SOPHOS

CIBERSEGURIDAD: EL RETO HUMANO

Resultados de una encuesta independiente a 5000 directores de TI de 26 países

Monográficos de Sophos Octubre de 2020

Introducción

El papel de los profesionales cualificados en materia de ciberseguridad nunca ha sido más crítico. Si bien los avances en automatización y tecnología han desempeñado un papel importante en el fortalecimiento de las ciberdefensas de las empresas, los programas de seguridad realmente efectivos siguen precisando del componente humano.

La importancia que siguen teniendo los profesionales de la seguridad se explica en gran parte por la evolución de los ciberataques. Detrás de cada ciberamenaza hay un ciberdelincuente, y los ataques avanzados de hoy en día a menudo combinan la última tecnología con el hacking manual en vivo. La protección contra estos ataques llevados a cabo por seres humanos requiere la experiencia humana.

Este amplio estudio permite sacar nuevas conclusiones sobre el estado de los conocimientos y recursos de ciberseguridad en todo el mundo. Revela las realidades a las que se enfrentan los equipos de TI en cuanto a la prestación de ciberseguridad llevada a cabo por humanos y explora la forma en que las empresas responden a los retos que se les presentan.

En el estudio también se exponen datos únicos sobre la relación entre el hecho de que una empresa se vea afectada por el ransomware y sus prácticas diarias de ciberseguridad.

Acerca de la encuesta

Sophos encargó a la empresa de investigación especializada Vanson Bourne que encuestara a 5000 directores de TI de 26 países entre enero y febrero de 2020. Sophos no desempeñó ningún papel en la selección de los encuestados y todas las respuestas se proporcionaron de forma anónima.

PAÍS	N.º DE ENCUESTADOS
Australia	200
Bélgica	100
Brasil	200
Canadá	200
China	200
Colombia	200
República Checa	100
Francia	300
Alemania	300

PAÍS	N.º DE ENCUESTADOS
India	300
Italia	200
Japón	200
Malasia	100
México	200
Países Bajos	200
Nigeria	100
Filipinas	100
Polonia	100

PAÍS	N.º DE ENCUESTADOS
Singapur	200
Sudáfrica	200
España	200
Suecia	100
Turquía	100
EAU	100
Reino Unido	300
Estados Unidos	500

Dentro de cada país, el 50% de los encuestados pertenecían a organizaciones de entre 100 y 1.000 empleados, mientras que el 50% pertenecía a organizaciones de entre 1.001 y 5.000 empleados. Los encuestados procedían de diversos sectores, tanto públicos como privados.

SECTOR	N.º DE ENCUESTADOS
TI, tecnología y telecomunicaciones	979
Venta al por menor, distribución y transporte	666
Fabricación y producción	648
Servicios financieros	547
Sector público	498
Servicios empresariales y profesionales	480
Construcción y propiedad	272
Energía, petróleo/gas y servicios públicos	204
Medios de comunicación, ocio y entretenimiento	164
Otros	542

Resumen ejecutivo

Los equipos de TI están mostrando progresos en muchas batallas

- **Los equipos de TI están al día con los parches de seguridad.** Tres cuartas partes de los equipos de TI aplican parches en ordenadores de sobremesa, servidores, aplicaciones y dispositivos abiertos a Internet en el plazo de una semana desde su publicación. Los parches de los servidores y recursos con conexión a Internet se aplican más rápidamente, y el 39 % de los encuestados los aplica en un plazo de 24 horas.
- **La prevención tiene prioridad.** De media, los equipos de TI dedican casi la mitad de su tiempo (45 %) a la prevención, el 30 % a la detección y el 25 % restante a la respuesta.
- **Los directores de TI están al día con la ciberseguridad.** La mayoría dice que tanto ellos (72 %) como sus equipos (72 %) están al día con las ciberamenazas o por delante de ellas. Solo el 11 % opina que están considerablemente por detrás.

La mejora de la ciberseguridad precisa de personas, que escasean

- **La búsqueda de amenazas realizada por humanos es una necesidad urgente.** El 48 % de los encuestados ya la ha incorporado en sus procedimientos de seguridad y otro 48 % tiene previsto implementarla en el plazo de un año.
- **La falta de conocimientos en materia de ciberseguridad repercute directamente en la protección.** Más de una cuarta parte (27 %) de los directores de TI aseguraron que su capacidad para encontrar y retener a profesionales de seguridad TI cualificados es el principal reto a su capacidad de prestar seguridad TI, mientras que el 54 % afirmó que es un desafío importante.

Las empresas están cambiando la forma en que ofrecen seguridad

- **La subcontratación de la seguridad TI está aumentando rápidamente.** Actualmente, el 65 % subcontrata algunas o todas sus tareas de seguridad TI. Para el 2022, está previsto que aumente al 72 %. El porcentaje de empresas que utilizan exclusivamente personal interno bajará del 34 % al 26 %.
- **Mejorar la eficiencia operativa es una prioridad fundamental.** Cuatro de cada diez (39 %) encuestados afirmaron que mejorar la eficiencia operativa y la escalabilidad es una de sus mayores prioridades para el equipo de TI este año.

Las víctimas del ransomware muestran actitudes y comportamientos diferentes a los de aquellos que nunca se han visto afectados

- **Las víctimas del ransomware están más expuestas a la infección de terceros.** El 29 % de las empresas afectadas por el ransomware en el último año permiten que cinco o más proveedores se conecten directamente a su red, en comparación con solo el 13 % de las que no se vieron afectadas por el ransomware.
- **El ransomware daña la confianza profesional.** Los directores de TI cuyas empresas se vieron afectadas por el ransomware son casi tres veces más propensos a pensar que están "considerablemente por detrás" de las ciberamenazas que aquellos que no sufrieron ataques (17 % frente a un 6 %).
- **Sufrir un ataque acelera la implementación de la búsqueda de amenazas realizada por humanos.** El 43 % de las víctimas del ransomware tienen previsto implementar la búsqueda de amenazas realizada por humanos en seis meses, frente al 33 % de los que no sufrieron un ataque.
- **Las víctimas han aprendido la importancia de contar con profesionales de seguridad cualificados.** Más de un tercio (35 %) de las víctimas del ransomware afirmaron que contratar y retener a profesionales de seguridad TI cualificados es su principal reto en materia de ciberseguridad, frente a solo el 19 % que no se había visto afectado.

Los equipos de TI están mostrando progresos en muchas batallas

Empecemos con las buenas noticias: los equipos de TI se las arreglan para mantenerse al día con muchos aspectos de la ciberseguridad. Consiguen mantener muchas bolas en el aire y, de este modo, protegen a sus empresas contra innumerables amenazas.

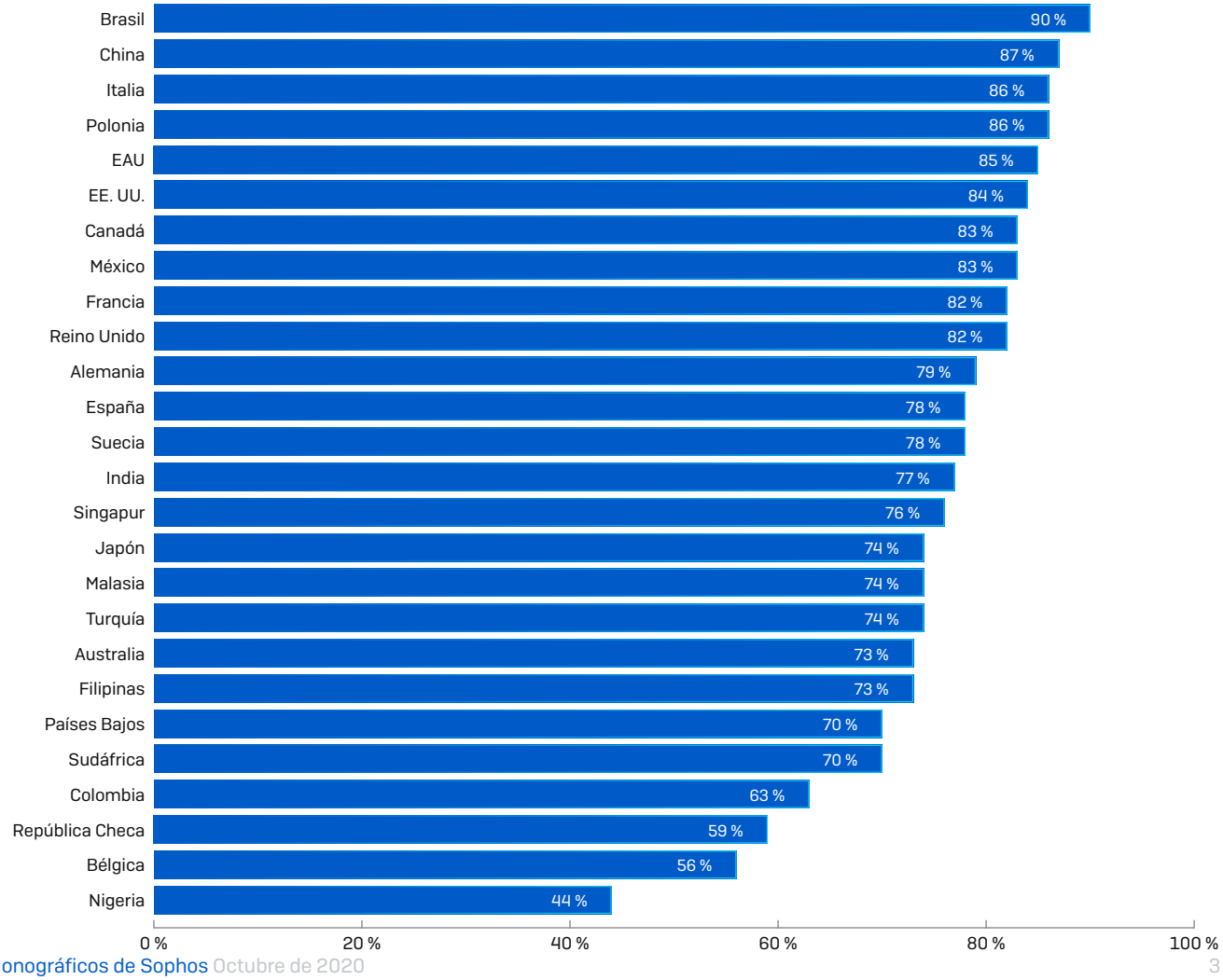
Los equipos de TI están al día con los parches de seguridad

"Aplique los parches con prontitud y frecuencia" es un mantra habitual de los expertos en seguridad y es una máxima que los equipos de TI se han tomado muy en serio. Los encuestados son conscientes de la necesidad de aplicar los parches rápidamente: muchos de ellos lo hacen a las 24 horas de su publicación, y las tres cuartas partes lo hacen en el plazo de una semana. Los parches de los servidores y recursos abiertos a Internet se aplican más rápidamente, y el 39 % de los encuestados los aplica en un plazo de 24 horas.

	APLICAN PARCHES EN 24 HORAS	APLICAN PARCHES EN UNA SEMANA	APLICAN PARCHES EN UN MES
Dispositivos de escritorio	36 %	41 %	14 %
Servidores	39 %	38 %	14 %
Aplicaciones	36 %	40 %	15 %
Recursos abiertos a Internet	39 %	38 %	14 %

Sin embargo, el 22 % admite que tarda más de una semana en aplicar los parches en dispositivos de escritorio, siendo los encuestados de Nigeria, Bélgica y la República Checa los que más tardan.

Porcentaje de encuestados que aplican parches a los ordenadores de sobremesa en el plazo de una semana desde su publicación

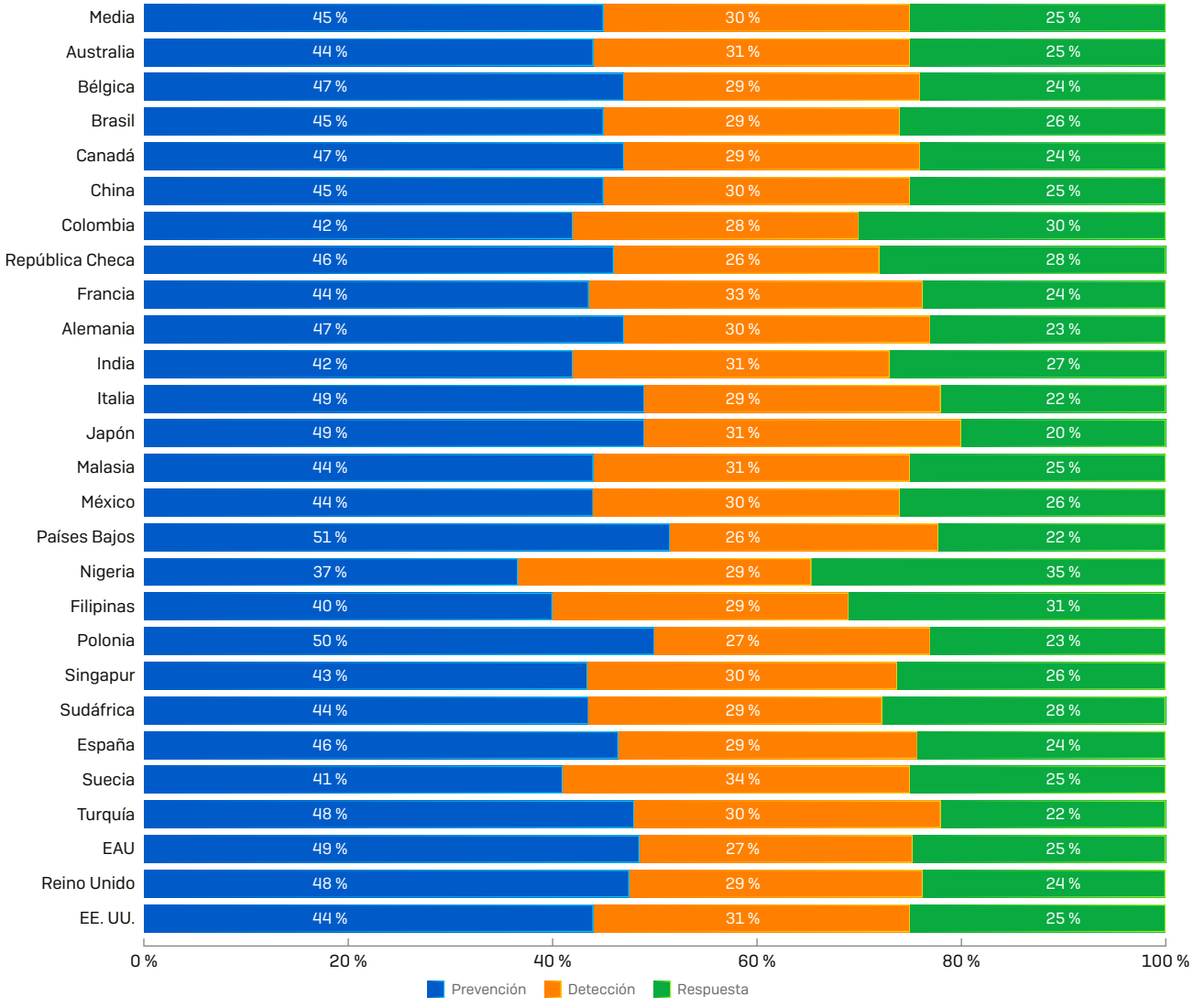


La prevención tiene prioridad

De media, los equipos de TI dedican casi la mitad de su tiempo (45 %) a la prevención, el 30 % a la detección y el 25 % restante a la respuesta. Los datos revelaron algunas variaciones según la región: de los países encuestados, los equipos de TI de los Países Bajos son los que más tiempo dedican a la prevención (51 %); los equipos de TI suecos son los que más tiempo dedican a la detección (34 %); y las empresas nigerianas son las que más tiempo dedican a la respuesta (35 %).

Si bien el equilibrio entre la prevención y la detección es un enfoque sensato a la ciberseguridad, el hecho de dedicar un tiempo considerable a la respuesta suele sugerir que no se detienen los incidentes. Los índices de respuesta altos indican que una empresa experimenta un elevado número de incidentes, que los incidentes solo se detectan en una fase muy tardía, o ambas cosas.

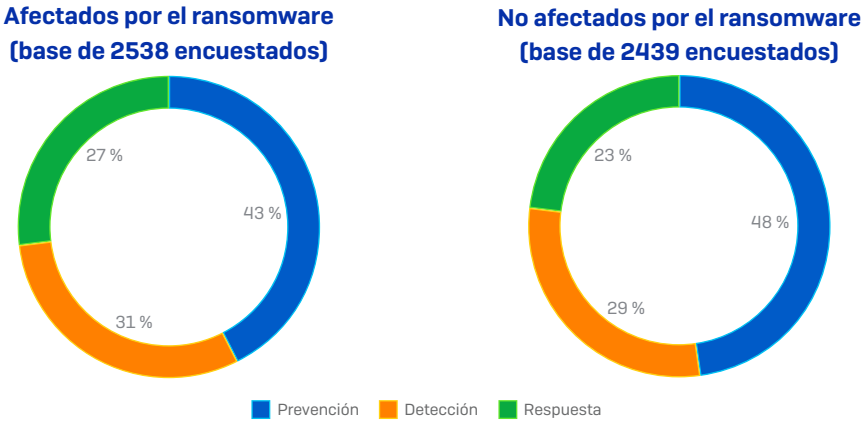
División del tiempo entre la prevención, la detección y la respuesta



Por motivos de redondeo, en algunos casos los totales no suman el 100 %.

Las víctimas del ransomware dedican menos tiempo a la prevención y más tiempo a la respuesta

El 51 % de los encuestados admitió que su empresa había sufrido un ataque de ransomware durante los doce meses anteriores. Las empresas que fueron víctimas del ransomware se centran más en la detección y la respuesta que las que no se vieron afectadas. Por el contrario, las empresas que no sufrieron ningún ataque de ransomware dedican más tiempo a la prevención que las que sí lo sufrieron.



Puede que este creciente enfoque preventivo haya ayudado a las empresas que no se vieron afectadas a prevenir los ataques: una defensa sólida siempre comienza con la mejor protección. Al mismo tiempo, es posible que las víctimas del ransomware estén más alerta ante la naturaleza compleja y de varias fases de los ataques avanzados, por lo que dedican más recursos a detectar y responder a los indicios de que un ataque es inminente.

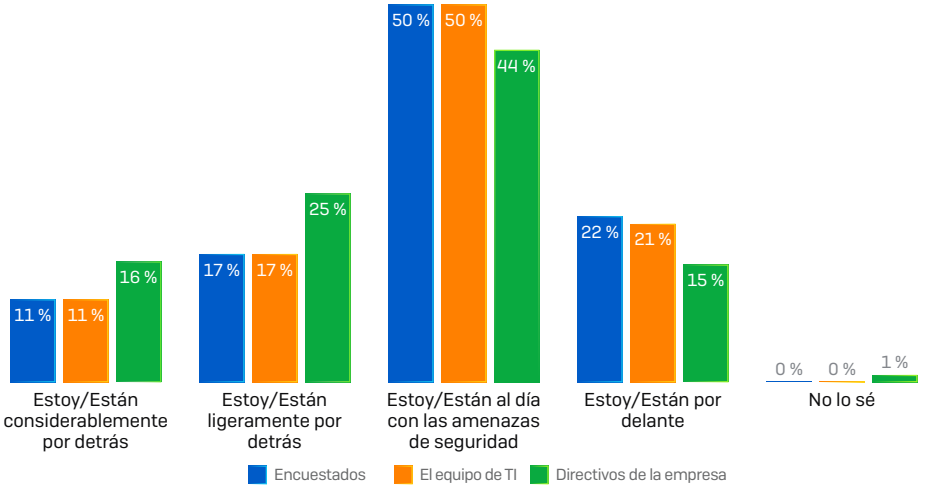
Para obtener más información sobre cómo identificar que los atacantes de ransomware le tienen en el punto de mira, lea el artículo de SophosLabs Cinco indicios de que está a punto de ser atacado.

Los directores de TI están al día con la ciberseguridad

A pesar de la naturaleza rápidamente cambiante de las amenazas de ciberseguridad, los profesionales de TI creen que están logrando mantenerse al día con las ciberamenazas. La mayoría de los directores de TI opina que tanto ellos (72 %) como sus equipos (72 %) están al día con las ciberamenazas o por delante de ellas. Del 28 % de los responsables de TI que creen que van a la zaga, el 17 % opina que está solo ligeramente detrás de las ciberamenazas, mientras que solo el 11 % piensa que está considerablemente por detrás.

Estas cifras ocultan notables variaciones en función de la región: los encuestados de Polonia, México y Turquía son los que más probabilidades tenían de decir que iban por delante de las ciberamenazas (39 %, 34 % y 31 % respectivamente), mientras que los encuestados de Nigeria (60 %), Suecia (57 %) y Alemania (49 %) son los que más probabilidades tenían de afirmar que iban a la zaga. Cabe señalar que estos datos responden a las percepciones de los encuestados (y, por lo tanto, es probable que influyan factores culturales) y no son una medida real del grado de actualización de las personas.

Opinión de los encuestados sobre el grado de actualización de las personas de su empresa con respecto a las amenazas de ciberseguridad



Mientras que los directores de TI, por lo general, están seguros de que ellos y su equipo están al día, el 41 % creen que sus directivos van a la zaga (el 25 % creen que están ligeramente detrás y el 16 % considerablemente por detrás). En muchos sentidos esta diferencia es comprensible: los directivos empresariales raramente se especializan en ciberseguridad. Sin embargo, pone de relieve el reto al que se enfrentan los equipos de TI para lograr que la dirección comprenda los riesgos que supone la ciberseguridad y las solicitudes de inversión asociadas.

Los ataques de ransomware dañan la confianza de los profesionales de TI

Si examinamos los datos con más detenimiento, vemos que los ataques de ransomware infligen un daño considerable a la confianza de los directores de TI y sus equipos, más allá de las repercusiones para el negocio.

Casi el triple de los directores de TI cuyas empresas se vieron afectadas por el ransomware el año pasado creen que están "considerablemente por detrás" de las ciberamenazas, en comparación con los directores de TI cuyas empresas no sufrieron ningún ataque (17 % frente a un 6 %). Este menor grado de confianza se plasma en la percepción que el director de TI tiene tanto del equipo de TI como de los directivos de la empresa, como se ilustra en la siguiente tabla.

	ESTÁ CONSIDERABLEMENTE POR DETRÁS DE LAS AMENAZAS (%)	ESTÁ AL DÍA CON LAS CIBERAMENAZAS (%)
Directores de TI (encuestados)		
Afectados por el ransomware	17 %	43 %
No afectados por el ransomware	6 %	57 %
Equipos de TI (percepción del encuestado)		
Afectados por el ransomware	15 %	43 %
No afectados por el ransomware	6 %	58 %
Directivos de la empresa (percepción del encuestado)		
Afectados por el ransomware	20 %	39 %
No afectados por el ransomware	11 %	49 %

Una vez más, es importante recordar que estas respuestas son la percepción del encuestado y no una medida del grado de actualización real. Es posible que el hecho de haber sido víctima de un ataque de ransomware sirva para enfrentarse a la realidad y, como resultado de sus experiencias, las víctimas del ransomware comprendan mejor la situación.

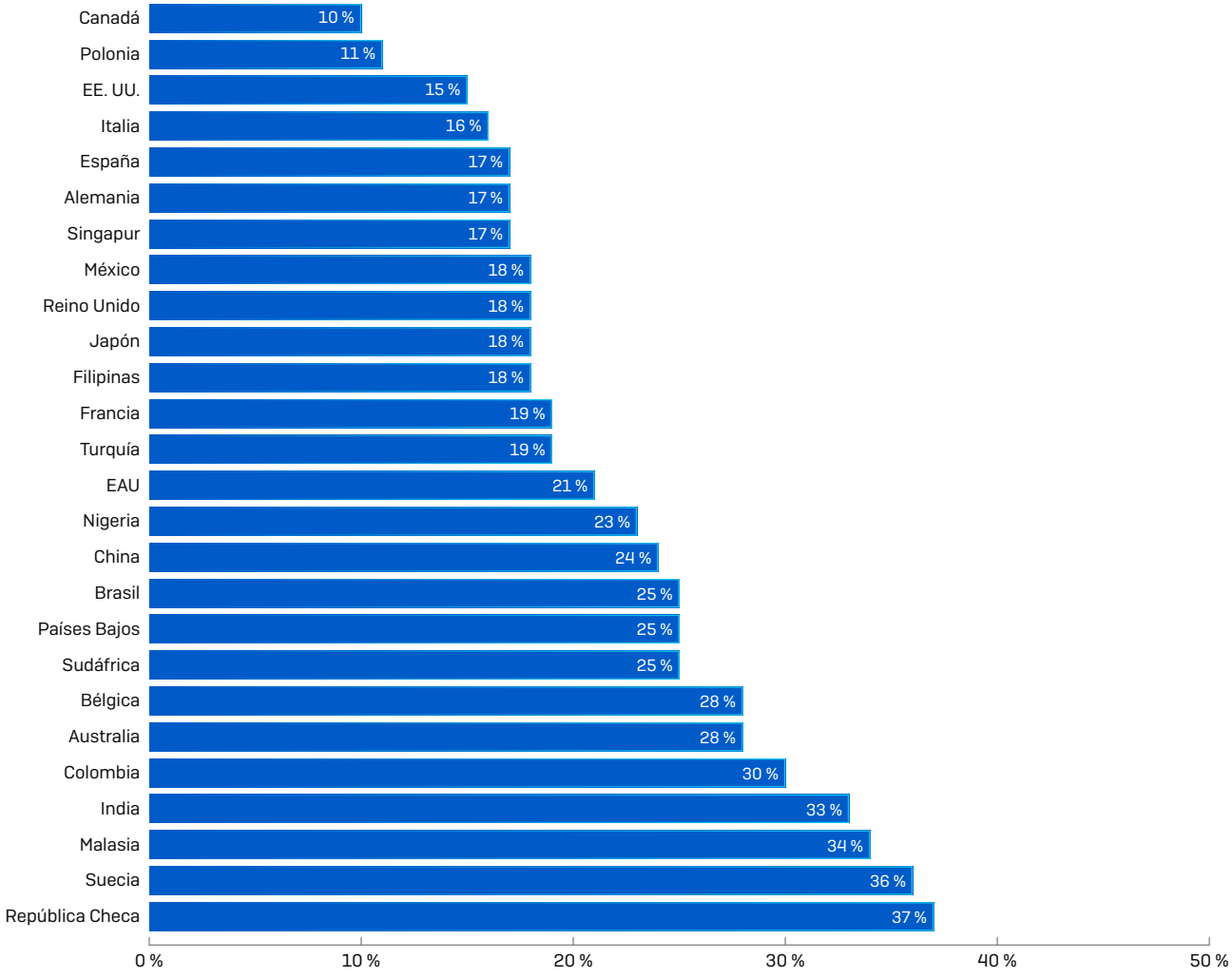
La mejora de la ciberseguridad precisa de personas, que escasean

Aunque los equipos de TI están ganando muchas batallas, la guerra está lejos de ganarse. A pesar de los esfuerzos de los responsables de TI y sus equipos, las ciberamenazas siguen siendo un desafío constante, hasta el punto de que poco más de la mitad de los encuestados (51 %) dijo que minimizar el riesgo de un ciberataque es un punto de atención prioritaria para los próximos 12 meses. Las razones de esto saltan a la vista cuando analizamos la amplia gama de retos de seguridad que encaran los equipos de TI.

Los equipos de TI se enfrentan a un constante aluvión de ciberataques, con amenazas procedentes de múltiples direcciones y con objetivos diversos. Como ya se ha mencionado, el 51 % de los encuestados sufrió un ataque de ransomware en el último año y los delincuentes lograron cifrar los datos en el 73 % de estos ataques*. La seguridad en la nube también es un reto, ya que el 70 % de las empresas que alojan datos o cargas de trabajo en la nube pública han experimentado algún incidente de seguridad en el último año**.

Otro reto que se presenta a los equipos de TI es el de proteger las posibles conexiones directas a su red por parte de empresas de terceros, como servicios de contabilidad o proveedores de TI. De media, los encuestados afirman que tienen tres proveedores que se conectan a sus sistemas. Sin embargo, uno de cada cinco encuestados (21 %), porcentaje que se eleva a un tercio (o más) en la República Checa, la India, Malasia y Suecia, permite que cinco o más proveedores se conecten. En cambio, en Canadá y Polonia solo uno de cada diez encuestados afirmó que tenía cinco o más proveedores con acceso remoto.

Porcentaje de empresas con cinco o más proveedores que pueden conectarse directamente a la red



Permitir que proveedores externos se conecten a la red entraña intrínsecamente riesgos de seguridad, así como ventajas comerciales. Cuantos más proveedores puedan conectarse, mayor será el reto y la carga de trabajo para los equipos de TI.

Las víctimas del ransomware están más expuestas a la infección de terceros

De las empresas afectadas por el ransomware en el último año, el 29 % permite que cinco o más proveedores se conecten directamente a su red, en comparación con el 13 % de las que no se vieron afectadas por el ransomware. El 9 % de las víctimas señalaron a los proveedores externos como método de entrada, por lo que claramente se trata de un vector de ataque importante.

Si bien hay muchos motivos comerciales de peso para permitir que las empresas externas se conecten a su red, lo que está claro es que proteger su cadena de suministro debe ser una prioridad fundamental para todos los que adopten este enfoque. Una ciberseguridad sólida debe ser un criterio esencial para cualquiera que quiera conectarse a su red.

La búsqueda de amenazas realizada por humanos es una necesidad urgente

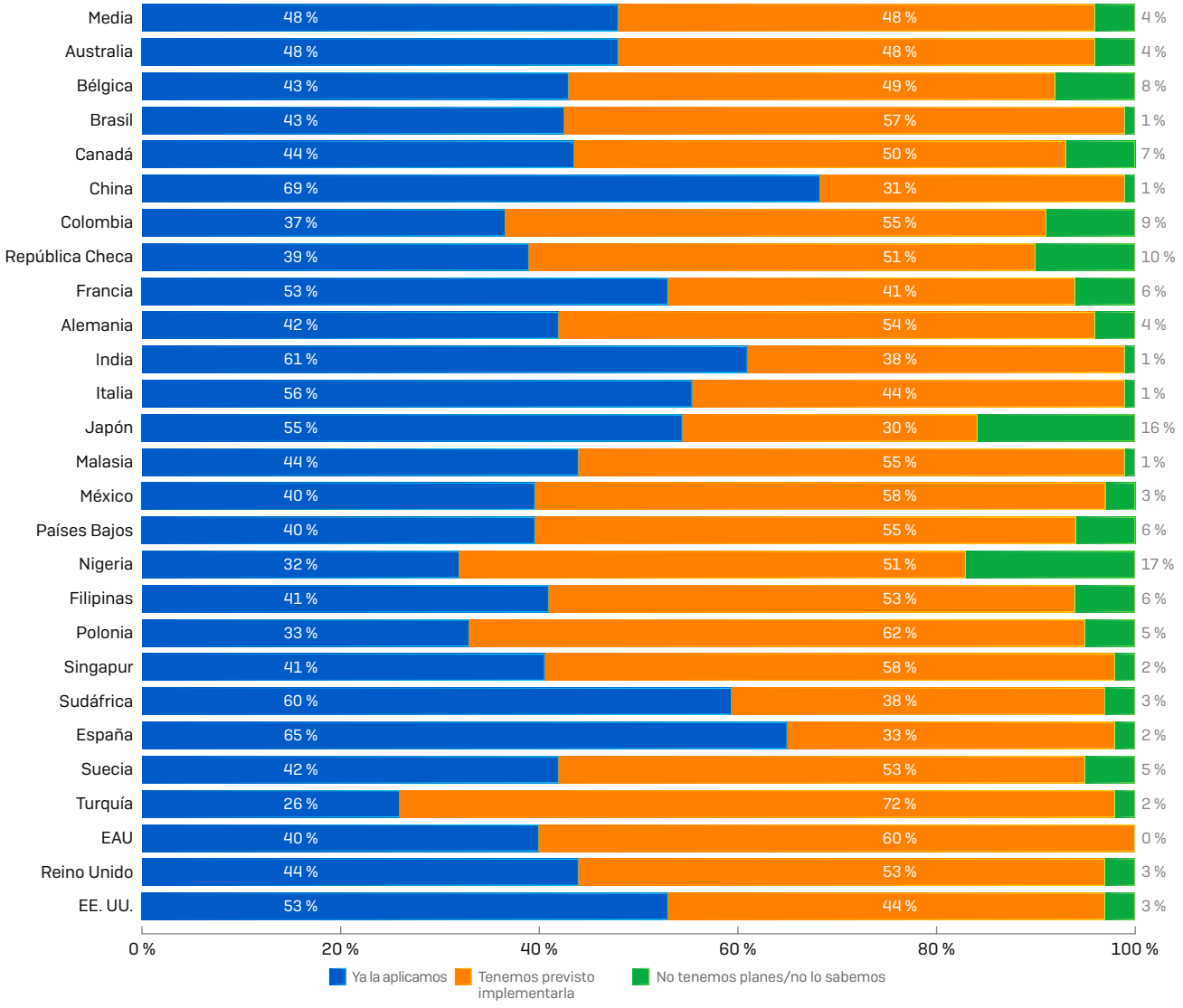
Las ciberamenazas más devastadoras suelen implicar ataques llevados a cabo por humanos, a menudo explotando herramientas y procesos legítimos como PowerShell. El hacking manual en vivo permite a los atacantes modificar sus tácticas, técnicas y procedimientos (TTP) sobre la marcha para eludir los productos y protocolos de seguridad. Una vez dentro de la red de la víctima, los atacantes pueden propagarse lateralmente, exfiltrar datos, instalar malware y puertas traseras para futuros ataques, y desplegar ransomware.

Si bien la tecnología, en particular la tecnología automatizada e inteligente, desempeña un papel importante, sigue siendo necesario contar con operadores expertos. Detener los ataques llevados a cabo por humanos requiere una búsqueda de amenazas realizada por humanos.

Prácticamente todos los encuestados reconocen la necesidad de este enfoque: el 48 % ya incorpora en sus procedimientos de seguridad la búsqueda de amenazas realizada por humanos para identificar la actividad maliciosa que puede pasar inadvertida a las herramientas de seguridad (como SIEM, protección de endpoints, firewall, etc.). Otro 48 % planea implementarla. Los encuestados también son conscientes de la urgencia de desplegar la búsqueda realizada por humanos, ya que prácticamente todos los encuestados (99,6 %) que quieren implementarla esperan hacerlo en el plazo de un año.

La situación de la búsqueda de amenazas realizada por humanos varía significativamente según la geografía. El 69 % de los encuestados de China ya han aplicado este enfoque, seguidos de cerca por España (65 %), la India (61 %) y Sudáfrica (60 %). Por el contrario, Turquía ha sido el país que más ha tardado en adoptar la búsqueda realizada por humanos, ya que solo el 26 % de los encuestados la aplica, mientras que Nigeria (32 %) y Polonia (33 %) van algo más adelantados.

Tiene previsto incorporar la búsqueda de amenazas realizada por humanos

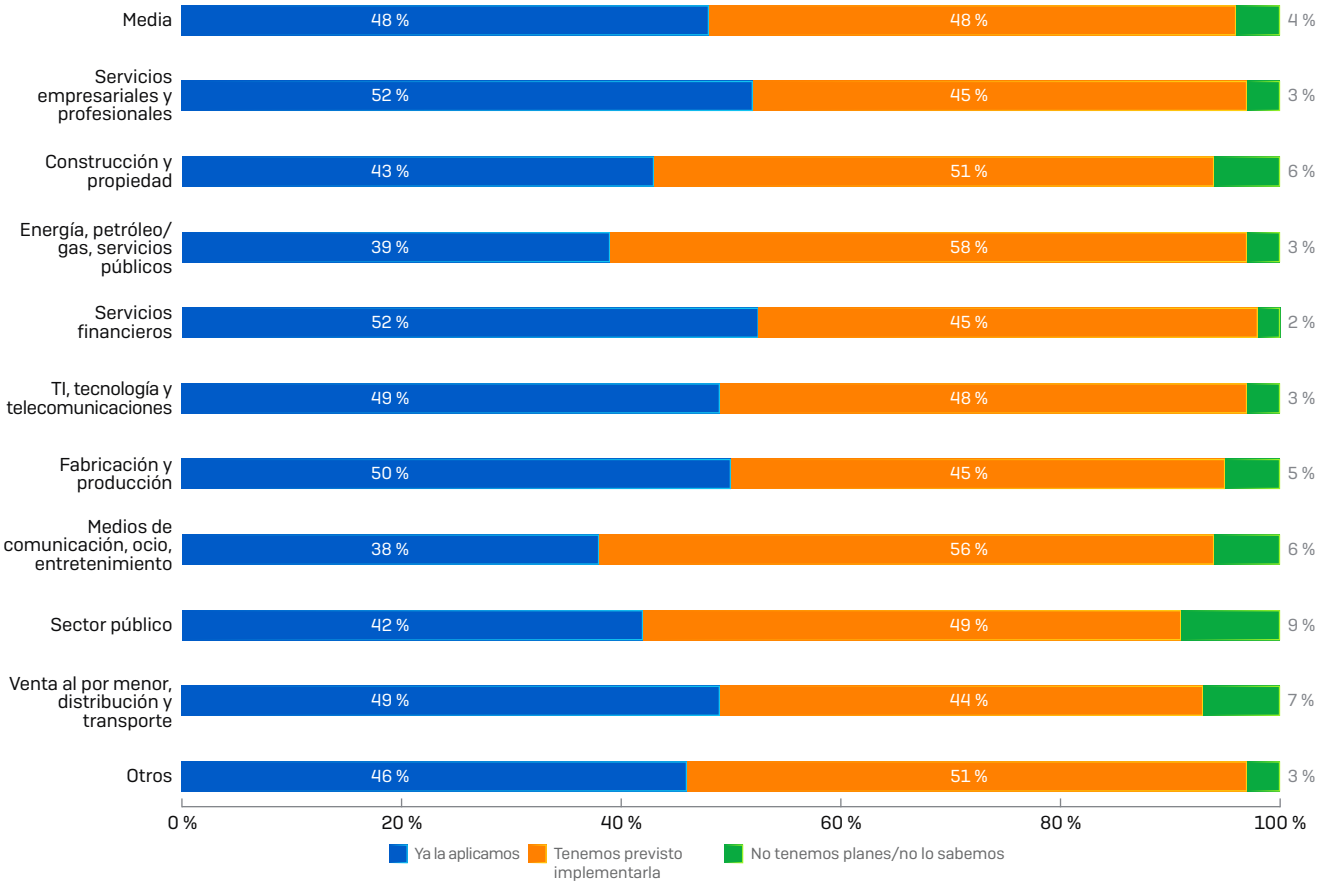


Por motivos de redondeo, en algunos casos los totales no suman el 100 %.

La encuesta también reveló diferentes niveles de preparación según el sector. Los servicios comerciales y profesionales y los servicios financieros lideran la implementación de la búsqueda realizada por humanos: el 52 % de los encuestados de ambos sectores afirma que su empresa ya aplica este enfoque.

Por el contrario, es menos probable que los encuestados de los sectores de medios de comunicación, ocio y entretenimiento (38 %) y los sectores de la energía, el petróleo/gas y los servicios públicos (39 %) afirmen que ya aplican la búsqueda de amenazas realizada por humanos. Dado que el sector energético es un posible objetivo de los ataques a estados nacionales, su vulnerabilidad frente a las amenazas llevadas a cabo por humanos es preocupante.

Tiene previsto incorporar la búsqueda de amenazas realizada por humanos, por sector

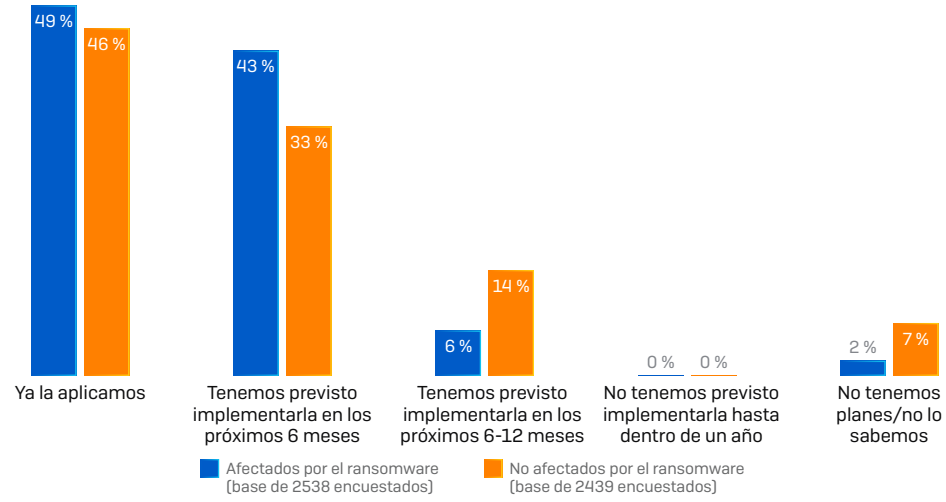


Por motivos de redondeo, en algunos casos los totales no suman el 100 %.

Sufrir un ataque de ransomware acelera la implementación de la búsqueda de amenazas realizada por humanos

Por lo general, el hecho de sufrir un ataque de ransomware influye poco en el deseo de una empresa de incorporar la búsqueda de amenazas realizada por humanos, aunque sí impulsa la urgencia en la aplicación. El 43 % de las víctimas del ransomware tienen previsto implementar la búsqueda de amenazas realizada por humanos en seis meses, frente al 33 % de los que no sufrieron un ataque. Estos datos sugieren que las víctimas del ransomware están muy motivadas para evitar que se repita el incidente.

Impacto de una experiencia reciente con el ransomware en la implementación de la búsqueda de amenazas realizada por humanos



La falta de conocimientos en materia de ciberseguridad repercute directamente en la protección

El 81 % de los encuestados afirmó que su capacidad para encontrar y retener a profesionales de seguridad TI cualificados es un gran reto a la capacidad de su empresa de ofrecer seguridad TI: el 54 % dijo que es un desafío importante, mientras que más de un cuarto (27 %) aseguró que es su mayor reto.

Todos los países mencionaron dificultades a la hora de contratar personal de TI cualificado. En Italia (94 %), la India (93 %) y Brasil y Colombia (ambos 92 %), más de nueve de cada diez encuestados afirmaron que su capacidad para encontrar y retener personal cualificado era un obstáculo importante para proteger a la empresa de las ciberamenazas.

Incluso en Sudáfrica, el país donde es menos probable que se vea la contratación de personal de ciberseguridad como un reto, más de seis de cada diez encuestados (62 %) dicen que les crea problemas importantes.

¿Hasta qué punto son la contratación y la retención de profesionales de seguridad TI cualificados un reto a la capacidad de su empresa de ofrecer seguridad TI?

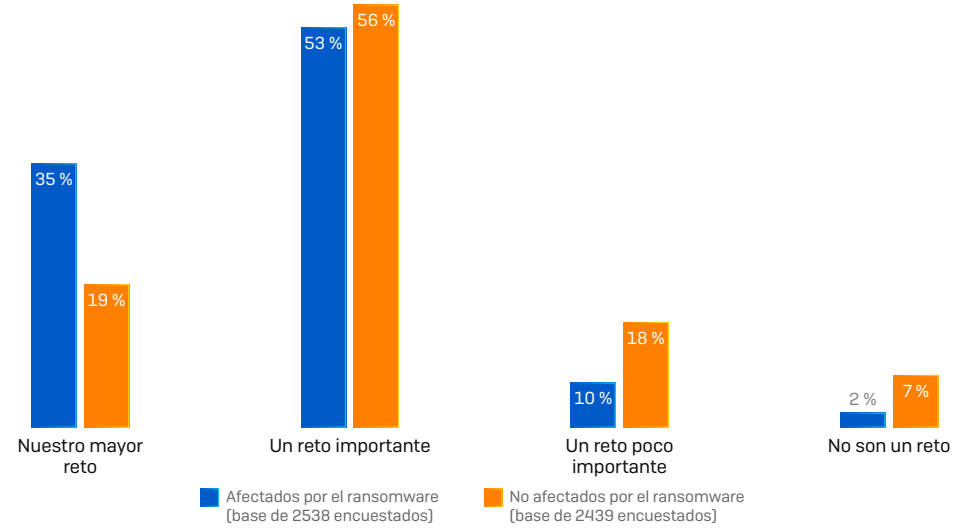
PAÍS	SON NUESTRO MAYOR RETO	SON UN RETO IMPORTANTE, PERO NO EL MAYOR	SON UN RETO POCO IMPORTANTE	NO SON UN RETO	NO LO SABEN
Media	27 %	54 %	14 %	4 %	0 %
Australia	17 %	57 %	22 %	5 %	0 %
Bélgica	24 %	52 %	24 %	0 %	0 %
Brasil	45 %	47 %	6 %	3 %	1 %
Canadá	19 %	55 %	18 %	7 %	2 %
China	24 %	54 %	18 %	4 %	0 %
Colombia	29 %	63 %	8 %	1 %	0 %
República Checa	33 %	47 %	18 %	1 %	1 %
Francia	23 %	62 %	11 %	4 %	0 %
Alemania	19 %	63 %	14 %	5 %	0 %
India	58 %	35 %	6 %	1 %	0 %
Italia	28 %	67 %	5 %	2 %	0 %
Japón	35 %	44 %	17 %	4 %	1 %
Malasia	26 %	54 %	16 %	4 %	0 %
México	27 %	62 %	6 %	6 %	0 %
Países Bajos	26 %	49 %	25 %	0 %	1 %
Nigeria	32 %	51 %	16 %	1 %	0 %
Filipinas	40 %	49 %	8 %	2 %	1 %
Polonia	9 %	59 %	20 %	12 %	0 %
Singapur	17 %	72 %	10 %	2 %	0 %
Sudáfrica	22 %	40 %	19 %	19 %	0 %
España	17 %	58 %	17 %	8 %	1 %
Suecia	44 %	41 %	13 %	1 %	1 %
Turquía	30 %	52 %	9 %	8 %	1 %
EAU	22 %	62 %	15 %	1 %	0 %
Reino Unido	14 %	64 %	20 %	2 %	0 %
EE. UU.	26 %	49 %	17 %	8 %	0 %

Las víctimas del ransomware han aprendido por las malas la importancia de contar con profesionales de seguridad cualificados

Sufrir un ciberataque tiene importantes repercusiones en las opiniones sobre el personal de ciberseguridad. Más de un tercio (35 %) de los encuestados que habían sido víctimas del ransomware durante el último año afirmaron que la contratación y la retención de profesionales de seguridad TI cualificados son su mayor reto en materia de ciberseguridad, y otro 53 % dijo que son un reto importante.

Por el contrario, entre las empresas que no se habían visto afectadas por el ransomware en el último año, solo el 19 % dijo que contratar y retener personal cualificado era su mayor reto, una diferencia de 16 puntos.

Medida en que la contratación y la retención de profesionales de seguridad TI cualificados son un reto a la capacidad de la empresa de ofrecer seguridad TI



Es probable que haya varios factores detrás de estas diferentes opiniones. En primer lugar, las consecuencias de contar con conocimientos de seguridad limitados están todavía muy presentes en la memoria de aquellos que se han visto afectados recientemente por los costes económicos, operacionales y de reputación de sufrir un ataque de ransomware.

Además, las víctimas del ransomware invariablemente habrán investigado el origen del ataque. Al hacerlo, habrán identificado las brechas en sus defensas que permitieron a los atacantes infiltrarse en su empresa y acceder a sus datos. Es probable que muchos hayan identificado la falta de personal con experiencia como un factor que contribuye a sufrir un ataque.

La contratación es la primera prioridad para los directores de TI

Una consecuencia de esta falta de conocimientos es que la contratación y la retención de personal ocuparon el primer puesto en la lista de prioridades de los directores de TI. El 55 % de los encuestados afirmaron que es una de sus prioridades para los próximos 12 meses, relegando la minimización del riesgo de un ciberataque al segundo puesto (cabe destacar que los encuestados podían seleccionar múltiples respuestas a esta pregunta).

Las empresas están cambiando la forma en que ofrecen seguridad

Es poco probable que los profesionales de TI se sorprendan por el reto que supone la dotación de recursos. La contratación en materia de ciberseguridad es una asignatura pendiente desde hace muchos años y, si bien resulta alentador que los responsables den prioridad a la asignación de recursos, la magnitud del reto sugiere que no habrá una solución rápida.

Vistos desde esta óptica, los cambios que los directores de TI están haciendo en la forma en que se ofrece ciberseguridad y su enfoque en la mejora de la eficiencia y la escalabilidad pueden considerarse una respuesta directa al reto planteado por la dotación de recursos.

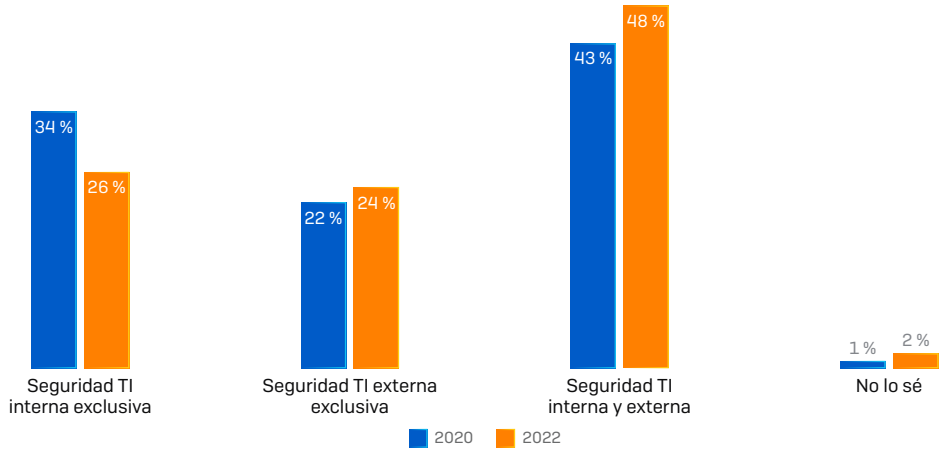
La subcontratación está creciendo rápidamente

La subcontratación de la ciberseguridad permite a las empresas beneficiarse de la experiencia de los profesionales de seguridad sin tener que contratarlos directamente. También suele darles acceso a niveles más altos de competencia en materia de seguridad que de otro modo no tendrían, gracias a la capacidad de los proveedores de servicios de seguridad de cultivar y desarrollar conocimientos especializados.

La subcontratación de la seguridad TI es la norma, y el 65 % ya la aplica de una forma u otra: el 43 % utiliza una combinación de seguridad interna y externa, mientras que el 22 % subcontrata la totalidad de su seguridad TI. El estudio reveló variaciones según la región. A la cabeza de la lista de externalización se encuentran China (76 %), los Emiratos Árabes Unidos (74 %) y Malasia y Singapur (ambos 73 %), donde alrededor de tres cuartas partes de los encuestados ya incluyen la subcontratación en la prestación de seguridad TI. En el otro extremo, en Bélgica (52 %), Francia (54 %) y Nigeria (54 %), poco más de la mitad de los encuestados utilizan actualmente proveedores de seguridad externos.

La tendencia mundial es que la externalización aumente en los próximos dos años, pasando del 65 % actual a casi tres cuartas partes (72 %) en 2022. El mayor cambio se producirá en el porcentaje de empresas que utilizan exclusivamente personal interno: se prevé que este baje del 34 % al 26 %. Se producirán aumentos tanto en el porcentaje de los que subcontratan la totalidad de su seguridad TI como de los que utilizan una combinación de conocimientos técnicos internos y externos.

Cómo las empresas ofrecen seguridad TI



Estos números globales ocultan algunas variaciones regionales interesantes:

- Los encuestados de España y la India tienen previsto incrementar la gestión de la seguridad TI únicamente a nivel interno. Aunque las cifras son relativamente bajas (del 34 % al 37 % en España, y del 33 % al 34 % en la India), resulta curioso que planeen apartarse de la tendencia mundial.
- En Filipinas, casi la mitad de los encuestados (48 %) tiene previsto externalizar la totalidad de la seguridad TI en 2022, lo que supone un aumento enorme con respecto al 30 % actual. Otros países que prevén una adopción superior a la media del enfoque de contratación externa exclusiva son la República Checa, Nigeria y Suecia (los tres con un 35 %) y Australia (34 %).
- Más de seis de cada diez encuestados tienen previsto aplicar un enfoque combinado de contratación interna y externa en China (67 %) y México (62 %).

Los directores de TI se centran en mejorar la eficiencia y la escalabilidad

Otra respuesta a la falta de conocimientos de seguridad TI es encontrar formas de sacar más partido de las habilidades que sí se tienen. Cuatro de cada diez (39 %) encuestados afirmaron que mejorar la eficiencia operativa y la escalabilidad es una de sus mayores prioridades para el equipo de TI este año. Los encuestados europeos y japoneses han hecho descender esta media, mientras que en China, Malasia y Sudáfrica más de la mitad de los encuestados la tienen en su lista de prioridades.

Conclusión

Las respuestas de 5000 directores de TI de 26 países han arrojado luz sobre los retos a los que se enfrentan los equipos de TI a la hora de gestionar y ofrecer seguridad TI. Si bien los equipos de TI están ganando muchas batallas –especialmente con la aplicación de parches y mantenerse al día con las amenazas de ciberseguridad–, la guerra está lejos de ganarse. Los profesionales de TI afrontan retos en múltiples frentes: desde el ransomware y la seguridad en la nube hasta la gestión de proveedores externos que pueden conectarse a la red.

Ante el aumento de los ataques llevados a cabo por humanos, la mayoría de las empresas están recurriendo a la búsqueda de amenazas realizada por humanos: antes de finales de 2020, el 95 % de los encuestados espera estar aplicándola de alguna manera. Al mismo tiempo, las dificultades para contratar y retener a profesionales de la ciberseguridad son un factor limitativo para la gran mayoría de las empresas. Las empresas que se han visto afectadas por el ransomware en el pasado reciente son particularmente conscientes de los efectos de esta falta de conocimientos en su capacidad de ofrecer una ciberseguridad eficaz.

Hay una clara correlación entre haber sufrido un ataque de ransomware y la actitud del equipo de TI. Las víctimas del ransomware están más expuestas a la infección de terceros que otras empresas, y también dedican más tiempo a la respuesta, lo que indica que tienen más incidentes de los que ocuparse. Al mismo tiempo, sus experiencias les han hecho más conscientes de la importancia de disponer de profesionales de ciberseguridad cualificados y de la urgencia de aplicar la búsqueda de amenazas realizada por humanos.

En vista de estos desafíos, resulta alentador ver cómo los equipos de TI desarrollan sus enfoques. El uso de expertos subcontratados parece que va a seguir aumentando en los próximos dos años; para el 2022, casi las tres cuartas partes de las empresas externalizarán la seguridad TI de una forma u otra. También se hace especial hincapié en incrementar la eficiencia operativa y la escalabilidad en muchas partes del mundo, de modo que los equipos de TI puedan hacer más con los profesionales cualificados de que disponen.

La ciberseguridad nunca se detiene. Los equipos de TI merecen un gran reconocimiento por lograr mantenerse al día con muchos aspectos de la seguridad. Dada la continua escasez de conocimientos en materia de ciberseguridad, los equipos de TI tendrán que encontrar diferentes formas de ampliar y mejorar sus defensas ante la evolución de las amenazas y, en particular, el aumento de los ataques llevados a cabo por humanos.

Cómo puede ayudar Sophos

Sea cual sea la forma en que quiera gestionar su seguridad TI, podemos ayudarle.

Servicio de búsqueda de amenazas realizada por humanos 24/7

Con Sophos Managed Threat Response (MTR), su empresa disfruta de la protección 24/7 de un equipo de élite de cazadores de amenazas y expertos en respuesta que detectan y neutralizan de forma proactiva las amenazas en su nombre. Estos profesionales de seguridad altamente cualificados son capaces de detectar y detener ataques avanzados llevados a cabo por humanos antes de que puedan afectar a su empresa.

Obtenga más información y consulte la Guía para la adquisición de servicios MDR.

Servicio de respuesta a incidentes en tiempo real

Cualquier empresa que esté sufriendo un incidente activo puede desplegar nuestro servicio **Rapid Response**. Nuestro equipo experto de gestores de respuesta a incidentes identificará y neutralizará la amenaza activa rápidamente. Ya sea una infección, un ataque o un acceso no autorizado que intenta burlar sus controles de seguridad, lo hemos visto y detenido todo.

Más información

Herramientas avanzadas de higiene de TI y de búsqueda de amenazas

Si prefiere realizar sus propias búsquedas de amenazas, la detección y respuesta para endpoints (EDR) de Sophos le ofrece las herramientas avanzadas necesarias para la búsqueda de amenazas y la higiene de las operaciones de seguridad TI. Las potentes funciones de búsqueda permiten a su equipo identificar y gestionar de forma proactiva los problemas de seguridad e higiene de TI, ampliando así su protección.

Obtenga más información y pruébelo gratis.

Sistema de ciberseguridad next-gen

Las empresas que despliegan un sistema de ciberseguridad next-gen de Sophos observan sistemáticamente una reducción del 50 % en la carga administrativa de TI. Al desplegar nuestras soluciones de endpoints y de firewall líderes en el mercado y administrarlo todo a través de la plataforma Sophos Central, los equipos de TI reducen a la mitad el tiempo dedicado a la gestión de la ciberseguridad, a la vez que mejoran su eficacia en materia de seguridad.

Obtenga más información y lea algunas historias de clientes.

Estudios detallados sobre el ransomware

SophosLabs y el equipo de Sophos MTR publican regularmente trabajos de investigación sobre las últimas técnicas de ransomware en el blog de Sophos.

* El estado del ransomware 2020. Encuesta global a 5000 directores de TI encargada por Sophos y realizada por Vanson Bourne.

** El estado de la seguridad en la nube 2020. Encuesta global a 3521 directores de TI encargada por Sophos y realizada por Vanson Bourne.

Acerca de Vanson Bourne

Vanson Bourne es una consultora independiente especializada en estudios de mercado para el sector tecnológico. Su reputación de análisis sólidos y creíbles basados en la investigación se asienta en rigurosos principios de investigación y en su capacidad para recabar las opiniones de los principales responsables de la toma de decisiones en todas las funciones técnicas y empresariales, en todos los sectores empresariales y en todos los principales mercados. Visítelos en www.vansonbourne.com

Ventas en España
Teléfono: (+34) 913 756 756
Correo electrónico: comercialES@sophos.com

Ventas en América Latina
Correo electrónico: Latamsales@sophos.com

05-10-20 WPES (DD)

SOPHOS