CISCO
SECURE

Prosperar como una pequeña o mediana empresa con una sólida estrategia de ciberseguridad

ESTUDIO DE RESULTADOS EN MATERIA DE SEGURIDAD

CISCO El puente a lo posible

Estudio de resultados en materia de seguridad de 2021: edición para pequeñas y medianas empresas

¿Qué hace al éxito de la ciberseguridad? ¿Existe evidencia de que las inversiones en seguridad dan como resultado resultados cuantificables? ¿Cómo sabemos qué sirve y qué no? Estos son los tipos de preguntas candentes que guían el Estudio de resultados en materia de seguridad de 2021 de Cisco, que reúne las experiencias de más de 4800 profesionales de TI, seguridad y privacidad en todo el mundo. Este documento es una consecuencia del estudio más amplio que se centra en las pequeñas y medianas empresas (PYMES).

La defensa de las organizaciones contra las amenazas cibernéticas es difícil para cualquier empresa, independientemente de su tamaño. Pero esto es particularmente cierto para las PYMES porque sus recursos suelen ser limitados y deben centrarse en gran medida en solo hacer inversiones que generen resultados impactantes. Los riesgos son mayores y priorizar lo más importante es fundamental para el éxito. Ayudar a identificar esas prioridades es de lo que se trata este informe.

Siga leyendo para descubrir cómo las PYMES se comparan con las grandes empresas en lo que respecta a la seguridad y qué factores clave contribuyeron a una planificación de seguridad exitosa en empresas como la suya.

Contenido

Hallazgos clave

Si toma algo de este estudio, debería ser que las cosas buenas vienen en paquetes pequeños.

Desde proveedores hasta profesionales, la industria de la ciberseguridad tiene la mala costumbre de suponer que el hecho de que algo sea más grande significa que es mejor. Pero este estudio presenta un caso convincente de que el tamaño más pequeño de su empresa no obstaculiza la posibilidad de grandes triunfos a la hora de desarrollar enfoques de seguridad exitosos. Estos son algunos ejemplos rápidos de lo que aprendimos del aporte colectivo de más de 850 PYMES que son pares de la suya.

La seguridad de las PYMES se ocupa de los negocios. ¿Creería que las PYMES pueden enseñarles a las empresas una o dos cosas sobre la seguridad eficaz?

¡Debería hacerlo, porque los datos muestran que los equipos pequeños y medianos son más exitosos que sus contrapartes más grandes en la creación de enfoques de seguridad que permiten el negocio! Este estudio pone de manifiesto el concepto de que la seguridad y el negocio en general comparten una relación integral en las PYMES.

No pierda de vista sus prioridades

El enfoque es fundamental para ejecutar cualquier estrategia, pero esto es especialmente cierto cuando los recursos son limitados. Las pequeñas y medianas empresas que afirmaron contar con una estrategia sólida para guiar las iniciativas de seguridad fueron significativamente más propensas a informar resultados exitosos. Además, tener una buena estrategia de seguridad era comparativamente más importante para las PYMES que para las grandes empresas.

El éxito radica en prepararse para el fracaso

Entre las 25 prácticas de seguridad que probamos, las capacidades de recuperación rápida tras un desastre fueron el mayor diferenciador de éxito entre las PYMES y las organizaciones más grandes. Esto probablemente se deba a dos hechos importantes: 1) inevitablemente, se producirán incidentes de seguridad, y, 2) en las PYMES, los incidentes tienen más impacto en el balance final. La planificación de la resiliencia a la luz de estos hechos es una estrategia ganadora.

Las amenazas modernas precisan tecnología moderna

Las PYMES que mantuvieron una pila tecnológica moderna lograron mayores tasas de éxito en cada uno de los 11 resultados de seguridad que medimos. Ninguna otra práctica contribuyó significativamente a más de cinco resultados. Además, este fue el factor común más fuerte entre los programas de TI que informaron un impacto operativo mínimo de la pandemia de COVID-19. Es difícil enseñar nuevos trucos a los antiguos técnicos, y todos sabemos que las amenazas cibernéticas nos arrojan todo tipo de trucos.

Acerca de la encuesta

Más de 4800 profesionales activos de TI, seguridad y privacidad de todo el mundo participaron en nuestro Estudio de resultados en materia de seguridad de 2021. De esos participantes, 857 representaron a las PYMES, y sus respuestas forman la base de este informe de seguimiento.

Acerca de la encuesta		
Muestreo	**Encuestados**	**Análisis**
Cisco contrató a una empresa de investigación de encuestas, YouGov, para realizar una encuesta totalmente anónima (fuente y encuestados) a mediados de 2020.	Encuestamos a más de 4800 profesionales activos de TI, seguridad y privacidad de 25 países. Aproximadamente el 18 % de los encuestados representó a las PYMES.	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.

Enfoque

- Indagamos sobre la adhesión de las organizaciones de los encuestados a 25 prácticas de seguridad que abarcan las áreas de gestión, estrategia, gastos, arquitectura y operaciones.
- Luego preguntamos sobre el nivel de éxito de cada programa en relación con aproximadamente una docena de objetivos o resultados de seguridad generales organizados en tres categorías principales: hacer posibles los negocios, administrar el riesgo y operar de manera eficiente.

La definición de lo que constituye una “pequeña” o “mediana” empresa difiere en todo el mundo, por lo que hemos adoptado las siguientes definiciones para su uso en este informe:

- Pequeña: 50 a 249 empleados[1] (el 8,5 % de los encuestados; n = 409)
- Mediana: 250 a 499 empleados (el 9,3 % de los encuestados; n = 448)
- Grande: 500 a 999 empleados (el 32 % de los encuestados)
- Compañía: más de 1000 empleados (el 50 % de los encuestados)

Figura 1: Sectores representados entre las empresas participantes

Fuente: Estudio de resultados en materia de seguridad de 2021 de Cisco

[1] Tenga en cuenta que las empresas con menos de 50 empleados no se incluyeron en la muestra objetivo para este estudio.

A partir de eso, queda claro que el Estudio de resultados en materia de seguridad de 2021 se inclina hacia organizaciones más grandes. Las PYMES colectivamente representan solo alrededor del 18 % de la muestra, pero tenga en cuenta que este porcentaje alcanza a 857 encuestados. (Un poco más de 400 de ellos provienen de pequeñas empresas, y aproximadamente 450 aterrizan en la categoría mediana). La representación desigual hace que sea difícil escuchar lo que esas empresas más pequeñas (pero importantes) tienen para decir, y es precisamente por eso que estamos produciendo este informe complementario centrado en la audiencia de las PYMES.

Otra cosa a tener en cuenta son los tipos de PYMES que participaron. En la Figura 1, se presenta un desglose de la industria. Puede ser útil hacer referencia a esto a medida que se consideran varios hallazgos de este estudio y cómo se aplican a su empresa.

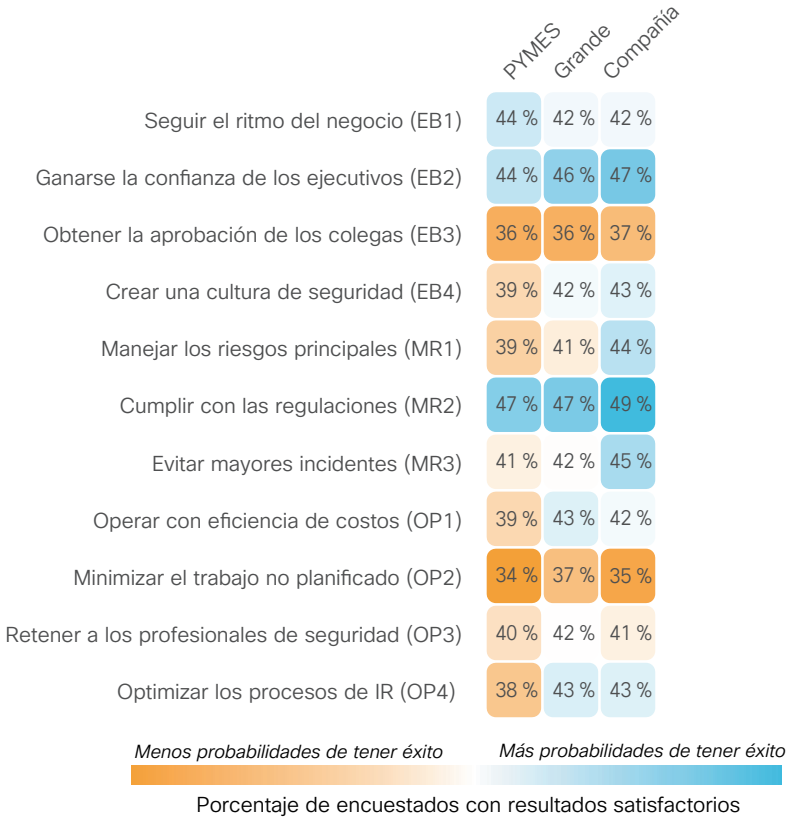
"No importa si usted es un banco de inversión multinacional en una operación pequeña de 130 personas como la nuestra; en adelante, cada institución financiera debe cumplir con las mismas reglas y normas de cumplimiento. Cisco Secure simplifica el trabajo de nuestros expertos en seguridad e ingenieros de redes".

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

Resultados de seguridad para las PYMES

Dado el título de este estudio, tiene sentido que comencemos con el fin en mente: los resultados de seguridad. Les pedimos a los encuestados que calificaran el nivel de éxito de su organización en 11 resultados de seguridad diversos de alto nivel que las empresas generalmente buscan lograr. Organizamos estos resultados en tres objetivos principales: hacer posibles los negocios, administrar el riesgo y operar con eficiencia.[2] Identificar las prácticas de seguridad que aumentan las posibilidades de lograr estos resultados es el objetivo principal de este estudio. Pero, primero, veamos cómo les va a las PYMES en relación con sus hermanos mayores en estos tres objetivos.

Figura 2: Comparación de las tasas de éxito informadas para cada resultado de seguridad entre los segmentos de negocios



Fuente: Estudio de resultados en materia de seguridad de 2021 de Cisco

Los porcentajes de la Figura 2 indican la proporción de organizaciones en cada segmento de tamaño que califican a sus empresas como altamente exitosas para cada resultado. Entonces, por ejemplo, el 44 % de las PYMES afirma que la seguridad se mantiene al día con el negocio dentro de su organización (parte superior izquierda). Volveremos a ese pequeño hecho en un momento.

Las funciones de seguridad de todos los tamaños parecen ser las más exitosas para cumplir con las normas de cumplimiento y ganar la confianza de los ejecutivos. Por otro lado, minimizar el trabajo no planificado y obtener el visto bueno de los pares que no pertenecen a la seguridad parece ser más difícil.

[2] Consulte el Estudio de resultados en materia de seguridad de 2021: Apéndice B: Lista completa de resultados en materia de seguridad para ver el texto completo de cada resultado, junto con la explicación y los ejemplos de evidencia que se proporcionaron a los encuestados como referencia para que califiquen el éxito de sus programas.

En términos de comparaciones del tamaño de la empresa, la Figura 2 revela tasas de éxito generalmente más altas entre las organizaciones más grandes. Sospechamos que esto se ajusta a las expectativas de muchos, ya que los recursos disponibles para alcanzar objetivos a menudo crecen junto con el tamaño de la organización. Pero, como dice el refrán, más dinero significa más problemas, y eso puede explicar por qué las diferencias entre los grupos de tamaño no son tan grandes como algunos podrían esperar.

Ese punto nos devuelve al factoide del 44 % mencionado anteriormente. Las PYMES superan en realidad a sus contrapartes más grandes en términos de seguridad para mantenerse al día con el negocio. Esto podría reflejar menos grados de separación entre los líderes empresariales y de TI en empresas más pequeñas. En algunos casos, por ejemplo, los emprendimientos tecnológicos, esos grupos pueden ser el mismo. E incluso cuando ese no es el caso, frases como “menos burocracia” y “sé a quién llamar” a menudo se mencionan como facilitadores a la hora de hacer las cosas en las PYMES. Esos mismos motivos también entran en juego cuando se realizan tareas de seguridad para ayudar al negocio.

En general, creemos que las PYMES deben sentirse alentadas por los resultados que se muestran en la Figura 2. Su tamaño más pequeño no impide grandes triunfos a la hora de desarrollar enfoques de seguridad exitosos. En la siguiente sección, veremos qué consejos tienen los datos para lograrlo.

> “No es necesario ser el blanco para convertirse en una víctima, y nadie es demasiado pequeño para resultar afectado”.
>
> Wouter Hindriks, líder técnico del equipo de Seguridad y red, Missing Piece

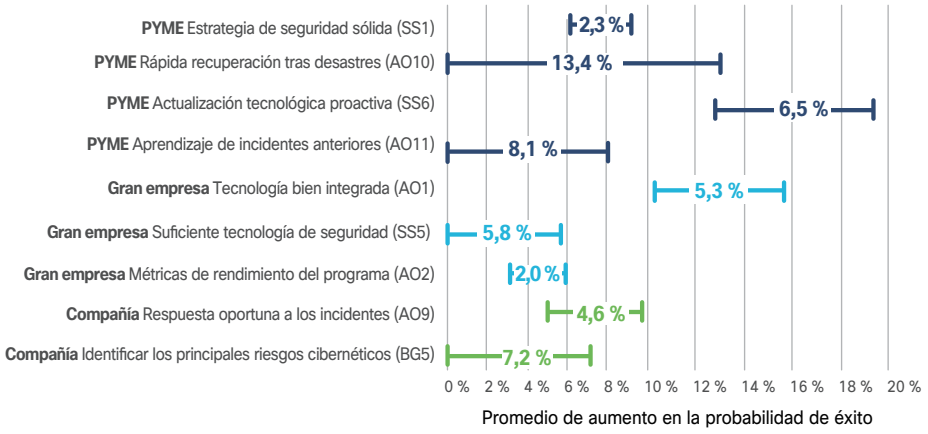
Factores generales de éxito de la seguridad para las PYMES

Además de los 11 resultados de la Figura 2, indagamos sobre la eficacia de los participantes del estudio para respetar un conjunto de 25 prácticas de seguridad comunes.[3] Decidimos no mostrar los niveles de implementación de todas estas prácticas porque: 1) es un gráfico realmente grande y 2) nuestro enfoque se centra en los resultados de este estudio. Pero, para quienes llevan la cuenta del puntaje, la ventaja de las empresas más grandes sobre las PYMES tiende a ser más pronunciada entre las prácticas que entre los resultados. Parecen malas noticias, pero podríamos decirlo así: las PYMES obtienen más beneficios (resultados exitosos) por su dinero (inversión en prácticas de seguridad).

Tras haber terminado con las preliminares, ahora podemos pasar a la parte divertida. Realizamos un análisis multivariable en los datos de las respuestas para medir cuáles de estas prácticas de seguridad se relacionan más estrechamente con lograr exitosamente cada uno de los objetivos. En otras palabras, ¿cuáles son los factores de éxito clave para la ciberseguridad en las PYMES? Primero respondamos esa pregunta centrándonos en el éxito general en todos los resultados. En las siguientes secciones, abordaremos prácticas que impulsan resultados específicos para pequeñas y medianas empresas.

En la Figura 3, se identifican las prácticas que, según los datos, ofrecen el mayor impulso para desarrollar un programa de seguridad exitoso en cada segmento comercial. El punto de partida para cada línea marca la tasa de éxito promedio de todos los participantes del estudio. El punto final de la línea indica cuánto más impacto tiene ese factor en las tasas de éxito entre las empresas en un segmento en particular.

Figura 3: Principales diferenciadores de éxito de seguridad para PYMES, grandes empresas y segmentos



Entonces, por ejemplo, las organizaciones que informan tener una estrategia de seguridad sólida tenían un 6,1 % más de probabilidades de informar un enfoque de seguridad muy exitoso. Una estrategia sólida entre las PYMES, en comparación, dio como resultado un aumento promedio del 8,4 % en las tasas de éxito, por una diferencia del 2,3 %. Las funcionalidades que garantizan la pronta recuperación tras un desastre no contribuyeron significativamente al éxito general de todos los encuestados, pero marcaron una gran diferencia (más del 13,4 % en promedio) para las PYMES.[4] Y así sucesivamente.

[3] Consulte el Apéndice C en el Estudio de resultados en materia de seguridad de 2021 para obtener el texto completo y la lista de estas prácticas.

[4] El punto de partida del 0 % que se muestra aquí y en otros gráficos similares indica que la práctica no tuvo un efecto estadísticamente significativo en la probabilidad de éxito de todos los encuestados.

Es probable que cada lector elabore su propia receta para el éxito de la seguridad de las PYMES a partir de los ingredientes de la Figura 3, y eso es algo que alentamos. Por nuestra parte, vemos tres temas principales reflejados en los datos: **enfoque, resiliencia** y **modernización.** Los analizaremos en los siguientes párrafos.

El enfoque es un componente fundamental de cualquier estrategia, especialmente para las PYMES, donde priorizar las iniciativas es primordial. Sin ella, las empresas pierden de vista lo que más importa, no pueden ejecutar con eficacia, desperdician recursos valiosos y, finalmente, pierden el rumbo. Un aumento del 8,4 % en las tasas de éxito para las PYMES con una estrategia sólida puede no parecer mucho, pero ayuda un poco. El hecho de que esté en la lista cuando otras 21 prácticas no mostraron diferencias significativas entre las PYMES y todos los encuestados significa que no se debe ignorar. Además, la naturaleza de la estrategia es tal que sus efectos indirectos sobre otras prácticas de seguridad pueden ser mayores que su efecto directo.

¿Es posible tener una cotización, o bien, extraer texto, para rellenar aquí? También podemos encontrar una imagen, pero lo hice en la página siguiente. Essundi gendereped qui alite delendem sus derum il min plab inihictur magnat assuntis esequo odipis militaq uassita vendis consece stiorepel iume iumendu ciamus alibus, veliquassin nonsed qui sum labo. Ci comni ut exces peliciur, videl ero quatem viducient.

Las funciones de TI y seguridad se han enfrentado a desafíos que superan con creces los de su proporción justa, por lo que probablemente la Conferencia RSA de 2021 (la conferencia de seguridad más grande del mundo) haya elegido la "Resiliencia" como tema central. Como se indicó en la explicación detrás de esa opción, "*las amenazas cibernéticas son implacables y nuestras soluciones deben recuperarse rápidamente de cualquier adversidad que nos arrojen".* Eso es exactamente para lo que están diseñadas las capacidades de recuperación tras un desastre, y la Figura 3 muestra que se traducen en grandes logros para la ciberseguridad de las PYMES.

¿Por qué? Bien, un estudio independiente de más de 50 000 eventos de pérdida cibernética durante un período de 10 años puede ofrecer una pista.[5] El análisis reveló que, si bien las PYMES no experimentan incidentes de seguridad tan a menudo como sus pares empresariales, el impacto relativo en sus resultados es mucho mayor cuando se producen. "*Una empresa de USD 100 mil millones que experimenta un evento cibernético típico (USD 292 000) debe esperar un costo que represente el 0,000003 % de los ingresos anuales. Una tienda familiar que genera USD 100 000 al año, por otro lado, probablemente perderá una cuarta parte de sus ganancias (USD 24 000) o más".* Por lo tanto, una recuperación rápida se vuelve fundamental para la resiliencia comercial.

La aplicación de los aprendizajes de incidentes de seguridad anteriores en la Figura 3 conecta el enfoque y los temas de resiliencia. Ninguna empresa, grande o pequeña, desea sufrir grandes violaciones o interrupciones, pero las lecciones aprendidas de ellas pueden ayudar a convertir los limones en limonada. Y estas lecciones no necesitan ser extraídas solo de sus propias experiencias; lo que sucedió con los socios, los pares y otras organizaciones también puede ser instructivo. Las empresas exitosas utilizan estas lecciones para centrar su estrategia de seguridad, reforzar las defensas y reforzar las capacidades de recuperación. El fracaso puede ser un buen maestro, tanto en los negocios como en la ciberseguridad.

[5] Estudio de conocimientos de riesgo de la información 20/20 (Cyentia Institute)

Y eso nos lleva a nuestro tercer tema: la modernización. Es cierto que la etiqueta "actualización tecnológica proactiva" no incluye la palabra "modernización", pero el texto presentado a los encuestados aborda este tema. "*Mi organización cuenta con una estrategia de actualización tecnológica proactiva mediante mejoras frecuentes con las mejores tecnologías de seguridad y TI disponibles".* La implementación de esa estrategia será diferente para cada organización, desde actualizaciones de hardware y software tradicionales hasta actualizaciones continuas proporcionadas a través de soluciones de software como servicio (SaaS) y proveedores de servicios administrados (MSP).

Para muchas PYMES, estas últimas opciones (SaaS y MSP) ofrecen una forma rentable de mantener una pila tecnológica moderna. La escalabilidad, la agilidad y la eficiencia a menudo se mencionan como los factores que impulsan la migración a la nube y las SaaS, pero, en la Figura 3, se presenta el caso para agregar seguridad a esa lista para las PYMES. Con ese modelo, muchas responsabilidades de seguridad fundamentales, como las actualizaciones de software, el control de acceso, la supervisión de amenazas y la respuesta ante los incidentes, pasan al proveedor de servicios y, por lo tanto, pasan al costo recurrente del servicio.

Además, podemos conectar este tema de la modernización con el de la resiliencia a raíz de eventos inesperados. Les preguntamos a los participantes del estudio cómo la pandemia de COVID-19 y la posterior transición al trabajo remoto afectaron a sus organizaciones. ¿Le gustaría adivinar qué práctica se destacó sobre todas las demás entre las empresas que informaron un impacto mínimo en las operaciones y la postura de riesgo cibernético? Así es: la actualización tecnológica proactiva.

En pocas palabras: las amenazas cibernéticas modernas requieren tecnología cibernética moderna. Esto puede parecer un costo prohibitivo para los presupuestos de las PYMES, pero las SaaS pueden ofrecer una ruta más accesible para experimentar los beneficios de seguridad de las últimas tecnologías.

Es bueno soñar en grande

Como este estudio se centra en las PYMES, hasta ahora hemos ignorado los factores de éxito clave para las organizaciones más grandes. Pero las PYMES que aspiran a ponerse esos zapatos podrían considerar lo que contribuye al éxito de las grandes empresas.

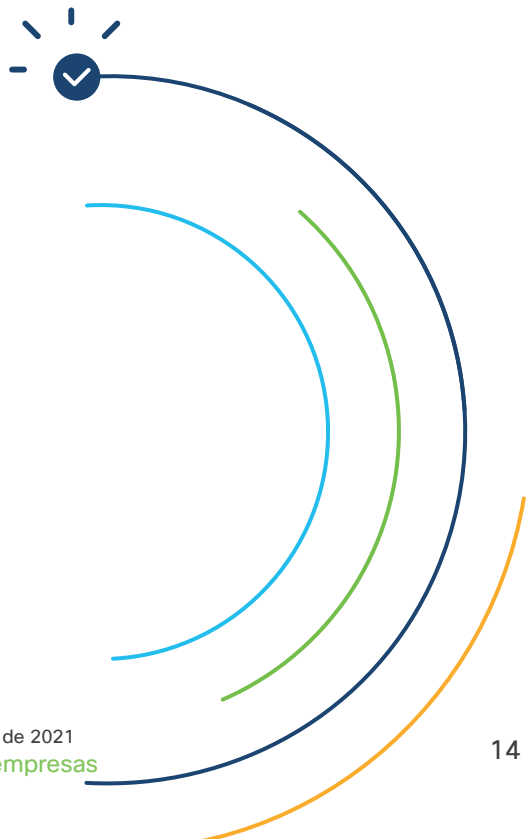
La Figura 3 reafirma que la importancia de contar con tecnologías de seguridad suficientes para respaldar esa estrategia crece junto con el negocio. También lo hace la necesidad de garantizar que esas tecnologías se integren bien entre sí. La medición del rendimiento de la seguridad a través de métricas completa la lista de diferenciadores para las grandes empresas.

Pasando a las organizaciones de clase empresarial, vemos que la identificación oportuna de los principales riesgos cibernéticos y las capacidades de respuesta rápida ante incidentes (IR) se vuelven cruciales. Sospechamos que se debe a que la atención de los agentes de amenazas, el tamaño de la superficie de ataque y la frecuencia de los incidentes tienden a aumentar con el tamaño y el perfil de la empresa. La transición de ser un objetivo de oportunidad a un objetivo de elección cambia radicalmente el juego y estas prácticas ayudarán incluso a la puntuación cuando usted esté listo para jugar a ese nivel.

Lograr resultados específicos

Todos quieren una mejor ciberseguridad en general, pero a veces es deseable o necesario buscar resultados específicos. Quizás al ver la lista de resultados de la Figura 2, usted haya pensado: “Me pregunto, ¿qué factores nos ayudarían a lograr *ese* resultado?”. Si es así, las siguientes secciones son para usted.

Debido a que la mayoría de los lectores de este informe representan pequeñas o medianas empresas, hemos dividido secciones dedicadas para cada una a continuación. Puede leer nuestro análisis y nuestras recomendaciones para ambos segmentos de negocios, por supuesto. Analizaremos primero los factores de éxito de las pequeñas empresas y luego pasaremos a las medianas.



"Mis experiencias anteriores con empresas masivas es que pueden ser bastante difíciles, incluso arrogantes, en lo que respecta a trabajar con ellas si eres una empresa pequeña. No hemos sentido eso con Cisco en lo más mínimo. De hecho, han realizado esfuerzos específicos para ayudar a nuestra pequeña empresa a seguir siendo competitiva".

Charl Tintinger, director de tecnología de Gigaclear

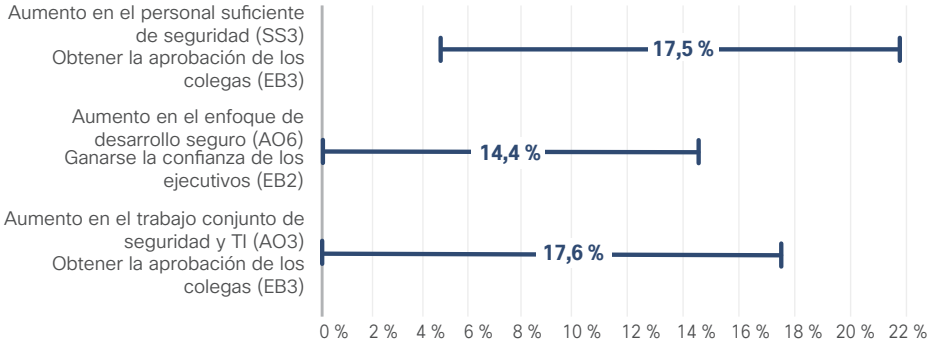
Factores de éxito clave de las pequeñas empresas

Antes dijimos que los resultados están organizados en tres categorías: hacer posibles los negocios, administrar el riesgo y operar con eficiencia. A continuación, encontrará los mismos encabezados, junto con gráficos que identifican las prácticas de seguridad más estrechamente relacionadas con el logro exitoso de cada objetivo por parte de las pequeñas empresas. Tenga en cuenta que nuestros Apéndices del Estudio de resultados en materia de seguridad de 2021 ofrecen versiones de texto completo de todas las etiquetas abreviadas para las prácticas y los resultados en las siguientes figuras.

Facilitar negocios

Como dice la etiqueta, este objetivo se centra en la misión de seguridad de respaldar y fomentar las actividades comerciales. Los resultados de esta categoría permiten reconocer que la seguridad no existe por la seguridad en sí misma; sino que sirve a los negocios. En la Figura 4, se muestran los tres principales diferenciadores para que las pequeñas empresas logren con éxito los resultados de este objetivo. A modo de recordatorio, el punto de partida para cada línea marca la tasa de éxito promedio de todos los participantes del estudio. El terminal de la línea indica cuánto más impacto tiene ese factor en las tasas de éxito entre las pequeñas empresas.

Figura 4: Principales tres diferenciadores de seguridad para habilitar a las pequeñas empresas



La correlación más sólida entre la práctica y los resultados en esta categoría es que contar con personal de seguridad suficiente mejora la aceptación de la seguridad por parte de pares de toda la empresa. Las funciones de TI y seguridad que trabajan juntos de manera colaborativa también contribuyen sustancialmente a ese mismo resultado. Dado que muchas pequeñas empresas no tienen personal de seguridad dedicado, ese mensaje puede ser poco deseado por algunos lectores. Pero "suficiente" y "juntos" son las palabras operativas aquí, no "dedicado". Un buen número de empresas que participaron en este estudio no contaban con personal de seguridad *dedicado*, pero aún así informaron enfoques exitosos de seguridad al contar con personal suficiente y colaborativo.

Dicho esto, inevitablemente llegará un momento en la vida de las organizaciones en crecimiento cuando el gorro de seguridad de la persona que usa muchos sombreros de TI comenzará a ser un poco ajustado. Y cuando no se intercambia por uno más grande, o si esos sombreros no se colocan equitativamente en múltiples cabezas, comienzan a obstaculizar el negocio. Y la Figura 4 sugiere que una de las primeras áreas que puede volverse evidente es perder la aceptación de otras personas o grupos de la organización. Quizás sea porque TI no puede admitir esa nueva iniciativa empresarial. Tal vez sea porque la tecnología o las complicaciones de seguridad sofocan la productividad. Independientemente de la razón, estos resultados destacan la importancia de contar con el talento de seguridad adecuado (ya sea compartido o dedicado) para prestar servicios a la empresa y su misión.

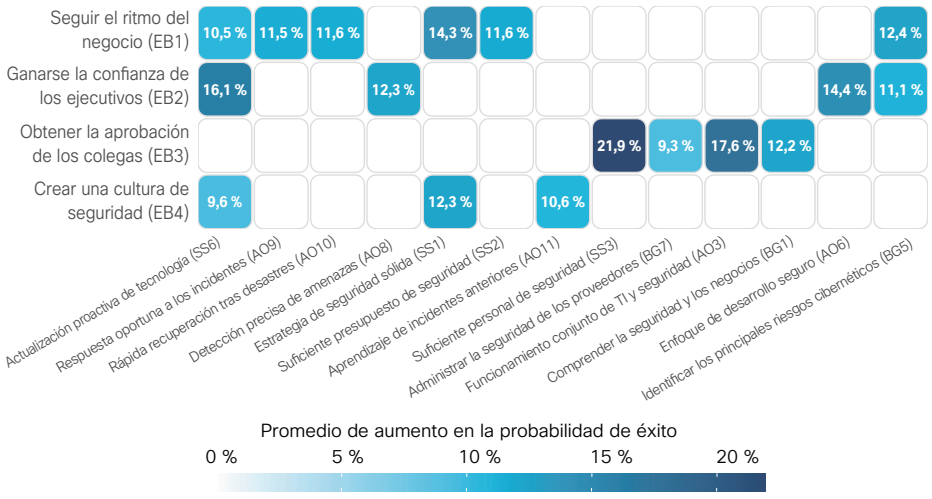
El otro factor que marca la diferencia de la Figura 4 vincula las prácticas de desarrollo de software seguro con la obtención de la confianza de los ejecutivos. Parece extraño, pero la respuesta a ese enigma radica en el hecho de que las empresas de desarrollo de software fueron el sector más grande representado entre las PYMES en este estudio. Por lo tanto, la producción de código seguro y sólido está intrínsecamente vinculada al balance de esas empresas (y probablemente a las cuentas bancarias personales de los ejecutivos).

Pero no es necesario ser una tienda de software para poner en práctica este principio. Cada vez que la seguridad se vuelve esencial para el negocio, obtiene un perfil más alto en la parte superior. Esté preparado para crear soluciones en lugar de obstáculos.

Eso resume las tres principales prácticas de seguridad y los diferenciadores de resultados para habilitar a las pequeñas empresas, pero sospechamos que muchos desearán ver qué otras opciones están disponibles para ellos. Con ese fin, la Figura 5 muestra todas las prácticas que se correlacionan significativamente con cualquiera de los cuatro resultados de este objetivo. Y como se puede ver con claridad, la lista de factores de éxito es mucho más larga que tres.

Los valores en la Figura 5, y otras similares a continuación, denotan el aumento promedio en la probabilidad de éxito de un resultado dado cuando las organizaciones informan un gran cumplimiento de una determinada práctica. El sombreado corresponde a la fuerza de la correlación entre la práctica y el resultado. Las combinaciones de práctica y resultado sin sombreado o valor indican que nuestro análisis no encontró una correlación estadísticamente significativa. Eso no significa que la práctica no sea útil; solo significa que no encontramos evidencia convincente de que conduzca a un mayor éxito para ese resultado.

Figura 5: Correlación de las prácticas de seguridad y los resultados para habilitar a las pequeñas empresas



Fuente: Estudio de resultados en materia de seguridad de 2021 de Cisco

Lo primero que se debe tener en cuenta con respecto a la Figura 5 es que cada resultado tiene múltiples formas en las que las prácticas de seguridad contribuyen a habilitar el negocio. Esa es una buena noticia porque sugiere que las pequeñas empresas pueden personalizar una ruta al éxito que se adapte a sus necesidades y capacidades.

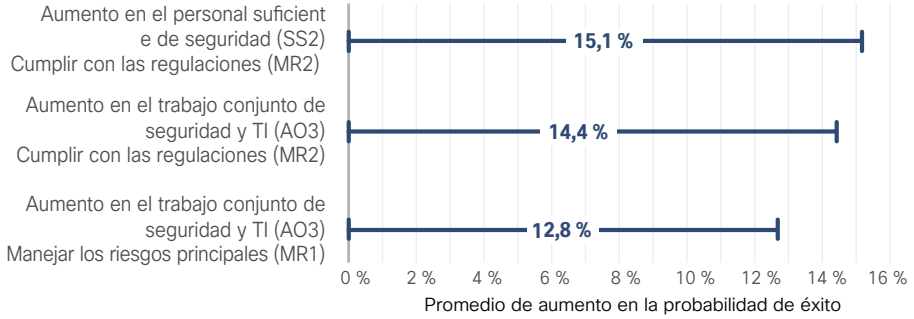
Más allá de eso, volvemos a ver el papel esencial que desempeña la tecnología moderna en la creación de pequeñas empresas seguras y exitosas. Mantener la arquitectura y los servicios actualizados ayuda a la seguridad a satisfacer las necesidades del negocio, gana la confianza de los ejecutivos y promueve una cultura de seguridad más sólida. Abordar esa pila de tecnología con una estrategia sólida y una sólida comprensión de las amenazas que buscan aprovecharla también genera ganancias en múltiples frentes.

No dude en pasar todo el tiempo que desee con la Figura 5. Gráficos como este ofrecen una especie de giro de “elija su propia aventura” en la planificación de la seguridad. Esperamos que la utilice para llegar a donde desea ir.

Administrar el riesgo

La mayoría de las personas piensa en administrar el riesgo cuando se les pregunta sobre la responsabilidad principal de la seguridad. Por supuesto, el riesgo es multifacético, por lo que elegimos examinar tres resultados, cada uno de los cuales proporciona una perspectiva distinta de cómo las pequeñas empresas administran el riesgo cibernético. En la Figura 6, se destacan los conjuntos de resultados de la práctica que presentan los diferenciadores más sólidos para las pequeñas empresas en lo que respecta a este objetivo.

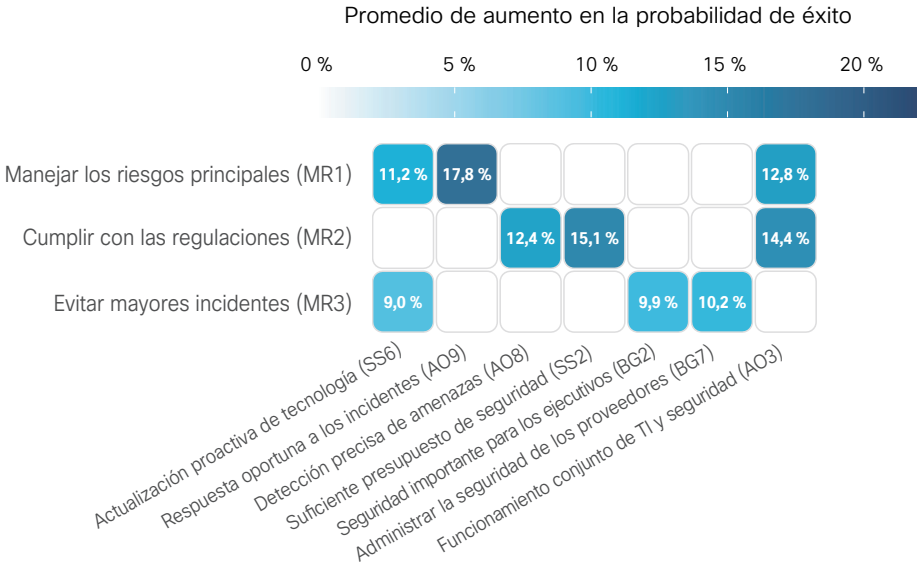
Figura 6: Principales tres diferenciadores de seguridad para administrar riesgos en pequeñas empresas



El cumplimiento ha sido durante mucho tiempo un factor de impulso para la adopción de la seguridad en organizaciones de todos los tamaños. Sin embargo, hemos escuchado de clientes y expertos que se está convirtiendo en un problema aún más grande para las pequeñas empresas. A medida que surgen más estándares y aumentan las regulaciones, la barra de requisitos mínimos sigue aumentando. Y si bien la mayoría de las grandes organizaciones deben superar esa barrera, no siempre es el caso de las empresas más pequeñas.

Los datos que se encuentran en la Figura 6 afirman que los presupuestos y la colaboración aumentan la capacidad de las pequeñas empresas para cumplir con sus obligaciones de cumplimiento. La asociación de “más presupuesto, más cumplimiento” no es sorprendente, pero aún podría ser un punto de datos útil para el liderazgo si los recursos son demasiado escasos, pero abundan las presiones regulatorias.

Figura 7: Correlación de prácticas de seguridad y resultados para la administración de riesgos en pequeñas empresas



Fuente: Estudio de resultados en materia de seguridad de 2021 de Cisco

Como se mencionó en la sección anterior, el concepto de colaboración entre TI y las funciones de seguridad puede ampliarse o reducirse según la empresa en cuestión. Para las pequeñas empresas, esto podría deberse a que la persona lleva múltiples sombreros, de los cuales la TI y la seguridad son solo dos. En esa situación, esto sugiere que la persona tiene suficiente tiempo y capacitación para hacer las dos cosas bien. A medida que las empresas crecen, esto podría convertirse en dos personas separadas que permanecerán en estrecho contacto y se consultarán en proyectos. Sin embargo, según se ve, la Figura 6 afirma que mantener la TI y la seguridad muy cerca es un diferenciador clave para administrar los principales riesgos cibernéticos en las pequeñas empresas.

En la Figura 7, se pueden encontrar prácticas adicionales de administración de riesgos que son prometedoras para las pequeñas empresas. La actualización tecnológica proactiva entra en escena una vez más, lo que mejora las posibilidades de mitigar riesgos cibernéticos críticos y evitar incidentes importantes. Marque otro punto para el tema de "las amenazas modernas requieren tecnología moderna". Probablemente aquí estemos viendo nuevamente los beneficios de las SaaS. El proveedor o MSP está reparando vulnerabilidades, monitoreando amenazas, respondiendo a incidentes, etc., como parte de los costos fijos predecibles.

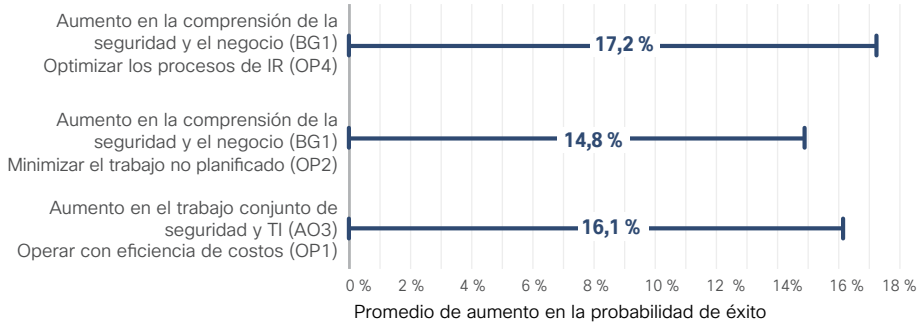
Hablando de responder a incidentes, las funcionalidades de la IR producen la mayor correlación en la Figura 7. Administrar los riesgos principales no se trata solo de evitar que sucedan cosas malas; se trata de minimizar su impacto y mantener la resiliencia cuando se producen.

La seguridad de la cadena de abastecimiento ha recibido mucha atención últimamente debido a algunas violaciones de alto perfil, por lo que vale la pena señalar que administrar la seguridad de los proveedores contribuye a evitar incidentes importantes. Las pequeñas empresas forman los pilares de las grandes cadenas de abastecimiento, y la investigación muestra que es más probable que estén en el lado receptor de los eventos cibernéticos que se propagan a través de esas relaciones entre organizaciones.[6] En la Figura 7, se muestra por qué las pequeñas empresas con aversión al riesgo deben evaluar la seguridad de sus socios clave.

Operar con eficiencia

Más allá de hacer posibles los negocios y administrar el riesgo, la capacidad para operar con eficiencia suele diferenciar un excelente programa de TI de los que son buenos. Este último conjunto de resultados de nuestro estudio aborda la rentabilidad, la ejecución de la estrategia, la gestión de los profesionales y los procesos de respuesta ante incidentes. Cosas importantes, especialmente para las pequeñas empresas.

Figura 8: Tres diferenciadores principales de seguridad para operar de manera eficiente en pequeñas empresas



Source: Cisco 2021 Security Outcomes Study

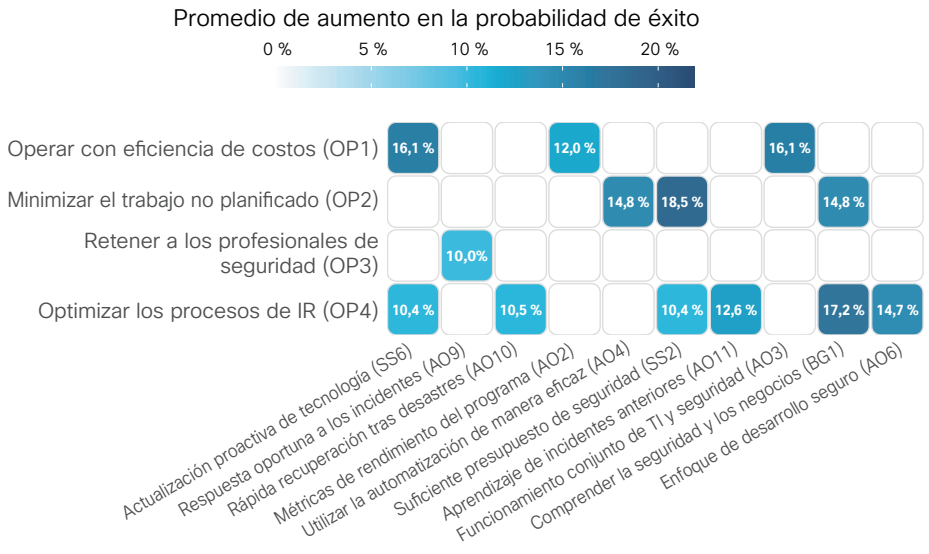
[6] Ondulaciones en la superficie de riesgo (RiskRecon, Cyentia Institute)

La Figura 8 nos devuelve a la noción de que la seguridad y el negocio comparten una relación integral en las pequeñas empresas. Según nuestro análisis, comprender cómo las iniciativas de seguridad respaldan los imperativos comerciales optimiza la respuesta ante los incidentes y minimiza el trabajo no planificado. Esto presenta una oportunidad para hacer que la capacitación en seguridad estándar sea más personal e impactante. El personal de TI debe saber cómo funciona el negocio y cómo sus responsabilidades se ajustan a su misión.

Y eso nos devuelve al trabajo conjunto de TI y seguridad. Si parece que la conversación continúa en esta dirección, tiene toda la razón. Es la única práctica que marca los tres principales diferenciadores para cada uno de los principales objetivos de seguridad en esta sección para pequeñas empresas. Independientemente de cuántas personas comprendan las funciones de seguridad y TI, las fricciones y las facciones entre ellas crean ineficiencias. El trabajo en equipo fomenta la rentabilidad, especialmente en una empresa pequeña.

Como hemos hecho en las secciones anteriores, la Figura 9 amplía la lista de prácticas de seguridad respaldadas por datos en esta categoría más allá de los tres principales diferenciadores para pequeñas empresas. Un presupuesto de seguridad suficiente, una actualización de tecnología proactiva y la garantía de que el personal comprenda la seguridad en el contexto de la empresa son beneficiosos para múltiples resultados.

Figura 9: Correlación de prácticas de seguridad y resultados para operar de manera eficiente en pequeñas empresas



Fuente: Estudio de resultados en materia de seguridad de 2021 de Cisco

La actualización tecnológica proactiva es un factor de éxito familiar en este momento. La Figura 9 lo vincula con enfoques de seguridad rentables y una respuesta a los incidentes optimizada. Sí, la modernización de su pila de tecnología tiene un costo, ya sea hardware, software o SaaS. Pero aquí vemos evidencia de que la inversión colabora con su amortización a través de otros beneficios. Una respuesta deficiente a los principales incidentes de seguridad puede hacer que un presupuesto de TI se vuele más rápido que cualquier otra cosa.

De acuerdo con este tema, los presupuestos de seguridad suficientes y la minimización del trabajo no planificado marcan la correlación más sólida. Las empresas que tienen los recursos que necesitan no tienen que abandonar o alterar constantemente los planes, lo que les permite hacer las cosas.

Recursos para una seguridad exitosa en pequeñas empresas

Centro de recursos de seguridad de Cisco Small Business

Promociones y pruebas gratuitas de Cisco Small Business

Oferta de Cisco Designed Secure Remote Work

Para ver el texto completo de cada resultado y las prácticas de seguridad, junto con la explicación y los ejemplos de evidencias que se proporcionaron a los encuestados como referencia para que califiquen el éxito de sus programas, consulte el **Apéndice B y C del Estudio de resultados en materia de seguridad de 2021.**

"¿Alguna vez intentó resolver un problema técnico y consideró que estaba recibiendo un argumento de venta en lugar de una respuesta? A menudo lo he experimentado con otros proveedores, pero Cisco y SVA actúan como socios que tienen en cuenta los mejores intereses de Stenger".

Frank Bettenworth, CIO de Strenge GmbH & Co. KG

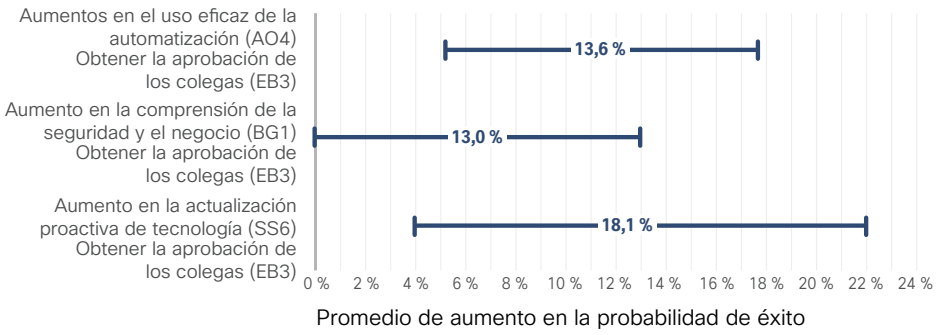
Factores de éxito clave de las medianas empresas

Antes dijimos que los resultados están organizados en tres categorías: hacer posibles los negocios, administrar el riesgo y operar con eficiencia. Encontrará los mismos encabezados a continuación junto con gráficos que identifican las prácticas de seguridad que se correlacionan más estrechamente con el logro exitoso de cada objetivo por parte de las empresas medianas. Tenga en cuenta que nuestros Apéndices del Estudio de resultados en materia de seguridad de 2021 ofrecen versiones de texto completo de todas las etiquetas abreviadas para las prácticas y los resultados en las siguientes figuras.

Facilitar negocios

Como dice la etiqueta, este objetivo se centra en la misión de seguridad de respaldar y fomentar las actividades comerciales. Los resultados de esta categoría permiten reconocer que la seguridad no existe por la seguridad en sí misma; sino que sirve a los negocios. La Figura 10 muestra los tres principales diferenciadores para que las empresas medianas logren resultados con este objetivo. A modo de recordatorio, el punto de partida para cada línea marca la tasa de éxito promedio de todos los participantes del estudio. El terminal de la línea indica cuánto más impacto tiene ese factor en las tasas de éxito entre las medianas empresas.

Figura 10: Principales tres diferenciadores de seguridad para permitir los negocios en empresas medianas



Fuente: Estudio de resultados en materia de seguridad de 2021 de Cisco

Dado que los tres principales diferenciadores de seguridad para permitir que las empresas medianas se vinculen con el resultado de obtener la aceptación de pares, debemos aclarar lo que eso implica. El ejemplo de evidencia dada a los encuestados para ayudarlos a evaluar este resultado incluye: 1) TI alistando a otros grupos en la construcción de una defensa cooperativa, 2) una sólida comunicación entre organizaciones y 3) un sentido justo de "dar y recibir" entre colegas para un bien mayor. En cambio, una cultura de quejas y la tensión interdepartamental es una señal de que existen dificultades para alcanzar este objetivo.

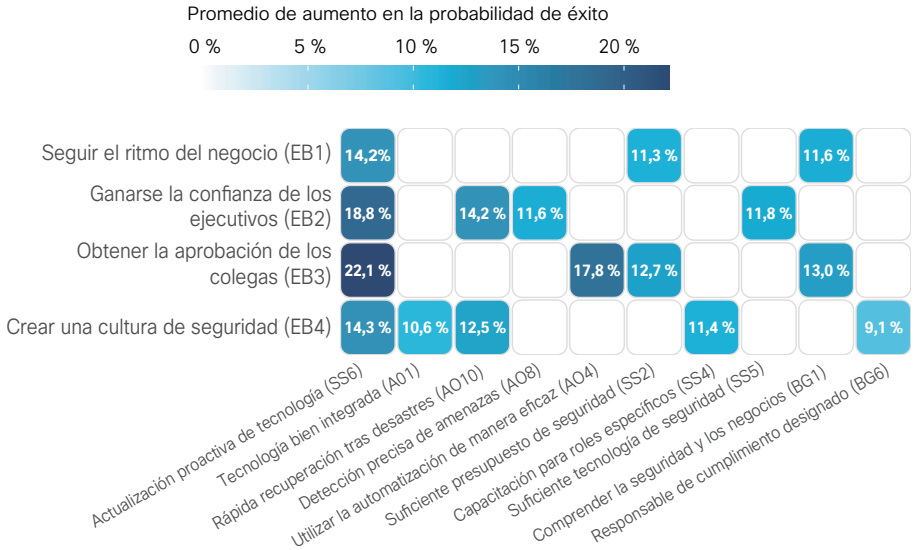
Con ese contexto, el vínculo entre la automatización y la obtención de la aprobación de los pares establecido por la Figura 10 tiene más sentido. A medida que las empresas medianas crecen y maduran, los procesos de TI se entrelazan cada vez más en múltiples grupos. La optimización de estos procesos a través de la automatización ayuda a garantizar que las cosas no se bloqueen ni se rompan en algún punto intermedio, y que todos puedan seguir haciendo lo que deben hacer en lugar de detenerse para solucionar problemas.

Los datos también refuerzan el concepto de que la seguridad y la empresa comparten una relación integral en las empresas medianas. Una mejor comprensión del rol de la seguridad en la misión más amplia mejora la aceptación de los pares en toda la empresa y ayuda a las iniciativas de seguridad a seguir el ritmo de los imperativos comerciales en evolución (consulte la Figura 11). Creemos que esto presenta una oportunidad para hacer que la capacitación en seguridad estándar (y a menudo aburrida) sea más personal e impactante. El personal de TI debe saber cómo funciona el negocio y cómo sus responsabilidades se ajustan a su misión.

Por último, pero no menos importante, la Figura 10 destaca el papel esencial que desempeña la tecnología moderna en la creación de empresas medianas seguras y exitosas. Mantener la tecnología actualizada (a menudo a través de SaaS, MSP, etc.) ayuda a fomentar la aceptación de los pares y, como verá en la Figura 11, satisface las necesidades de la empresa, gana la confianza de los ejecutivos y promueve una cultura de seguridad más sólida. Si nos pregunta, esa es una impresionante lista de logros.

Los valores en la Figura 11, y otras similares a continuación, denotan el aumento promedio en la probabilidad de éxito de un resultado dado cuando las organizaciones informan un gran cumplimiento de una determinada práctica. El sombreado corresponde a la fuerza de la correlación entre la práctica y el resultado. Las combinaciones de práctica y resultado sin sombreado o valor indican que nuestro análisis no encontró una correlación estadísticamente significativa. Eso no significa que la práctica no sea útil; solo significa que no encontramos evidencia convincente de que conduzca a un mayor éxito para ese resultado.

Figura 11: Correlación de prácticas de seguridad y resultados para permitir los negocios en empresas medianas



Fuente: Estudio de resultados en materia de seguridad de 2021 de Cisco

Eso concluye las tres prácticas de seguridad y diferenciadores de resultados principales para las empresas medianas, pero sospechamos que muchos desearán ver qué otras opciones están disponibles para ellos. Con ese fin, la Figura 11 muestra todas las prácticas que se correlacionan significativamente con cualquiera de los cuatro resultados de este objetivo. Y como se puede ver con claridad, la lista de factores de éxito es mucho más larga que tres.

Lo primero que se debe tener en cuenta con respecto a la Figura 11 es que cada resultado tiene múltiples formas en las que las prácticas de seguridad contribuyen a habilitar el negocio. Esa es una buena noticia porque sugiere que las empresas medianas pueden personalizar una ruta hacia el éxito que se adapte a sus necesidades y capacidades.

En cuanto a los factores de éxito específicos de la Figura 11, las empresas con capacidades de recuperación inmediata ante desastres informan una mayor confianza de los ejecutivos y una mejor cultura general de seguridad. La tranquilidad de que el negocio sobrevivirá (quizás incluso prospere) ante los principales eventos adversos alivia las preocupaciones en la cima y fomenta el propósito compartido en todos los niveles.

Los presupuestos suficientes ayudan a TI a mantenerse al día con las cambiantes necesidades de seguridad de la empresa. También obtienen la aceptación de sus pares, probablemente porque TI no está tomando prestados recursos de otros departamentos o porque es un obstáculo recurrente para el progreso. No todas las empresas medianas cuentan con un presupuesto de seguridad exclusivo, por lo que este mensaje puede ser bastante inoportuno para algunos lectores. Pero “suficiente”

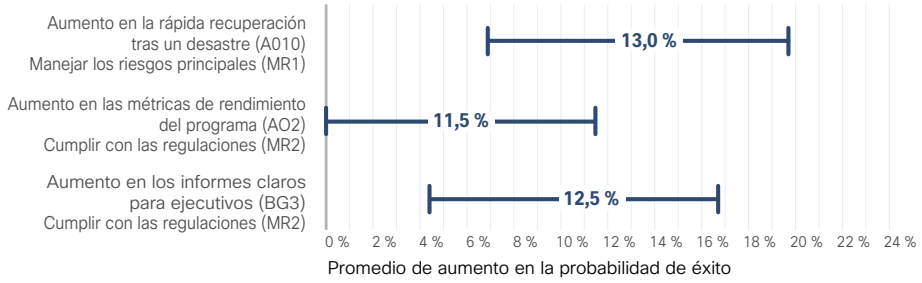
es la palabra operativa aquí, y no “dedicado” ni “ilimitado”. Este podría ser un buen punto de datos para poner al frente del liderazgo si los recursos son escasos, pero la empresa necesita avanzar rápidamente.

No dude en pasar todo el tiempo que desee con la Figura 11. Gráficos como este ofrecen una especie de giro de “elija su propia aventura” en la planificación de la seguridad. Esperamos que la utilice para llegar a donde desea ir.

Administrar el riesgo

La mayoría de las personas piensa en administrar el riesgo cuando se les pregunta sobre la responsabilidad principal de la seguridad. Por supuesto, el riesgo es multifacético, por lo que elegimos examinar tres resultados, cada uno de los cuales proporciona una perspectiva distinta de cómo las empresas medianas administran el riesgo cibernético. En la Figura 12, se destacan los conjuntos de resultados de la práctica que presentan los diferenciadores más sólidos para las empresas medianas en lo que respecta a este objetivo.

Figura 12: Tres diferenciadores de seguridad principales para administrar el riesgo en empresas medianas



Fuente: Estudio de resultados en materia de seguridad de 2021 de Cisco

No es sorprendente ver que el tema de la resiliencia se afirma una vez más entre los principales diferenciadores para administrar los principales riesgos cibernéticos y, según la Figura 13, evitar también los principales incidentes de seguridad. Según la mayoría de las cuentas, las empresas medianas enfrentan una creciente amenaza de ransomware y otros eventos de seguridad disruptivos. Mantener capacidades sólidas para recuperarse rápidamente de tales incidentes y minimizar el impacto en el negocio es imprescindible para administrar los principales riesgos cibernéticos actuales.

Los dos diferenciadores restantes de la Figura 12 comparten temas comunes de comunicación y cumplimiento. Si bien las métricas de rendimiento y los informes ejecutivos generalmente no marcan ninguna casilla en la lista de verificación de requisitos de cumplimiento, las empresas que realizan un seguimiento e informan métricas útiles probablemente estén mejor posicionadas para ofrecer evidencia a los auditores sobre el estado de los controles de seguridad regulados. El marco de trabajo de ciberseguridad del NIST (aunque no es un estándar reglamentario) ofrece este consejo: *“se alienta a las organizaciones a identificar claramente y saber por qué [las métricas] son importantes y cómo contribuirán a la administración general del riesgo de ciberseguridad”.*

En la Figura 13, se pueden encontrar prácticas adicionales de administración de riesgos que son prometedoras para las empresas medianas. La actualización tecnológica proactiva entra en escena una vez más, lo que mejora las posibilidades de lograr los tres resultados dentro del alcance de la administración de riesgos. Mantener el hardware y el software actualizados pone a las organizaciones en una mejor posición para hacer frente a cualquier amenaza o destino que se les presente. Marque otro punto para el tema de "las amenazas modernas requieren tecnología moderna". Probablemente aquí estemos viendo nuevamente los beneficios de las SaaS. El proveedor o MSP está reparando vulnerabilidades, monitoreando amenazas, respondiendo a incidentes, etc. a un costo manejable.

Figura 13: Correlación de prácticas de seguridad y resultados para la administración de riesgos en empresas medianas

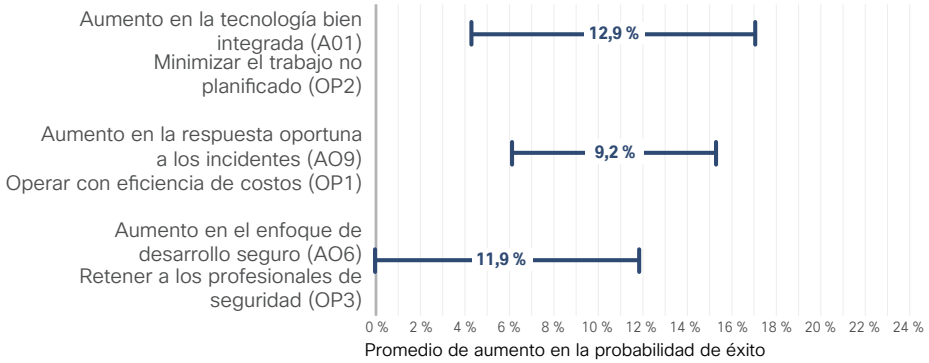
Fuente: Estudio de resultados en materia de seguridad de 2021 de Cisco

La conexión entre aprender de incidentes anteriores y evitar incidentes futuros limita con la tautología. Pero eso es exactamente para lo que está diseñada la práctica, y el hecho de que la Figura 13 indique que funciona proporciona una buena justificación para hacer el esfuerzo de hacerlo en verdad. Centrarse primero en abordar los problemas de seguridad que han afectado a su organización y a sus pares es una forma inteligente de maximizar la reducción de riesgos y minimizar los costos. Luego, puede ampliar el alcance de la corrección de riesgos desde allí. Si no conoce su historial, lo repetirá.

Operar con eficiencia

Más allá de hacer posibles los negocios y administrar el riesgo, la capacidad para operar con eficiencia suele diferenciar un excelente programa de TI de los que son buenos. Este último conjunto de resultados de nuestro estudio aborda la rentabilidad, la ejecución de la estrategia, la gestión de los profesionales y los procesos de respuesta ante incidentes. Cosas importantes, especialmente para empresas medianas.

Figura 14: Tres diferenciadores de seguridad principales para operar de manera eficiente en empresas medianas



Fuente: Estudio de resultados en materia de seguridad de 2021 de Cisco

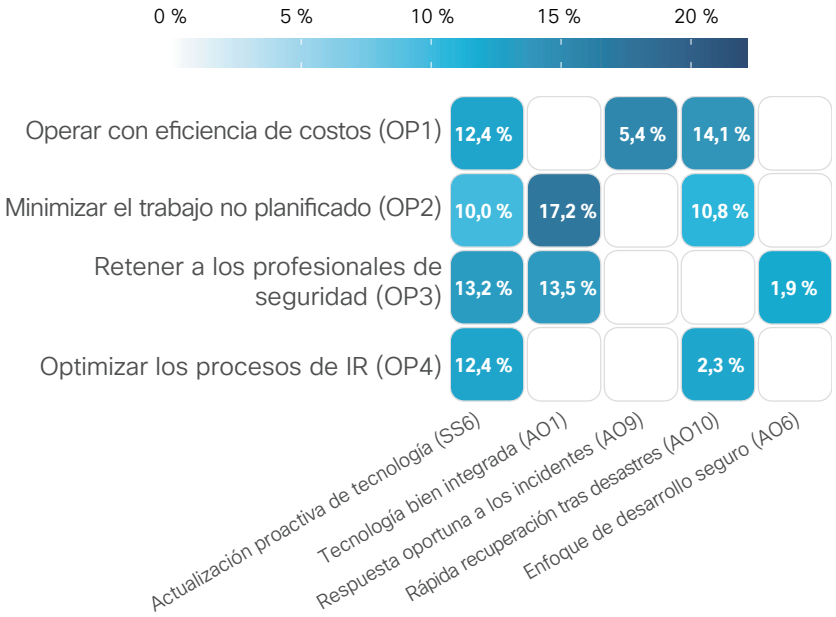
A medida que las empresas crecen, su ecosistema de TI tiende a ser más complejo y fragmentado. Como resultado, “recuerdo cuando esto solía ser tan fácil” es una queja común que acompaña a los crecientes problemas de las medianas empresas. Y esas quejas solo se intensifican a medida que tendencias como el trabajo remoto fragmentan aún más el ecosistema. La integración alivia esos problemas al permitir que las tecnologías de la información funcionen como una unidad transparente y segura, lo que minimiza el trabajo no planificado. Las personas son libres de concentrarse en proyectos importantes en lugar de tareas cotidianas y comenzar a abrumar al personal de TI con elogios de acción de gracias. (Bien, esa última parte puede ser exagerada, pero el resto es acertado).

Una gran cantidad de dinero puede desperdiciarse muy rápidamente en la “niebla de la guerra” que a menudo rodea los incidentes de seguridad. Un estudio reciente descubrió que la mala respuesta a los incidentes duplica con creces el costo medio de los grandes eventos cibernéticos.[7] Garantizar la implementación, la prueba y la práctica de un plan de IR ayuda a realizar operaciones de seguridad y TI más rentables.

Y esto nos lleva al tercer emparejamiento de resultados de la práctica en la Figura 14, que sugiere un enfoque seguro para el desarrollo de software que ayuda a retener el talento en seguridad. Es apenas un rasguño, pero recuerde que las tiendas de software son el sector más común entre los encuestados en este estudio. En vista de esto, esta correlación tiene más sentido. Un buen talento reconoce una buena práctica.

Como hemos hecho en secciones anteriores, la Figura 15 amplía la lista de prácticas de seguridad respaldadas por datos más allá de los tres diferenciadores principales. En aras de la uniformidad, comencemos con una actualización tecnológica proactiva. ¿Ha notado que esta práctica se correlaciona con cada resultado que medimos para las empresas medianas, incluidas las cuatro que se muestran aquí? Sí, la modernización de su pila de tecnología puede tener un costo, ya sea hardware, software o SaaS. Pero esto presenta evidencia convincente de que la inversión se amortizará a través de muchos otros beneficios. La mala eficiencia operativa es mucho más costosa a largo plazo que las actualizaciones periódicas de TI.

Figura 15: Tres diferenciadores de seguridad principales para operar de manera eficiente en empresas medianas



Fuente: Estudio de resultados en materia de seguridad de 2021 de Cisco

[7] Estudio de conocimientos de riesgos de la información 20/20 – Xtreme, Cyentia Institute. https://www.cyentia.com/wp-content/uploads/IRIS2020-Xtreme.pdf

Mencionamos la integración de tecnología con respecto a la Figura 14, pero la Figura 15 también la conecta con la retención de conocimientos y experiencia en seguridad. A nadie le gusta combatir la fragmentación de TI, especialmente en empresas medianas donde la expectativa es menos burocracia y tecnología heredada.

Veamos la importancia de la resiliencia en las empresas medianas. La pronta recuperación tras un desastre se correlaciona con tres de cuatro resultados asociados con este objetivo. Y así debe ser. Es difícil operar de manera eficiente cuando los períodos prolongados de interrupción detienen todo.

"Las PYMES deben recurrir a Cisco para obtener asistencia de TI. Existe la noción de que solo se centran en empresas más grandes, pero hoy en día hay muchas soluciones y programas adaptados a empresas más pequeñas también".

Gustavo Guida, jefe de marketing, Cheetah

Recursos para una seguridad exitosa en empresas medianas

El cuaderno de estrategias de ciberseguridad para empresas medianas

Pruebas gratuitas de Cisco para empresas medianas

Trabajo remoto seguro para empresas medianas

Para ver el texto completo de cada resultado y las prácticas de seguridad, junto con la explicación y los ejemplos de evidencias que se proporcionaron a los encuestados como referencia para que califiquen el éxito de sus programas, consulte el **Apéndice B y C del Estudio de resultados en materia de seguridad de 2021.**

Acerca de Cisco Secure

Ya sea que su organización sea grande o pequeña, lo más probable es que la seguridad se haya vuelto más compleja con los años. Más amenazas generan más productos específicos, lo que puede complicar aún más la investigación y la respuesta.

Durante varios años, Cisco ha estado en la misión de simplificar la seguridad. Con el lanzamiento de nuestra plataforma Cisco SecureX, hemos aportado mayor visibilidad y automatización para optimizar y fortalecer la defensa contra amenazas. SecureX integra tecnologías de Cisco y de terceros, lo que permite que diversos productos de seguridad y de TI (y equipos) trabajen juntos para una protección más completa. Al automatizar las funciones de seguridad comunes, SecureX ayuda a los equipos a hacer más con menos y a centrarse en iniciativas más estratégicas.

Los clientes pueden beneficiarse de nuestra plataforma SecureX integrada, ya sea que tengan una o varias tecnologías Cisco Secure, lo que supone una ventaja para las organizaciones de cualquier tamaño. Dado que es una plataforma nativa de la nube, SecureX le permite agregar fácilmente nuevas tecnologías y funcionalidades a medida que sus necesidades evolucionan.

Descubra cómo nuestro **portafolio de seguridad** y nuestra **plataforma integrada** pueden ayudarlo a protegerse de lo que sucede ahora y de lo que está por venir.

Comience con una **prueba gratuita**.

Sede central en América
Cisco Systems Inc
San José, CA

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

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

Publicado en abril de 2021 SMB_04_2021

cisco SECURE

CISCO

SECURE