Serie de Reportes de Ciberseguridad de Cisco 2020

Reporte para Pequeña y Mediana Empresa

Seguridad

Gran seguridad en un mundo de pequeñas empresas

10 mitos sobre la ciberseguridad de las pymes

El puente a lo posible

Contenido

¿Su ciberseguridad protege a su organización según lo previsto?

Si es propietario o trabaja para una pequeña o mediana empresa (también conocida como pyme), ya ha superado desafíos importantes. Desde aumentar el capital inicial y saber cuándo contratar, hasta administrar los costos operativos y diseñar estrategias para escalar... es difícil. Emocionante, significativo y personal... pero difícil.

Y al enfrentarse a una situación sin precedentes, como tratar de mantener sus operaciones a flote en una pandemia o recesión, ¿cómo se administra? ¿En qué debe centrarse para mantenerse seguro? ¿Cómo protege a su organización de ciberataques si está operando con personal reducido?

Esos instintos emprendedores surten efecto. En tiempos de crisis, por necesidad, surgen ideas nuevas mientras se adapta a nuevos enfoques para trabajar. A pesar de todo, encuentra maneras de mantenerse productivo y competitivo.

¿La ciberseguridad desempeña un papel importante cuando hay muchos otros problemas emergentes a tener en cuenta?

Claro que sí. Este informe está diseñado para brindarle información exacta sobre cómo la ciberseguridad puede desempeñar un papel fundamental en potenciar a las pequeñas y medianas organizaciones para que no solo sobrevivan, sino que prosperen y aceleren su éxito. ¿Cómo lo hacemos? Mediante el uso de datos para derribar los mitos generalizados que están desorientando las suposiciones de seguridad de las pymes.

El sector de la seguridad a menudo ha sido injustamente duro con las pequeñas y medianas empresas en lo que respecta a reconocer cómo se prioriza la ciberseguridad. Podría parecer como si los proveedores lo complacieran, suponiendo que no toma a la seguridad con seriedad, y prosiguieran a explicarla ("ciberexplicarla", podría decirse).

Este informe, basado en una encuesta de casi 500 pymes (organizaciones de 250 a 499 empleados) revela que no solo toman la seguridad muy en serio, sino que su enfoque innovador y empresarial hacia la seguridad también resulta rentable. Es hora de derribar algunos mitos sobre la manera en que las pymes utilizan sus recursos de ciberseguridad.

Usaremos los resultados anuales de nuestra encuesta de parámetros de CISO y los resultados de conversaciones con pequeñas y medianas empresas para echar por tierra algunos mitos, sobre temas como cuántas pymes tienen departamentos dedicados a la búsqueda proactiva de amenazas y los tipos de amenazas cibernéticas a las que se enfrentan.

En otras palabras, estaremos poniendo bajo la lupa los factores clave que están afectando su ciberseguridad. Por ejemplo, aprendimos sobre las consecuencias que una infraestructura obsoleta puede tener en una intrusión y la duración. También aprendimos que cuanto más proveedores utiliza, mayor será el tiempo de inactividad desde su intrusión más grave. Exploraremos sus estrategias más impactantes y presentaremos datos que demuestren que sus empresas se recuperan con mayor rapidez luego de una intrusión de datos de lo se esperaba en el sector.

Por si todas las presiones de ser una empresa pequeña no fueran suficientes, ahora es evidente que las presiones externas pueden obligar a una parte o a toda su fuerza laboral a ser remota en algún momento. Como afirmó recientemente en su boletín de noticias Graham Cluley, analista independiente de ciberseguridad y blogger: “Podemos estar trabajando desde casa, pero los hacks siguen llegando”. Es posible que debamos adaptarnos a maneras de trabajar diferentes a las que estamos acostumbrados y, en tiempos de crisis, es fundamental priorizar.

Lo que este informe pretende hacer es destacar qué estrategias están funcionando. Esperamos que esto ayude con las decisiones que está tomando sobre cómo usted y su fuerza laboral administrarán la seguridad en el futuro y cómo la ciberseguridad puede ayudarlo a acelerar su éxito.

> “La seguridad desempeña un papel importante en nuestra organización. Realizamos funciones de back-end para tres cooperativas de ahorro y crédito en los Estados Unidos, así como un centro de llamadas combinado. La seguridad nos ayuda a reunir los aspectos clave de nuestro negocio para la eficiencia operativa”.
>
> Kevin Hatch, ingeniero de Redes,
> Open Technology Solutions

Explorando 10 mitos

Posturas de seguridad de pymes frente a grandes empresas

Para evaluar los mitos comunes sobre las posturas de seguridad de las pymes, comparamos las respuestas de la encuesta en diversas funcionalidades de ciberseguridad de las pymes (de 250 a 499 empleados) en comparación con las organizaciones más grandes (500 empleados o más).

Lo que descubrimos en nuestros datos de investigación derribó varios mitos. Aquí, investigamos esos mitos y brindamos datos para refutarlos, lo que deja a las pymes mejor paradas frente a la seguridad de lo que se pensaba.

Notas:

1. Para los fines de esta investigación, definimos las pequeñas y medianas empresas, o “pymes”, como organizaciones de 250 a 499 empleados. Tenga en cuenta que los datos de la encuesta pueden ser diferentes en las organizaciones con menos de 250 empleados.
2. Se redondearon todos los porcentajes y hemos omitido el pequeño porcentaje de respuestas “No sé” a las preguntas de la encuesta. Por estos motivos, es posible que la cuenta no siempre sume 100 % en los gráficos proporcionados. Fuente de datos de la encuesta: Estudio de parámetros de CISO de 2020.

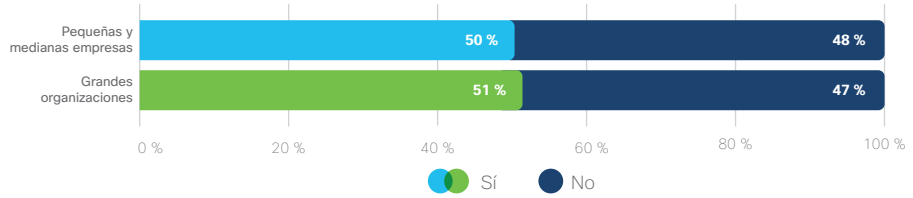
Mito 1: Solo las grandes organizaciones se enfrentan al escrutinio público, en todas sus formas

Un mito común es que los medios de comunicación solo quieren hablar sobre las intrusiones masivas y devastadoras de datos corporativos o gubernamentales. Esto podría llevar a algunas organizaciones más pequeñas a creer que no deberán afrontar mucho escrutinio público, si lo hubiera, al sufrir un ataque cibernético.

FALSO: el año pasado, las organizaciones más pequeñas enfrentaron el mismo nivel de escrutinio público que sus colegas más grandes.

En la figura 1, se muestra que no hay pruebas sustanciales sobre una diferencia entre las pymes y las organizaciones más grandes en lo que respecta a enfrentar el escrutinio público.

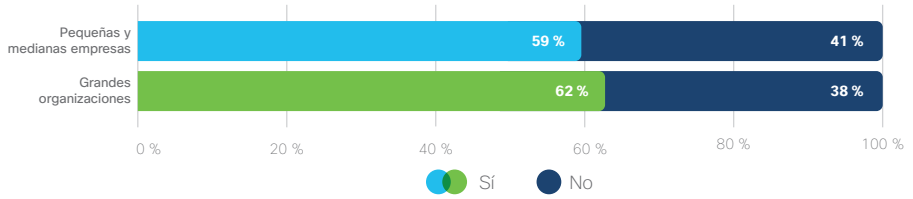
Figura 1. ¿Alguna vez su organización tuvo que enfrentarse al escrutinio público tras una intrusión a la seguridad? Pyme N = 481; 500 + N = 2319.



Fuente: Informe de Cisco Gran seguridad en un mundo de pequeñas empresas, 2020

En segundo lugar, el 59 % de las pymes revelaron voluntariamente su intrusión de datos más importante el año pasado (en comparación con el 62 % de las empresas más grandes). Esto sugiere que las empresas más pequeñas se toman seriamente su compromiso con los clientes y partners.

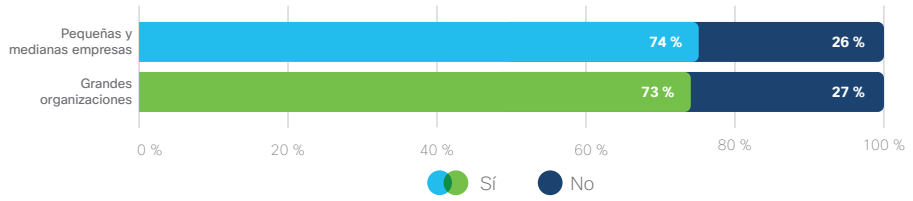
Figura 2. ¿La intrusión de seguridad más importante del año pasado que tuvo que administrarse bajo el escrutinio público fue de público conocimiento debido a la divulgación voluntaria de su organización? Pyme N = 241; 500 + N = 1190.



Fuente: Informe de Cisco Gran seguridad en un mundo de pequeñas empresas, 2020

En tercer lugar, las empresas más pequeñas están desbordadas de consultas de los clientes sobre cómo están manejando sus datos, frente a no recibir consultas. El 74 % de las pymes nos comentaron que los clientes o clientes potenciales han realizado estas consultas (similar al 73 % de las organizaciones más grandes). Esto demuestra que los clientes se preocupan de que sus datos personales sigan siendo privados independientemente de quién los tenga y que es crucial el elemento de confianza hacia quien los brindan.

Figura 3. ¿Sus clientes o clientes potenciales consultan sobre la privacidad de los datos y el manejo de la información personal? Pyme N = 432; 500 + N = 2117.



Fuente: Informe de Cisco Gran seguridad en un mundo de pequeñas empresas, 2020

La razón por la que las pymes están recibiendo estas consultas es que las normativas y la gestión de riesgos del proveedor van en descenso. Comienza con las grandes empresas. Luego, las grandes empresas auditan a sus proveedores, las empresas medianas. Y luego, un par de años después, las organizaciones medianas auditan

a sus proveedores, las empresas más pequeñas. Impulsadas por las intrusiones o la privacidad de los datos, las pymes no son inmunes a la investigación y deben considerarse tan responsables como sus equivalentes más grandes.

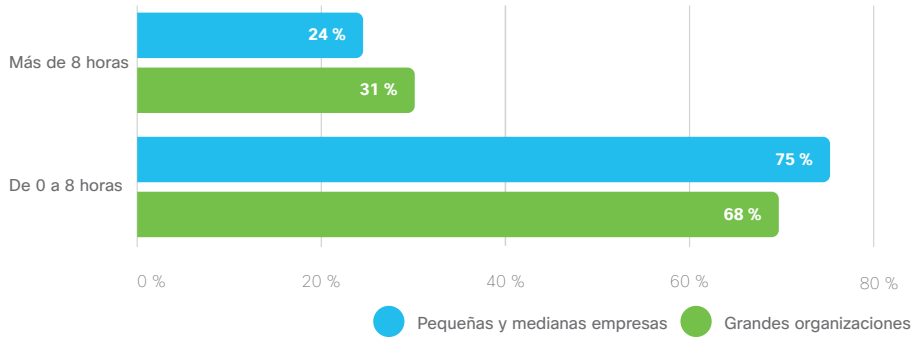
Mito 2: Las empresas más grandes sufren menos tiempo de inactividad y se recuperan más rápido de los ataques

Cuando una pyme se ve golpeada por un ataque cibernético que da lugar a un nivel de inactividad (pérdida de horario comercial), el mito sugiere que no tienen los recursos para recuperarse tan rápido como sus equivalentes más grandes.

FALSO: nuestros datos sugieren que hay muy poca diferencia en la cantidad de tiempo de inactividad que sufren las pymes y las organizaciones más grandes.

Si resumimos algunos de estos hallazgos, podemos ver que el 24 % de las pymes se enfrentó a tiempos de inactividad de más de ocho horas el año pasado debido a su intrusión más grave a la seguridad, un poco por debajo de las organizaciones más grandes en 31 %.

Figura 4. Volviendo a pensar en la intrusión de seguridad más grave que su organización administró el año pasado, ¿cuánto tiempo estuvieron caídos los sistemas debido a la intrusión? Pyme N = 388; 500 + N = 1877.



Fuente: Informe de Cisco Gran seguridad en un mundo de pequeñas empresas, 2020

También comparamos estas cifras con el informe sobre pymes “Pequeño pero poderoso” de Cisco de 2018 y se han realizado algunas mejoras significativas en los últimos dos años para las organizaciones más pequeñas. Hace dos años, el 40 % de las pymes sufrió un tiempo de inactividad de más de ocho horas luego de la intrusión más grave.

Es necesario reconocer aquí que una grave intrusión puede provocar grandes interrupciones en empresas de cualquier tamaño. No se trata de quién tiene los mayores niveles de tiempo de inactividad, sino de lo que puede hacer su pyme para garantizar que sus recursos no se extiendan más allá de sus capacidades. Aquí es donde la automatización puede ser un multiplicador de fuerzas para proporcionar alertas tempranas y una rápida recuperación para minimizar el tiempo de inactividad y mantener su negocio a flote en estos momentos de adversidad. Según nuestro Informe de referencia de CISO 2020, la mayoría (77 %) de los encuestados de las organizaciones de todos los tamaños planean aumentar la automatización para simplificar y acelerar la respuesta en sus ecosistemas de seguridad durante el próximo año.

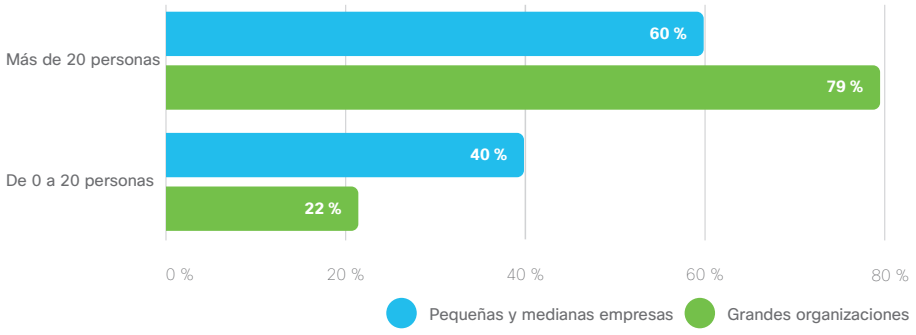
Mito 3: Las pymes carecen de personal dedicado a la seguridad

Con todos colaborando en lo que sea necesario en las pymes, se supone que la ciberseguridad es solo un aspecto del trabajo de alguien. Y que esta persona también está equilibrando otros aspectos de la administración de TI, como la administración de centros de datos y la evaluación del nuevo hardware. El mito es que las pymes tienen pocos recursos dedicados, si los hubiera, para la ciberseguridad.

FALSO: si bien este puede ser el caso para algunos, masivamente las pymes nos dijeron que cuentan con empleados dedicados a la ciberseguridad. De hecho, menos del 1 % de las pymes nos dijo que no tenía a nadie dedicado a la seguridad. Quizás aún más sorprendente, el 60 % afirmó que contaba con más de 20 personas dedicadas a la seguridad, aunque no especificamos el nivel de participación que puede implicar la dedicación o si los empleados eran subcontratados con un proveedor de servicios de seguridad administrados (MSSP).

¿Y cómo se compara con las empresas más grandes? El porcentaje de organizaciones más grandes que tienen más de 20 personas dedicadas a la seguridad es significativamente mayor (79 %), lo cual es de esperar.

Figura 5. ¿Cuántos empleados en su organización están dedicados a la seguridad? Pyme N = 481; 500 + N = 2319.



Fuente: Informe de Cisco Gran seguridad en un mundo de pequeñas empresas, 2020

Estas cifras muestran que las pymes tienen más recursos de seguridad dedicados de los que quizás se pensaba. ¿Esto significa que la escasez de talentos de ciberseguridad ya no es un problema para las pymes?

Sin duda no iríamos tan lejos.

Las pymes nos dijeron que la falta de personal capacitado es en realidad su tercer desafío más grande. Su principal desafío son las restricciones de presupuesto, seguida de la compatibilidad con los sistemas antiguos. El tercer lugar está vinculado al personal capacitado y las prioridades de la competencia conjunta.

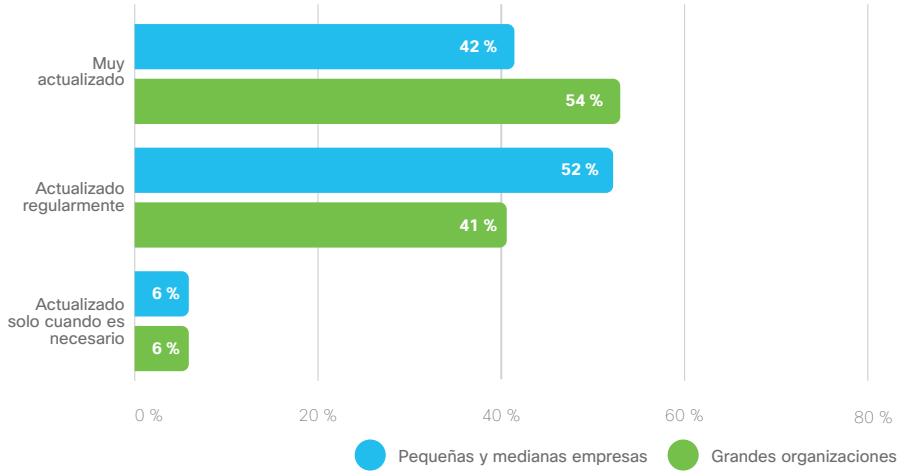
Considere esto como un signo del desafío de ciberseguridad que enfrentan las empresas más pequeñas: reconocen que son un objetivo y que los ataques contra ellos son cada vez más sofisticados. Para combatirlo, se están colocando en la mejor posición posible. Y para las organizaciones de pymes, eso significa invertir en las personas adecuadas.

Mito 4: Las grandes empresas tienen infraestructuras más actualizadas

Con la frecuencia de los consumidores que se actualizan al smartphone más reciente, puede parecer que las organizaciones más grandes pueden permitirse reemplazar cada elemento de su infraestructura de seguridad. Pero ¿qué sucede con las empresas más pequeñas, donde esa inversión ciclada podría tener mayor impacto en su presupuesto de TI anual?

PARCIALMENTE CIERTO: al pedirles que describan sus infraestructuras y su estrategia para invertir y reemplazar las tecnologías de seguridad clave es cuando las pymes nos dijeron que casi todas las pymes son perseverantes en mantener su infraestructura actualizada.

Figura 6. ¿Cómo describiría la infraestructura de seguridad de su organización? Pyme N = 481; 500 + N = 2319.



Fuente: Informe de Cisco Gran seguridad en un mundo de pequeñas empresas, 2020

Es cierto que las pymes no tienen infraestructuras tan actualizadas como las empresas más grandes (el 54 % de las grandes empresas afirma que están muy actualizadas, en comparación con el 42 % de las pymes). Sin embargo, un 94 % colectivo de pymes afirma que se actualiza periódica o constantemente. Por lo tanto, la gran mayoría ciertamente no se aferra a los equipos antiguos hasta que se vuelven obsoletos e inseguros.

Para las pymes, se trata de maximizar lo que tienen, en lugar de perseguir cada nuevo producto de seguridad. Muchas veces, hemos visto a nuestros clientes de pymes pensar con originalidad para ampliar aún más su seguridad.

> "Como empresa pequeña, necesitamos la mayor cantidad de información de la menor cantidad de sistemas posibles para maximizar la eficiencia. Nuestra solución de seguridad basada en la nube (Cisco AMP para Endpoints) ha demostrado ser un sistema crucial para operar toda nuestra infraestructura. No solo es importante para proteger los recursos, sino que también brinda acceso instantáneo a la información de la máquina, los entornos de usuario y la generación de informes para ayudar con la solución de problemas de Centro de Asistencia. Esto elimina la necesidad de contar con un sistema de software independiente. Somos capaces de aprender y adaptarnos constantemente al funcionar de esta manera".
>
> Alan Zaccario, vicepresidente de Tecnología de la información y ciberseguridad, New Castle Hotels and Resorts

Mito 5: Las pymes enfrentan amenazas diferentes a las de las empresas más grandes

Los delincuentes cibernéticos quieren el premio más grande, por lo que usarán sus tácticas más discretas y peligrosas contra las empresas más grandes, ¿verdad?

PARCIALMENTE CIERTO: comparamos los tipos de ciberataques que informaron las pymes y las grandes empresas que han experimentado en el último año con la cantidad de tiempo de inactividad (pérdida de horario comercial) que provocaron los ataques. Lo hicimos con cuatro categorías en función de la cantidad de empleados en la organización y clasificamos los eventos más propensos a crear más de 24 horas de tiempo de inactividad.

Figura 7. La cantidad de empleados se correlacionan con el tiempo de inactividad en horas debido a la mayoría de las intrusiones graves en el último año y qué tipo de ataque lo provocó. 250–499 N = 388; 500–999 N = 746; 1000–9999 N = 863; 10 000 + N = 268.

Fuente: Informe de Cisco Gran seguridad en un mundo de pequeñas empresas, 2020

Los resultados son interesantes en términos de cuáles son las amenazas que causan más daño. Lo que descubrimos es que el ransomware no discrimina. Para las pymes y las grandes empresas, el ransomware fue la principal amenaza más probable de causar más de 24 horas de tiempo de inactividad del sistema.

En cambio, DDoS raramente provoca el mayor impacto para las organizaciones más pequeñas, pero es el tercer tipo de ataque más destructivo en términos de tiempo de inactividad para organizaciones de más de 10 000 empleados. En cambio, se informa que la suplantación de identidad (phishing) es un gran problema para las organizaciones pequeñas, pero está muy por debajo en la escala para las organizaciones más grandes.

Los atacantes que implementan un malware limpiador tienen el único propósito de destruir o alterar los sistemas o los datos. Para las pymes y las empresas con más de 10 000 empleados, el malware limpiador provocó un tiempo de inactividad de entre 17 y 24 horas en el último año. A diferencia del malware que contiene datos de rescate (ransomware), cuando un agente malicioso decide utilizar un limpiador en sus actividades, no hay ninguna motivación financiera directa. Para las empresas, a menudo este es el peor tipo de ataque, ya que no hay expectativas de recuperación de datos.

Las credenciales robadas también parecen ser un problema significativo para las pymes, lo que provocó un promedio de 17 a 24 horas de inactividad en el último año.

También debe tenerse en cuenta que algunos agentes de amenazas se especializan en ciertas empresas de tamaño, mercados verticales o regiones geográficas. Por lo tanto, si bien las tácticas pueden ser comparables (como se muestra en la figura anterior), los agentes de amenazas son diferentes.

Mito 6: Las pymes no realizan la búsqueda de amenazas de manera proactiva

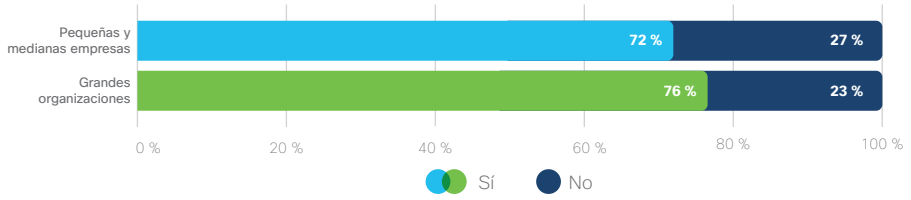
La búsqueda de amenazas es un ejercicio proactivo de seguridad, con la intención de encontrar y erradicar a los atacantes que han penetrado su entorno sin encender la alarma. Esto contrasta con las investigaciones tradicionales y las respuestas que provienen de las alertas que aparecen luego de que se haya detectado una actividad potencialmente maliciosa.

Todo el concepto de búsqueda de amenazas parece como si implicara la investigación de una misteriosa escena del crimen, con sus matices y complejidad fuera del alcance de las empresas más pequeñas. Las pymes tienen las manos llenas tratando de investigar las alertas; no tienen tiempo de buscar otras amenazas, ¿verdad?

FALSO: a partir de los datos de la encuesta, no solo el 72 % de las pymes tiene empleados dedicados a la búsqueda de amenazas, sino que también se acerca al porcentaje de organizaciones grandes que tienen un departamento de búsqueda de amenazas.

Aunque sus niveles de madurez pueden diferir de las organizaciones más grandes debido a la menor cantidad de recursos, nuestros datos sugieren que las pymes reconocen el valor de un enfoque proactivo hacia la ciberseguridad y lo están adoptando.

Figura 8. ¿Su organización cuenta con un departamento o equipo interno dedicado a la búsqueda de amenazas? Pyme N = 481; 500 + N = 2319.



Fuente: Informe de Cisco Gran seguridad en un mundo de pequeñas empresas, 2020

Puede leer más sobre la práctica de la búsqueda de amenazas y cómo se están desempeñando otras empresas en nuestro informe reciente, Caza de amenazas ocultas: incorporación de la búsqueda de amenazas en su programa de seguridad.

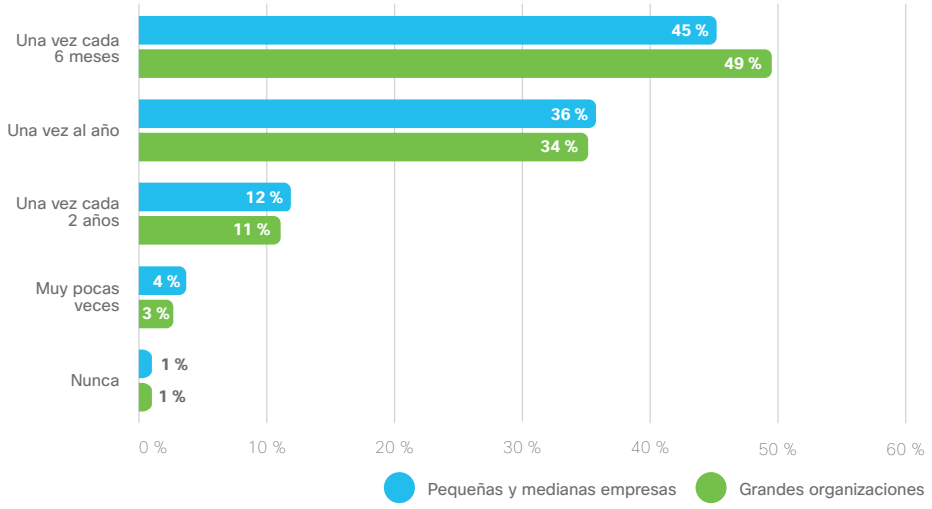
Mito 7: Las empresas más pequeñas no prueban sus planes de respuesta ante incidentes con simulacros/ejercicios

Como solía decir Mike Tyson: “todo el mundo tiene un plan hasta que reciben un puñetazo en la cara”. Hasta que sepa cómo funciona su plan de respuesta ante incidentes, solo valen las palabras en la página.

Pero las empresas más pequeñas no cuentan con lujo de tiempo y los recursos para poner a prueba sus planes, ¿verdad? Seguramente esto causará más interrupciones de lo que merece.

FALSO: este mito simplemente no es cierto. Solo el uno por ciento de las pymes nunca prueba su plan y el cuatro por ciento raramente lo hace. El 12 % prueba cada dos años, el 36 % prueba anualmente y el mayor porcentaje (45 %) prueba cada 6 meses.

Figura 9. ¿Con qué frecuencia su organización realiza un simulacro o ejercicio para probar el plan de respuesta de su empresa frente a un incidente de ciberseguridad? Pyme N = 481; 500 + N = 2319.



Fuente: Informe de Cisco Gran seguridad en un mundo de pequeñas empresas, 2020

¿Cómo se compara esto con las empresas más grandes? Los resultados son muy similares, por lo que la noción de que las pymes no planifican tan bien como las empresas más grandes se derriba en el contexto de la respuesta ante incidentes.

Mito 8: Por algún motivo, el liderazgo de las pymes no se toma seriamente la seguridad y la privacidad de los datos

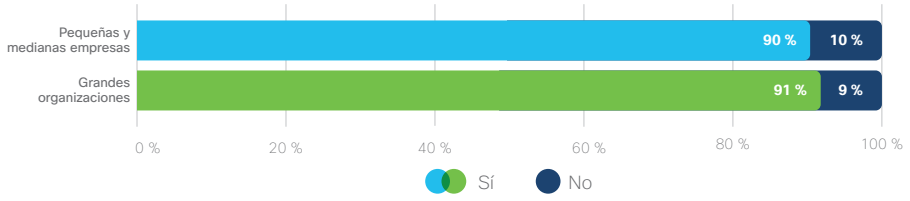
Este es el grande: el que la industria colectiva desafortunadamente ha estado propagando durante años. Como pyme, está en la penumbra en cuanto al peligro en el que se encuentra y no ha cultivado una cultura organizativa en torno a la seguridad y la privacidad de los datos.

FALSO: nuestros datos demuestran que este mito está muy alejado de la realidad. Y hay tres maneras de demostrarlo a partir de nuestra encuesta de los responsables de la toma de decisiones de TI de organizaciones de diferentes tamaño.

Privacidad de los datos

En primer lugar, nuestros datos demuestran que el 90 % de los encargados de tomar decisiones de TI dentro de las pymes afirma que está familiarizado con su programa de privacidad de datos, en comparación con el 91 % en empresas más grandes; no es una gran diferencia.

Figura 10. ¿Generalmente está familiarizado con el programa de privacidad de datos en su organización? Pyme N = 481; 500 + N = 2319.

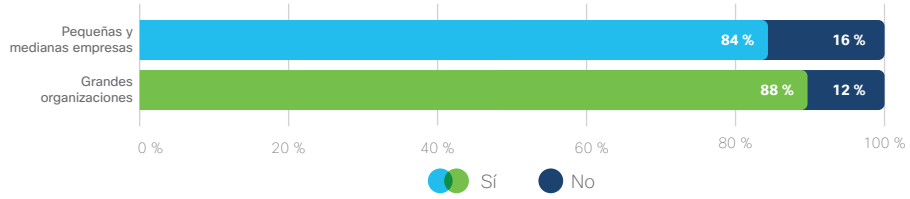


Fuente: Informe de Cisco Gran seguridad en un mundo de pequeñas empresas, 2020

Capacitación sobre concientización en seguridad

En segundo lugar, en el 84 %, la mayoría de las organizaciones pyme hacen obligatoria la capacitación en concientización sobre seguridad y solo a un ritmo ligeramente menor que las organizaciones más grandes.

Figura 11. ¿Es obligatoria la capacitación en concientización sobre ciberseguridad de los empleados en su organización? SMB N = 464; 500 + N = 2272.

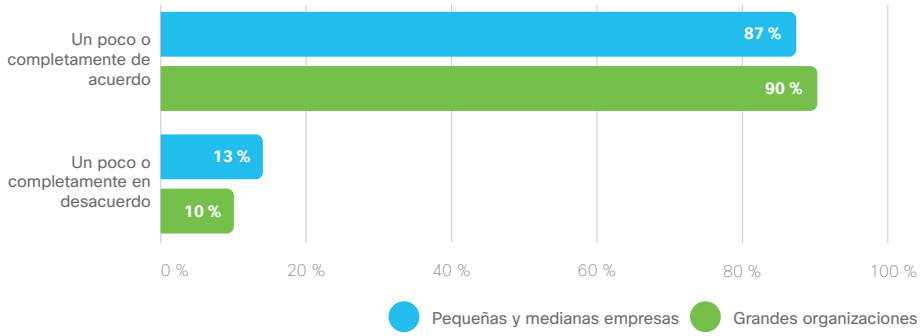


Fuente: Informe de Cisco Gran seguridad en un mundo de pequeñas empresas, 2020

Participación de ejecutivos

En tercer lugar, el 87 % de los ejecutivos en las pymes coincide que la seguridad es una alta prioridad. Esto es solo tres puntos porcentuales detrás de las empresas más grandes.

Figura 12. Los líderes ejecutivos de mi organización consideran que la seguridad es de absoluta prioridad. Pyme N = 481; 500 + N = 2319.

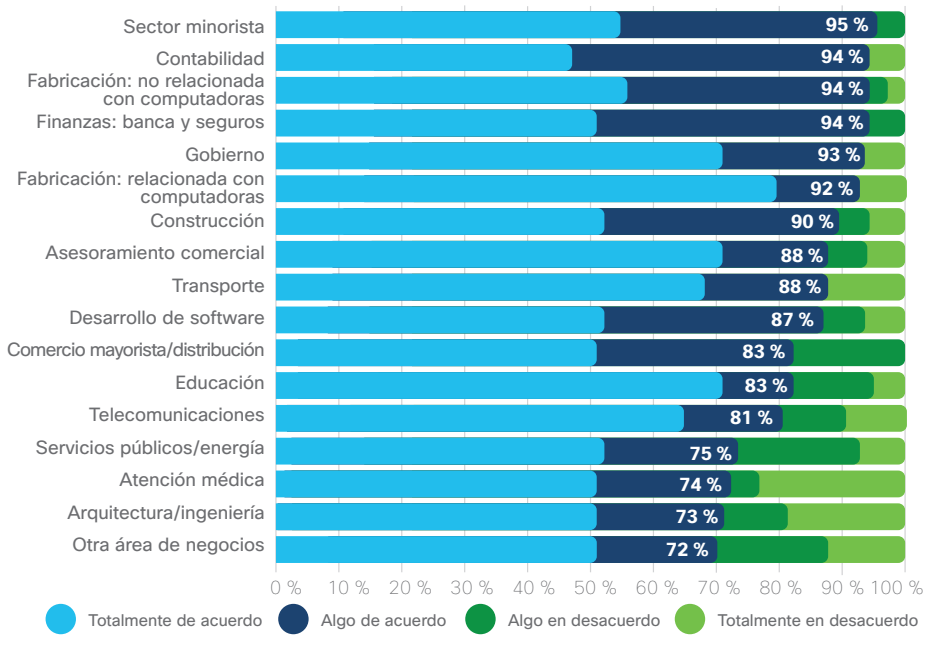


Fuente: Informe de Cisco Gran seguridad en un mundo de pequeñas empresas, 2020

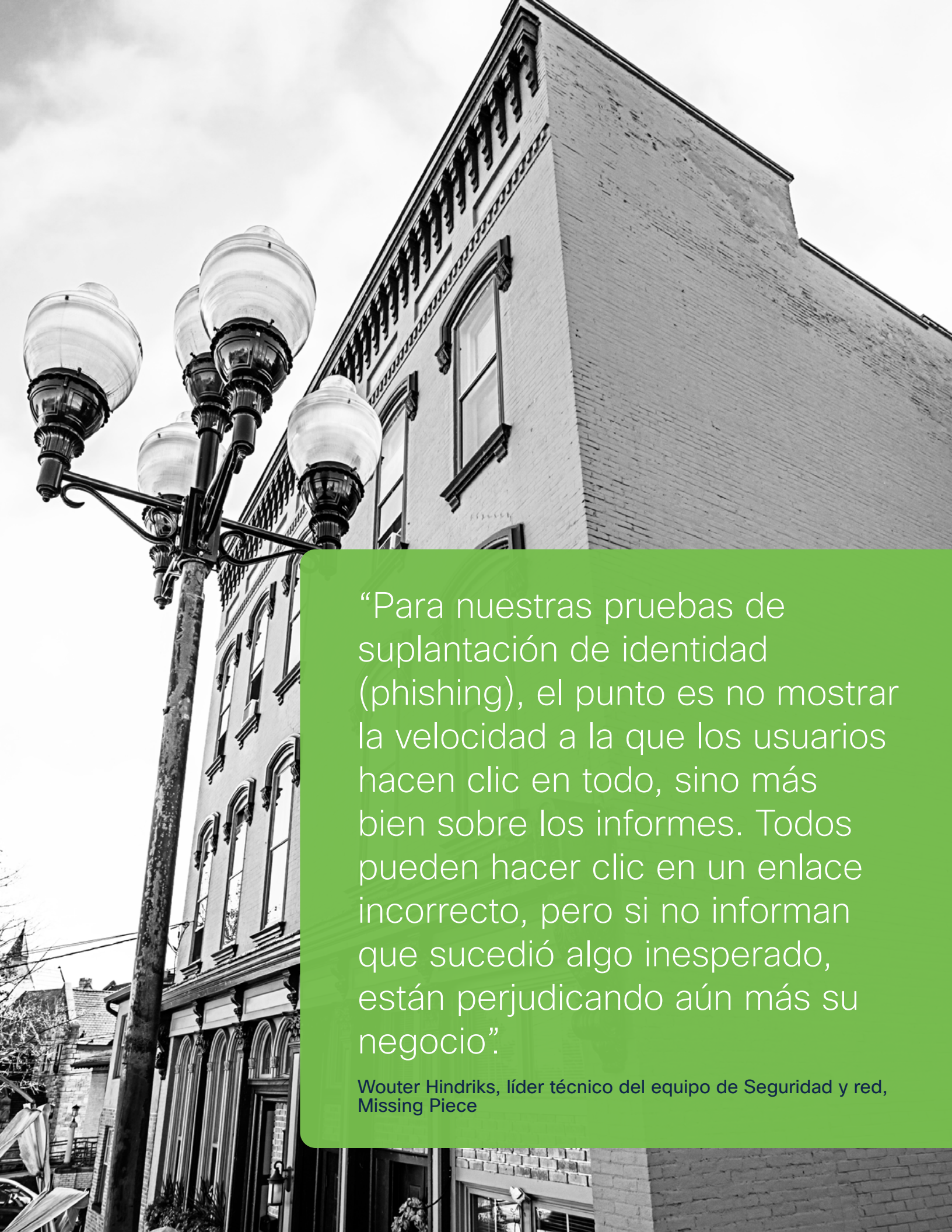
A menudo escuchamos a nuestros clientes decir (y estamos de acuerdo) que la seguridad debe penetrar en toda la empresa para tener algún efecto y que el soporte ejecutivo es fundamental para poner en funcionamiento la seguridad. Esto es tan cierto para una pyme como lo es para una organización más grande y, en la mayoría de los casos, es más fácil de lograr en un entorno posiblemente más ágil.

En base a los hallazgos de estas tres preguntas de la encuesta, descubrimos que las pymes, de hecho, han cultivado las culturas de la organización en torno a la seguridad y la privacidad de los datos. Más de dos tercios de los encuestados en todos los sectores afirmaron que su liderazgo ejecutivo consideró que la seguridad era una alta prioridad (vea la figura 13 que muestra solo respuestas de las pymes).

Figura 13. Los líderes ejecutivos de mi organización consideran que la seguridad es de absoluta prioridad. SMB N = 481.



Fuente: Informe de Cisco Gran seguridad en un mundo de pequeñas empresas, 2020



“Para nuestras pruebas de suplantación de identidad (phishing), el punto es no mostrar la velocidad a la que los usuarios hacen clic en todo, sino más bien sobre los informes. Todos pueden hacer clic en un enlace incorrecto, pero si no informan que sucedió algo inesperado, están perjudicando aún más su negocio”.

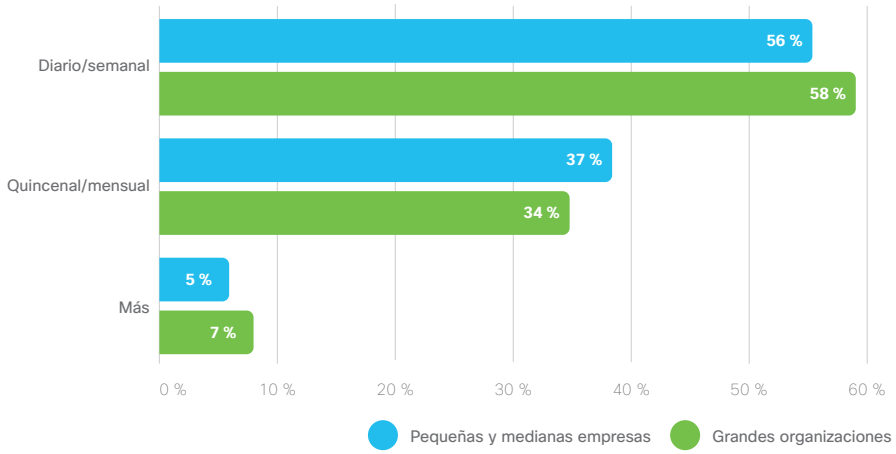
Wouter Hindriks, líder técnico del equipo de Seguridad y red, Missing Piece

Mito 9: Las organizaciones más pequeñas no aplican parches a las vulnerabilidades regularmente

Los parches a menudo se encuentra en los principios básicos de la ciberseguridad, pero en la práctica, pueden ser difíciles de implementar. Un mito sugiere que las pymes prefieren usar sus recursos en otro lugar que encontrar maneras de minimizar la interrupción causada por los parches.

FALSO: el 56 % de las pymes aplican parches diariamente o semanalmente, en comparación con el 58 % de las grandes empresas, lo que muestra que, para las rutinas de aplicación de parches muy habituales, todos los tamaños de negocios se aproximan.

Figura 14. ¿Con qué regularidad su empresa aplicó parches a las vulnerabilidades divulgadas en el software? Pyme N = 481; 500 + N = 2319.



Fuente: Informe de Cisco Gran seguridad en un mundo de pequeñas empresas, 2020

Nuestros datos demuestran que las empresas y las organizaciones con entre 500 a 999 empleados son los más propensas a sufrir un incidente de una vulnerabilidad conocida, lo que demuestra que aquellos en la categoría de pyme son realmente más eficaces en la aplicación de parches a vulnerabilidades conocidas que algunas empresas más grandes, lo que genera menos incidentes.

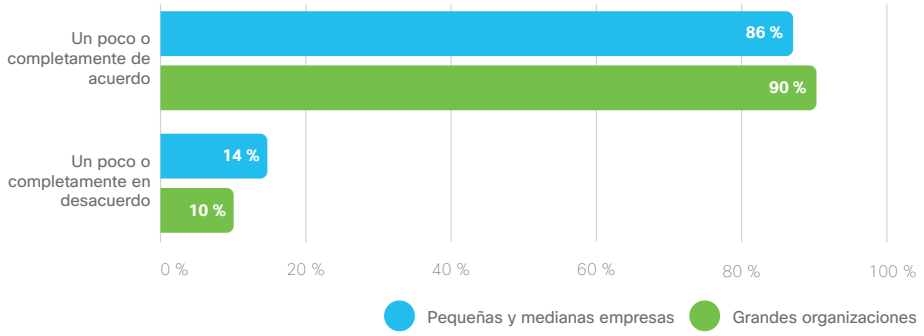
La aplicación de parches es fundamental como defensa inicial, como se define, por ejemplo, en los Estados Unidos por la SP 800-53 del NIST y el Center for Internet Security® (CIS®). Y las pymes lo comprueban.

Mito 10: Las pymes no pueden medir la eficacia de sus programas de seguridad

Se han efectuado suposiciones de que las empresas más pequeñas emplean más de un enfoque de “disparar y rezar” por la ciberseguridad. Lo que implica es que no tienen implementadas las medidas para poder monitorear y medir lo que realmente funciona y, por lo tanto, no pueden optimizar lo que tienen.

FALSO: un sorprendente 86 % de las pymes afirma que cuentan con métricas claras para evaluar la eficacia de su programa de seguridad, en comparación con el 90 % de las organizaciones más grandes.

Figura 15. El equipo ejecutivo de mi organización ha definido métricas claras para evaluar la eficacia de nuestro programa de seguridad. Pyme N = 481; 500 + N = 2319.



Fuente: Informe de Cisco Gran seguridad en un mundo de pequeñas empresas, 2020

Los datos de nuestra encuesta demostraron que existe una diferencia mínima en el uso de métricas claras, independientemente del tamaño de la organización. Esto puede deberse en parte a la manera en que los productos de ciberseguridad han evolucionado a lo largo de los años: los mejores están diseñados para brindar indicadores muy claros de lo que están encontrando, y lo que esto significa, a fin de facilitar la generación de informes.

Pero con la importancia de “no se puede arreglar lo que no se puede medir”, las pymes podrían desempeñarse mejor, ya que solo el 46 % respondió que *están totalmente de acuerdo* en que sus ejecutivos han definido métricas claras, en comparación con el 53 % de las grandes organizaciones.

Aprovechar las oportunidades para optimizar su seguridad

Si bien hemos demostrado que las pymes merecen una reputación mucho mejor por tener prácticas de seguridad sólidas, es evidente que aún hay un deseo de realizar mejoras. En el panorama actual de proveedores, no es fácil contar con la seguridad adecuada y no queremos pintar una panorama totalmente optimista y poco realista.

Agotamiento de la ciberseguridad

Definimos al agotamiento de la ciberseguridad como prácticamente renunciar a anticiparse a los agentes de amenazas maliciosas e, increíblemente, las empresas más pequeñas están sufriendo precisamente el mismo nivel de agotamiento de la ciberseguridad que las empresas más grandes. Tanto las pymes como las grandes empresas llegan al 41 % de los encuestados que experimentan agotamiento mientras que el 58 % no. Es evidente que hay un deseo y una necesidad de ser más eficientes en la administración de la seguridad.

Adopción de la concientización sobre ciberseguridad por parte de los empleados

Las pymes y las organizaciones más grandes que tenían dificultades para lograr que los usuarios adoptaran programas de concientización sobre ciberseguridad no mostraron diferencias significativas en el tiempo de inactividad.

Es evidente que sabemos que los usuarios tienen un impacto: pueden ser su primera línea de defensa. Sin embargo, no se trata de considerar que los usuarios son “el eslabón más débil”. En cambio, se trata de involucrar a los usuarios en su estrategia de seguridad para que la adopción se convierta en algo común.

La democratización de la seguridad es un tema que Wendy Nather, jefa del consejo de asesoría CISO en Cisco, presentó como una presentación participativa en la conferencia RSA 2020. (También puede escuchar una entrevista con Wendy en el podcast de historias de seguridad de Cisco).

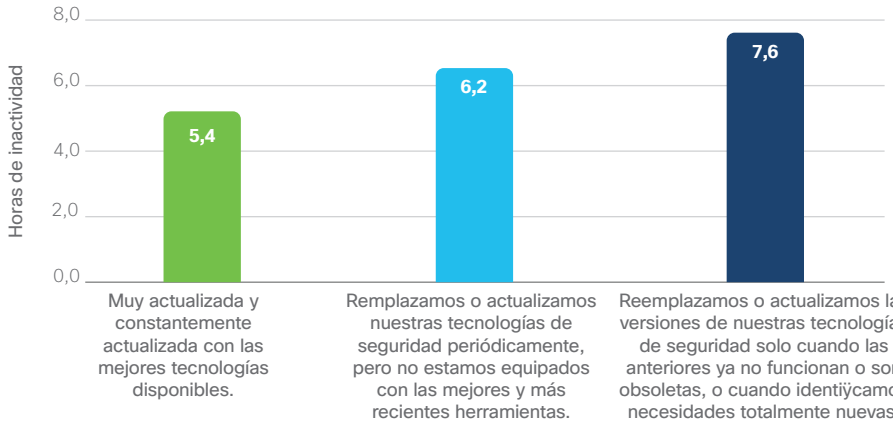
“En lugar de señalar a todos los que caen en uno de nuestros ataques simulados de suplantación de identidad (phishing), celebramos a todos los que lo denuncian. Mida el comportamiento que está intentando fomentar”.

Wendy Nather, jefa de asesoría de los CISO, Cisco

Reducción del tiempo de inactividad

¿Es cierto que cuanto más antiguo sea su hardware y software, menos eficaz serán en derrotar amenazas nuevas y emergentes? Nuestros datos parecen respaldar esta teoría en el caso de las pymes.

Figura 16. ¿Cómo describiría la infraestructura de seguridad de su organización correlacionada con la cantidad de horas de inactividad que resultan de la intrusión más impactante del año pasado? SMB N = 481.



Fuente: Informe de Cisco Gran seguridad en un mundo de pequeñas empresas, 2020

Los encuestados de las pymes que afirmaron que solo reemplazan o actualizan sus tecnologías de seguridad cuando ya no trabajan experimentaron 7,6 horas de inactividad luego de su intrusión más grave el año pasado. Aquellos que nos dijeron que cuentan con una infraestructura muy actualizada experimentaron 5,4 horas.

¿Eso significa que estamos alentándolo a tirar todo por la borda y solo adquirir la última herramienta? No, en absoluto. Nuestra experiencia con la ciberseguridad ha demostrado que es más importante centrarse en la integración de lo que tiene que aún está funcionando, en lugar de dejar que se vuelva obsoleta y complementarla con tecnologías más nuevas según sea necesario.

Si le preocupa que su infraestructura esté desactualizada, hay algunos aspectos a tener en cuenta. El más importante es garantizar que tenga la flexibilidad para hacer frente a los cambios. Idealmente, debe ofrecer la automatización y el análisis integrados que colaboran en la administración de políticas y dispositivos, la detección de amenazas desconocidas y la coordinación de la respuesta y el cambio de políticas.

Averigüe si su plataforma puede aplicar análisis para identificar anomalías de comportamiento en el tráfico de red en la nube y en las instalaciones. Debe poder hacerlo, al tiempo que aplica políticas y adapta automáticamente el acceso a la red y las aplicaciones para los terminales comprometidos.

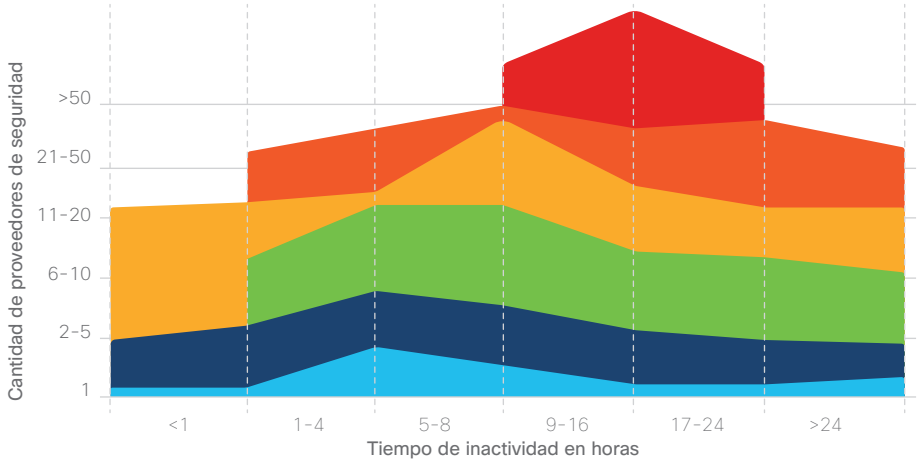
Para obtener más información, lea 5 Questions to Ask Your Security Platform Vendor.

Complejidad del proveedor

Para muchas organizaciones, la propagación del riesgo de seguridad puede parecer implicar un aumento de proveedores. Pero, ¿cuáles son las consecuencias de este enfoque? ¿Cuán difícil es administrar un entorno de varios proveedores y tener más proveedores amplía su cobertura, lo que genera una mejor seguridad al reducir el tiempo de inactividad?

Increíblemente, mientras más proveedores utilizaban los encuestados de las pymes, más tiempo de inactividad informaron desde su intrusión más grave. Se pasó de un promedio de cuatro horas con un proveedor a un promedio de más de 17 horas con más de 50 proveedores, lo que es un aumento de más de cuatro veces.

Figura 17. Cantidad de proveedores de seguridad utilizados en el entorno de seguridad [pyme N = 472] y tiempo de inactividad de los sistemas debido a la mayor intrusión de seguridad administrada en el último año [pyme N = 388].



Fuente: Informe de Cisco Gran seguridad en un mundo de pequeñas empresas, 2020

Como queda claro en la figura 17, cuantos más proveedores tenga (de abajo hacia arriba), mayor será el tiempo de inactividad (de izquierda a derecha). No solo la expansión de los proveedores en un entorno típico de seguridad de pymes provoca una complejidad innecesaria y flujos de trabajo ineficientes, sino que también puede hacer o interrumpir su negocio en términos de tiempo de inactividad del sistema.

Una gran táctica para mitigar los complejos desafíos provocados por un entorno de varios proveedores es adoptar una plataforma abierta basada en el portafolio que permita que sus soluciones funcionen en conjunto.

Recursos para proteger su recorrido hacia el futuro

Para resumir,nuestros datos muestran que las pymes se han estado tomando la seguridad con seriedad en su planificación estratégica y operaciones diarias. Estas son muy buenas noticias para usted.

Sin embargo, como también demostró nuestro Estudio de parámetros de CISO 2020, todos los días afloran nuevos desafíos de seguridad.

Y para las pymes, se magnifica la presión para continuar y aumentar el negocio. Sumemos a esto una fuerza laboral móvil y remota cada vez mayor y tenemos la tormenta perfecta.

Para ayudarlo en este proceso, visite nuestro sitio web dedicado a sus pequeñas o medianas empresas Soluciones de seguridad para pequeñas empresas. Y estos son algunos recursos adicionales para ayudarlo a usar la ciberseguridad para acelerar su éxito:

- El fin de la contraseña... Por fin,
- Cloud Security para el futuro de su negocio
- Selector de productos para pequeñas empresas
- 3 consejos para elegir un firewall de próxima generación para pequeñas empresas
- Casos de estudio de pequeñas empresas

En Cisco, construimos nuestra plataforma de seguridad con la idea de que las soluciones de seguridad deben funcionar como equipo: aprender unas de otras, escucharse mutuamente y responder como una unidad coordinada. Creemos que este es un enfoque sistemático que simplifica la seguridad y la hace más eficaz.

Cisco SecureX integra su infraestructura existente para una experiencia uniforme. Unifica la visibilidad, permite la automatización y fortalece la seguridad en toda la red, los terminales, la nube y las aplicaciones.

Protección de su fuerza laboral remota

En este momento, el cambio abrupto hacia el soporte masivo de trabajadores remotos crea una serie de desafíos de seguridad para mantener funcionando a su organización en un entorno muy diferente. Esto ejerce una tensión repentina en los equipos de TI y de seguridad a los que se les está encomendando rápidamente la tarea de brindar soporte para una cantidad sin precedentes de trabajadores fuera del sitio y sus dispositivos, sin comprometer la seguridad.

Para cualquier pyme que se adapte a una postura de trabajo más remota, ¿cómo se mantiene segura? Teniendo en cuenta esta nueva realidad, necesita una manera simple y sencilla de proteger a los trabajadores remotos a la velocidad y la escala de sus negocios.

Cisco quiere ayudarlo a permitir que sus empleados trabajen de forma remota y segura. Le recomendamos los siguientes pasos:

- **En primer lugar, domine los aspectos básicos** que hemos analizado en este informe: aplicación de parches a vulnerabilidades, capacitación de empleados, implementación de acceso de confianza cero con autenticación de varios factores (MFA) y protección de la red, los terminales, la nube y las aplicaciones.
- **En segundo lugar, equilibre la seguridad con la facilidad de uso.** Los empleados no deberían tener que leer la mente para saber qué saben los especialistas en seguridad. Tienen sus propios trabajos que hacer. Haga que la seguridad sea accesible para que sea perfecta para sus trabajos.
- **Y, en tercer lugar, asóciese con proveedores de seguridad** que lo ayudan a simplificar su infraestructura de seguridad, no a complicarla. Nuestros datos demuestran que existe una correlación con menos tiempo de inactividad de las intrusiones al involucrar a menos proveedores (y más estratégicos).

Para ver artículos, webinars y ofertas útiles para que su organización permanezca conectada de manera segura, visite: Cisco Secure Remote Worker.

Acerca de nuestros expertos

La seguridad de Cisco cuenta con una consejo de asesoría CISO formada por antiguos CISO que poseen una gran cantidad de conocimientos sobre ciberseguridad con antecedentes en una variedad de sectores. Además de proporcionar su información, orientación y experiencia para informar las recomendaciones que ofrecemos en la serie de informes sobre ciberseguridad, también respaldan a nuestros vendedores, partners y clientes en cuestiones como la protección de la transformación digital al cumplimiento, la privacidad, el monitoreo y la visibilidad, la confianza cero y la inteligencia de amenazas. Si desea hablar con un miembro de nuestro equipo de asesoría CISO, comuníquese con asktheciso@external.cisco.com.

Acerca de la serie de informes sobre ciberseguridad de Cisco

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

El Departamento de Seguridad de Cisco realiza una serie de publicaciones basadas en investigaciones e impulsadas por datos bajo el banner “Serie de ciberseguridad de Cisco”. Hemos ampliado la cantidad de títulos a fin de incluir diversos informes para profesionales de seguridad con intereses diferentes. Invocando la amplitud y profundidad de conocimientos de los investigadores de amenazas e innovadores en el sector de seguridad, los informes de la serie de este año incluyen el Estudio de parámetros de privacidad de datos, el Informe de amenazas y el Estudio de parámetros de CISO; otros se publicarán a lo largo del año.

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

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

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

Publicado en mayo de 2020 SMB_05_2020

cisco Segura

Seguridad