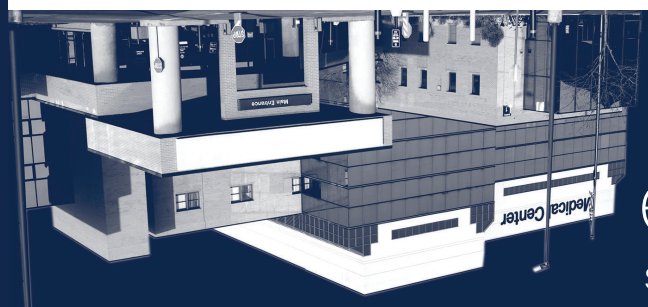
cisco SECURE

SEGURIDAD

RESULTADOS



estu

sector de

Introducción

¿Qué hace al éxito de un programa de ciberseguridad? ¿Existe evidencia de que las inversiones en seguridad logran resultados mensurables? ¿Cómo sabemos qué sirve y qué no? Este es el tipo de interrogantes al que apunta el Estudio de resultados en materia de seguridad de 2021 de Cisco. Este documento es una consecuencia de ese estudio que se centra exclusivamente en el sector de servicios de salud. Siga leyendo para descubrir qué instituciones de servicios salud se comparan con otras y qué factores clave contribuyeron al éxito de programas de seguridad como el suyo.

Para el Estudio de resultados en materia de seguridad de 2021, Cisco realizó una encuesta totalmente anónima (fuentes y encuestados) a más de 4800 profesionales de TI, seguridad y privacidad activos de todo el mundo. De esos participantes, 281 representaban a empresas del sector de servicios de salud. El instituto Cyentia Institute realizó un análisis independiente de los datos de la encuesta y generó los resultados que se presentan en este estudio.

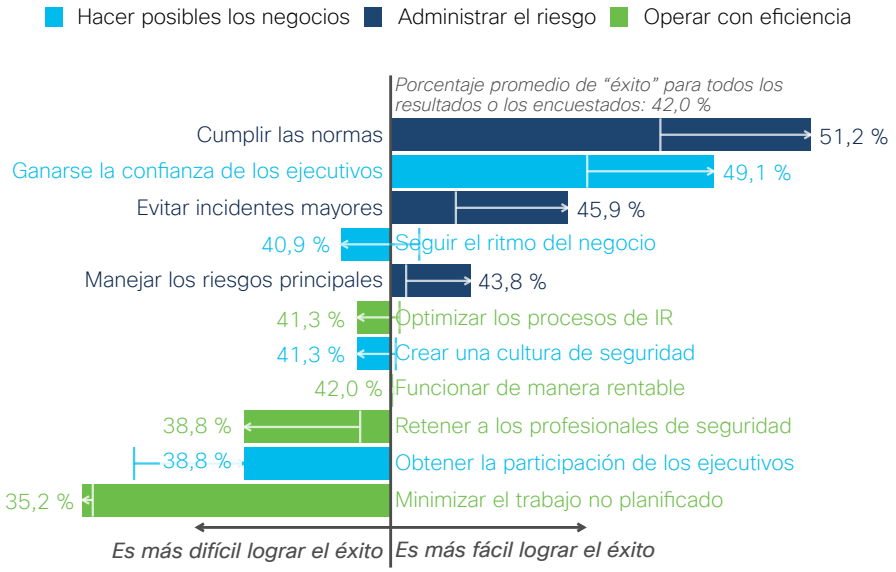
Resultados de los programas de seguridad

Les preguntamos a los encuestados sobre el nivel de éxito de su organización en 11 áreas generales de seguridad categorizadas según tres objetivos principales: hacer posibles los negocios, administrar el riesgo y operar de manera eficiente.[1] Nuestro objetivo final era identificar las prácticas de seguridad que fomentan cada uno de estos resultados, pero no nos adelantemos. Vale la pena detenerse aquí para ver dónde se destaca y dónde tiene problemas el sector de servicios de salud con estos resultados de seguridad en relación con otros sectores.

[1] Consulte el Apéndice B del Estudio de resultados en materia de seguridad de 2021 para ver el texto completo de cada resultado, 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.

En la Figura 1, se muestra el porcentaje de empresas del sector de servicios de salud que afirma que su programa de seguridad está logrando satisfactoriamente cada resultado respectivo de la lista. Por lo tanto, el 51,2 % afirma que cumple con las normas, el 49,1 % dice que los ejecutivos confían en el programa de seguridad, etc. La tasa general de éxito del programa en todas las organizaciones y los sectores es del 42 %, por lo que toda la cifra gira en torno a ese valor que marca la línea vertical. Los resultados con barras que se extienden a la derecha de esa línea tienden a ser más fáciles de lograr y los de la izquierda son más difíciles.

Figura 1: Tasas de éxito informadas para diversos resultados de seguridad en el sector de servicios de salud



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

Al igual que con el estudio principal, los resultados en el objetivo "Administrar el riesgo" generalmente muestran mayores niveles de éxito; aquellos en "Operar con eficiencia" parecen tener más dificultades, y "Hacer posibles los negocios" abarca toda la gama. Sin embargo, aquí es donde terminan las similitudes, porque los programas de seguridad en el sector de servicios de salud informan tasas de éxito variadas bastante difíciles de predecir.

¿Tiene curiosidad por saber cómo podemos hacer tal afirmación? Genial, debería tenerla. Analicemos los detalles sutiles de la Figura 1 que lo prepararán para tomar su propia decisión sobre el éxito relativo del sector de servicios de salud en lo que respecta a la seguridad. ¿Ve esa línea blanca vertical en el medio de la barra "Cumplir las normas"? Ese es el promedio general en todos los sectores del Estudio de resultados en materia de seguridad de 2021. Como se mencionó antes, la longitud total de la barra corresponde a la tasa de éxito de las instituciones de salud. Por lo tanto, esa línea horizontal con la flecha hacia la derecha muestra el aumento relativo del éxito informado para ese resultado (desde alrededor del 48 % en general hasta alrededor del 51,2 % para el sector de servicios de salud).

Los demás resultados pueden leerse de manera similar, pero preste atención a la dirección de la flecha. Si analizamos la Figura 1, vemos que el sector de servicios de salud supera el objetivo en cinco resultados, no lo alcanza en cinco y lo logra en dos. Uno de esos dos es una calificación del éxito general del programa de seguridad. Por lo tanto, podemos concluir que, en general, el sector de servicios de salud parece estar a la altura de lo que vemos en otros sectores en cuanto al éxito general de los programas de seguridad. Pero, ¿es posible que a su organización le vaya mejor? Nuestros datos dicen que sí. Continúe con la siguiente sección para saber cómo las instituciones de salud potenciaron el rendimiento de sus programas de seguridad.

Factores clave para el éxito

Además de los resultados anteriores, indagamos sobre la eficacia de los participantes del estudio para respetar un conjunto de 25 prácticas comunes en el ámbito de la seguridad.[2] Luego realizamos un análisis estadístico multivariable para medir cuáles de estas prácticas se relacionan más estrechamente con lograr exitosamente cada uno de los objetivos. En otras palabras, ¿qué factores contribuyen al éxito de los programas de seguridad entre las organizaciones del sector de servicios de salud? Veamos.

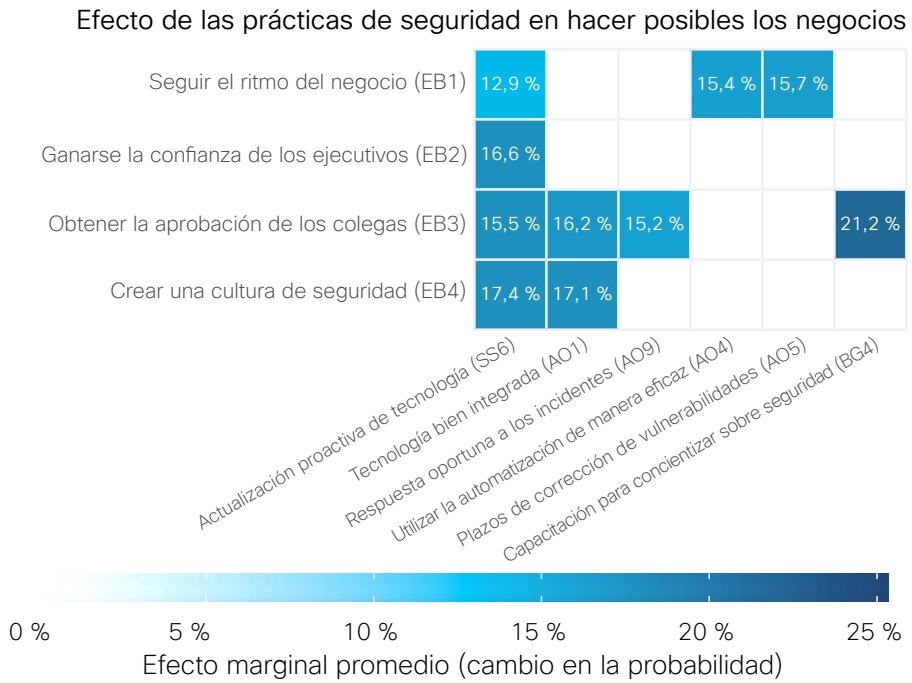
Valores de las figuras

Los valores en las Figuras 2 a 4 denotan el aumento promedio en la probabilidad de éxito de un resultado dado cuando las organizaciones informan un gran cumplimiento de una práctica específica. Entonces, por ejemplo, los resultados indican que una estrategia de actualización tecnológica proactiva aumenta las posibilidades del programa de seguridad de mantenerse al día con el negocio en un promedio de 12,9 % (cuadro superior izquierdo). Las combinaciones de práctica y resultado sin sombreado o valor indican que nuestro análisis no encontró una correlación estadísticamente significativa, lo que no implica que la práctica no sea útil. Simplemente no es un factor clave de éxito según los datos.

Hacer posibles los negocios

Como dice la etiqueta, este objetivo se centra en la misión del programa 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 2, se destacan varios factores que mejoran considerablemente la capacidad de los programas de seguridad de servicios de salud para hacer justamente eso.

Figura 2: Contribución de las prácticas de seguridad a los resultados asociados con hacer posibles los negocios



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

La actualización tecnológica proactiva desempeña un papel importante en todos los resultados del objetivo "Hacer posibles los negocios" de las instituciones de salud. El valor de la mejor infraestructura moderna no se puede subestimar. Este también fue un tema en todo el informe principal y, en todo caso, los resultados son aún más sólidos para los servicios de salud.

[2] 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.

Podemos afirmar esto también como una conversación: los que permiten que su infraestructura se degrade y solo la actualizan cuando se rompe obtuvieron tasas de éxito significativamente reducidas para hacer posibles los negocios.

También podemos analizar más profundamente los resultados. Si está interesado en fomentar una mentalidad de seguridad en toda su organización, una tecnología bien integrada va de la mano con las actualizaciones proactivas de tecnología. La inclusión de la capacitación en concientización sobre la seguridad sirve como un recordatorio de que los programas de seguridad exitosos no se centran solo en la tecnología. Aquí vemos que la capacitación aumenta significativamente la aceptación de los pares en toda la organización. Esto debería ser un gran aliciente para pensar en la capacitación en concientización sobre la seguridad como algo más que una casilla de verificación para satisfacer a los reguladores.

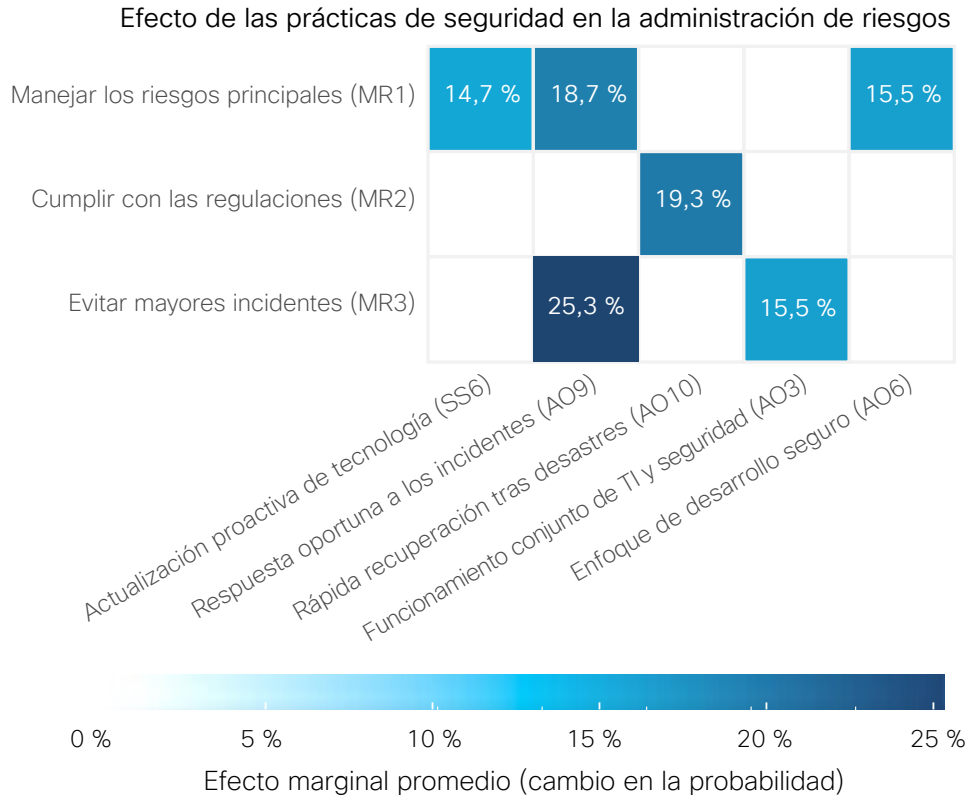
Es posible que veamos alguna correlación inversa aquí. Es difícil saber si una tecnología bien integrada genera equipos bien integrados, o viceversa. Probablemente sea un poco de ambas.

Por último, la automatización y los plazos específicos de corrección de vulnerabilidades ayudan a que la seguridad se mantenga al día con el negocio. Esos tres a menudo forman el pilar de las operaciones de seguridad y completan la conocida tríada de "personas, procesos, tecnología" de los programas de seguridad.

Administrar el riesgo

La mayoría de las personas piensa en administrar el riesgo cuando se les pregunta sobre la responsabilidad principal del programa de 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 la organización administra el riesgo.

Figura 3: Contribución de las prácticas de seguridad a los resultados asociados con la administración de riesgos



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

La actualización proactiva de tecnología aparece nuevamente como uno de los tres factores principales para reforzar las capacidades de administración de los principales riesgos cibernéticos que enfrenta la organización. Para adaptar un dicho popular: “La tecnología antigua no puede aprender a enfrentar nuevas amenazas”.

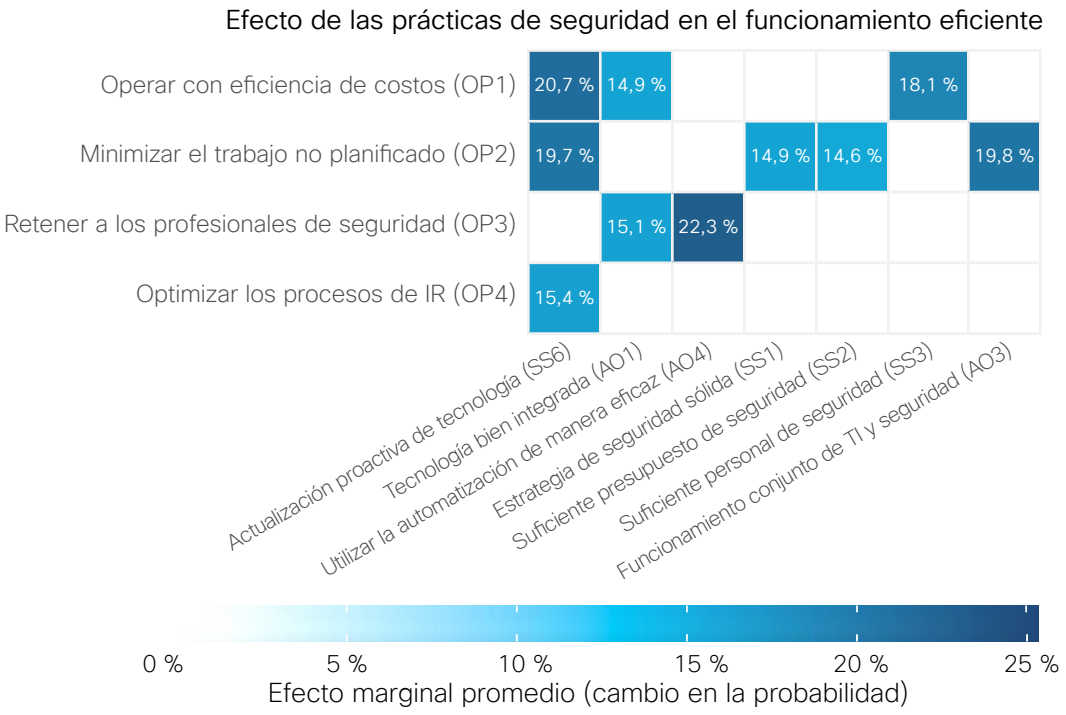
Las prácticas de respuesta oportuna a los incidentes y pronta recuperación tras desastres van de la mano y sirven como un buen recordatorio de que la gestión de riesgos no se trata solo de prevenir eventos de seguridad. Mitigar el impacto de esos eventos cuando ocurren es igual de importante. La asociación entre la recuperación tras desastres y el cumplimiento nos pareció extraña al principio, pero teniendo en cuenta cómo el ransomware paralizó a tantas instituciones de salud, sospechamos que los auditores podrían estar analizando estas capacidades.

Los dos últimos factores enumerados en la Figura 3 también parecen estar relacionados. Cuando varios equipos técnicos trabajan juntos, incluso durante el ciclo de vida de desarrollo de software, las instituciones de salud están mejor posicionadas para administrar los principales riesgos y evitar incidentes importantes. Es una buena receta para mejorar la colaboración y la cohesión entre los equipos de TI, seguridad y desarrollo.

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 seguridad de los que solo 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, ¿verdad? Veamos cómo puede ganar ventaja su programa.

Figura 4: Contribución de las prácticas de seguridad a los resultados asociados con operar con eficiencia



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

En esta sección, aparecen de nuevo algunas de las mismas prácticas de seguridad a fin de ayudar a las empresas a operar con eficiencia, mientras que también aparecen algunos métodos nuevos. En particular, una estrategia de actualización proactiva de tecnología es la única práctica que impulsa el éxito en los tres objetivos principales del programa de seguridad (y en 8 de 11 resultados). Si se toma el ejemplo de la medicina basada en la evidencia, este es un caso muy convincente para el tratamiento.

Centrarse en mejorar la integración de la tecnología, que afecta positivamente a 4 de los 11 resultados, también parece una decisión bien justificada. Esto también se sincroniza con la experiencia: "La infraestructura heredada y fragmentada conduce a operaciones eficientes", dijo nadie nunca.

El vínculo entre la automatización y la retención de profesionales es interesante. Sospechamos que las organizaciones que implementan esta práctica liberarán a su personal de seguridad de tareas mundanas y aburridas para centrarse en un trabajo más desafiante y gratificante. Es mucho más probable que los empleados con trabajos gratificantes se queden.

Omitiremos las siguientes tres prácticas de seguridad por ahora (no se preocupe, volveremos a ellas) para abordar rápidamente el factor de éxito más a la derecha, porque también lo vimos antes. Creemos que es muy intuitivo que los equipos técnicos que trabajan juntos minimicen el trabajo no planificado y el esfuerzo desperdiciado.

Eso nos deja con los tres métodos nuevos de la Figura 4, y parecen estar en un orden lógico. Establezca una estrategia de seguridad sólida, cuente con presupuesto suficiente para implementar esa estrategia y con el personal adecuado para que suceda. Obviamente es más fácil decirlo que hacerlo, pero es bueno saber que hay pruebas sólidas de que la implementación de componentes básicos como ese realmente genera mejores resultados de seguridad.

> "Debido a que defender nuestra red y nuestros datos contra malware, ransomware, suplantación de identidad (phishing) y otras amenazas puede ser, literalmente, un asunto de vida o muerte, necesitábamos una manera de ofrecer la máxima seguridad con un impacto mínimo en nuestras operaciones y la atención a los pacientes".
>
> Lee Cullivan, director general de seguridad de la información, Boston Medical Center

Acerca de Cisco Secure

En Cisco, 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 el portafolio Cisco Secure y la plataforma Cisco SecureX. Trabajamos para el 100 % de las empresas de Fortune 100, a fin de brindarles protección mediante la plataforma de ciberseguridad más completa e integrada del planeta. Sepa más sobre cómo simplificamos las experiencias, aceleramos el éxito y protegemos el futuro en cisco.com/go/secure.

También puede obtener más información sobre las soluciones de Cisco para la ciberseguridad de los servicios de salud en nuestro sitio web, o en uno de nuestros muchos blogs:

- Ciberseguridad de los servicios de salud: ¿Qué hay en juego?
- Protección de los dispositivos conectados a Internet en la nueva era de los servicios de salud
- Por qué los proveedores de servicios de salud necesitan soluciones seguras de telemedicina

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

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

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

Publicado en diciembre de 2020 HCRPT_12_2020

cisco SECURE

Estudio de resultados en materia de seguridad de Cisco

Lo invitamos a leer el Estudio de resultados en materia de seguridad global, aprovechar datos interactivos y ver videos cortos con algunos hallazgos clave en cisco.com/go/SecurityOutcomes.

Consulte también nuestra serie de blogs Estudio de resultados de seguridad y siga la conversación en las redes sociales mediante #SecurityOutcomes.

CISCO

SECURE