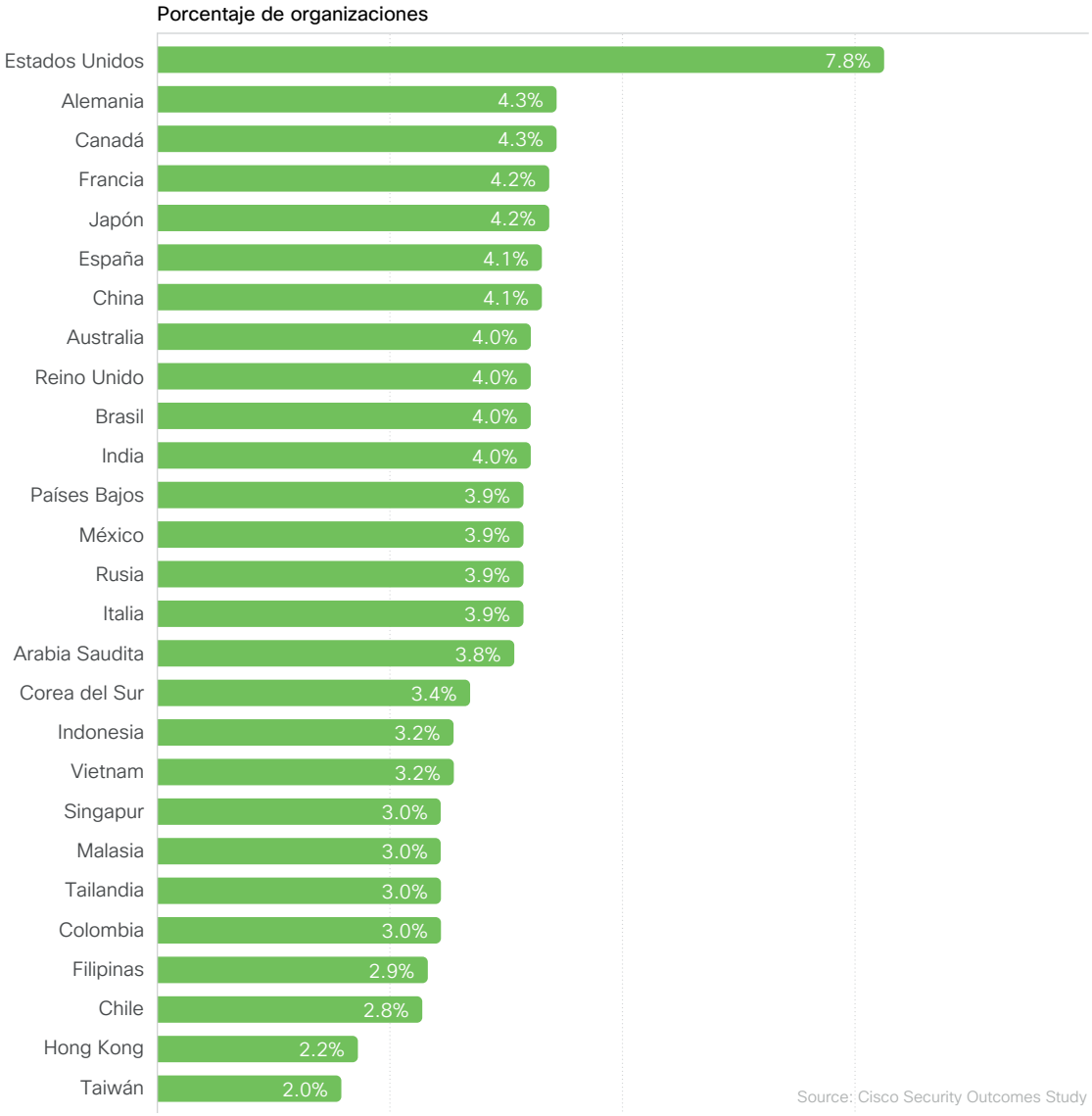


Figura A2: Países en los que las organizaciones participantes tienen su sede central

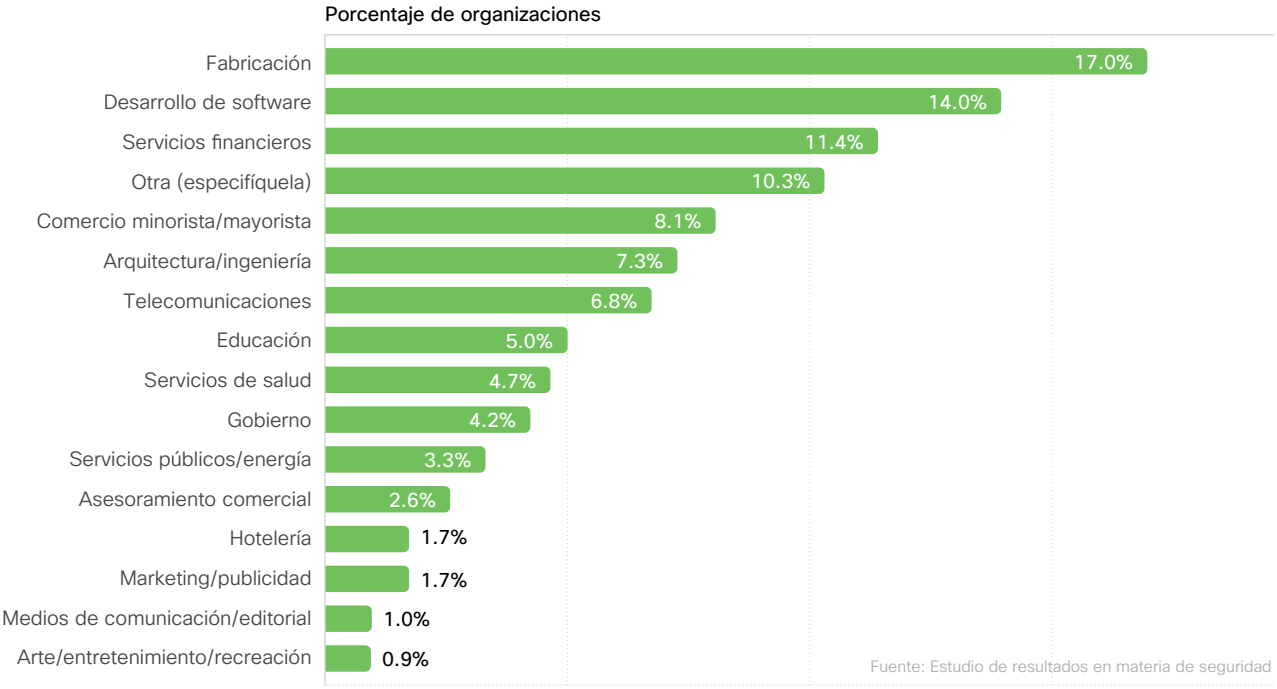


Figura A3: Sectores representados por organizaciones participantes

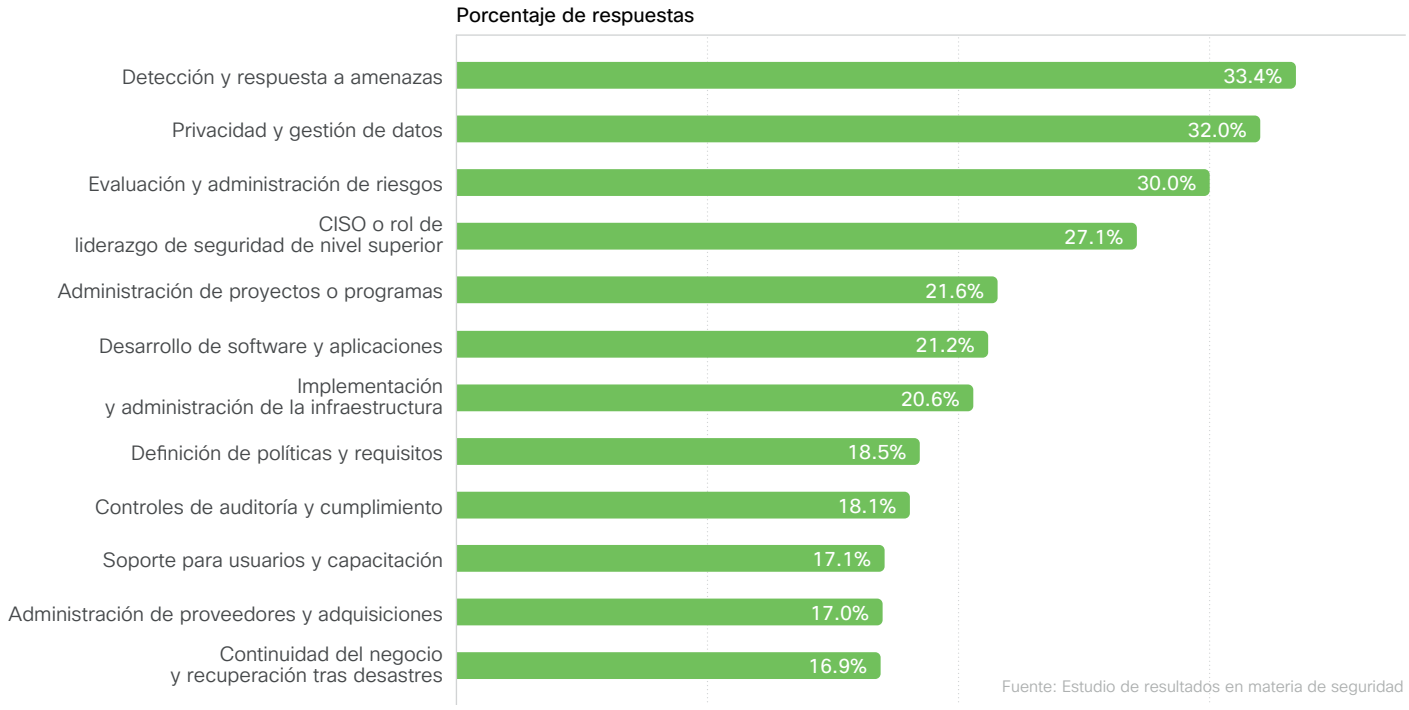


Figura A4: Responsabilidades laborales principales entre los encuestados

CISCO
SECURE

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA), Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Published December 2021

The bridge to possible