SOPHOS
Cybersecurity evolved.

El equipo de seguridad TI: 2021 y más allá

Resultados de una encuesta a 5400 directores de TI de 30 países

Monográficos de Sophos. Junio de 2021

Los equipos de TI han estado al frente de la respuesta a la pandemia en casi todas las organizaciones. TI ha desempeñado un papel directo y decisivo a la hora de permitir que las organizaciones siguieran trabajando a pesar de las restricciones y limitaciones impuestas por la COVID-19. Es en gran parte gracias a los comprometidos y dedicados equipos de TI de todo el mundo que tantas organizaciones han podido seguir funcionando durante la pandemia. Ayudaron a los centros educativos a impartir clases online, permitieron a las tiendas pasarse al comercio online y garantizaron que los organismos públicos pudieran seguir prestando servicios esenciales, por mencionar solo algunos ejemplos.

Este informe, basado en las observaciones que hemos recibido directamente de 5400 directores de TI de 30 países, pone de manifiesto las realidades a las que se han enfrentado los equipos de TI en los últimos 12 meses. Revela los cambios que han experimentado a lo largo de 2020, con especial atención a la ciberseguridad, y el impacto de esos cambios en los miembros de los equipos de TI. El informe también analiza el futuro de los equipos de seguridad TI: revela las expectativas de TI para los próximos cinco años y ayuda a las organizaciones a empezar a crear hoy mismo su equipo de TI del futuro.

Principales conclusiones

Cambios en las experiencias de los equipos de TI durante 2020

- **Creció la carga de trabajo de TI y de ciberseguridad:** el 63 % experimentó un aumento de la carga de trabajo no relacionada con la seguridad, mientras que el 69 % registró un aumento de la carga de trabajo de seguridad TI
- **Los ciberataques se hicieron más frecuentes:** el 61 % confirmó que se había producido un aumento del número de ciberataques a su empresa
- **Los equipos de TI pudieron mejorar sus competencias en materia de ciberseguridad:** el 70 % de los equipos de TI afirmó haber reforzado sus habilidades y conocimientos de ciberseguridad durante este periodo
- **La adversidad unió a los equipos:** el 52 % afirmó que la moral del equipo aumentó durante el año, y las probabilidades de experimentar un incremento en la motivación del equipo fueron considerablemente superiores en el caso de quienes sufrieron ataques (60 % frente al 47 %)

La situación actual

- **Los equipos de TI necesitan ayuda para lidiar con ataques complejos:** el 54 % afirmó que los ciberataques ahora son demasiado avanzados para que su equipo de TI se ocupe de ellos por su cuenta
- **Los equipos de TI se sienten bien preparados para los retos que se avecinan:** el 82 % cree que dispone de las herramientas y los conocimientos necesarios para investigar a fondo las actividades sospechosas

El equipo de TI del futuro

- **Los equipos de seguridad TI aumentarán de tamaño**
  - El 68 % prevé un incremento del personal de seguridad TI interno para 2023 y, el 76 %, para 2026
  - El 56 % estima que el personal de seguridad TI subcontratado aumentará para 2023 y, el 64 %, para 2026
- **La tecnología de IA es una herramienta clave en las futuras estrategias de seguridad**
  - El 92 % confía en que la IA les ayude a hacer frente al creciente número o complejidad de las amenazas

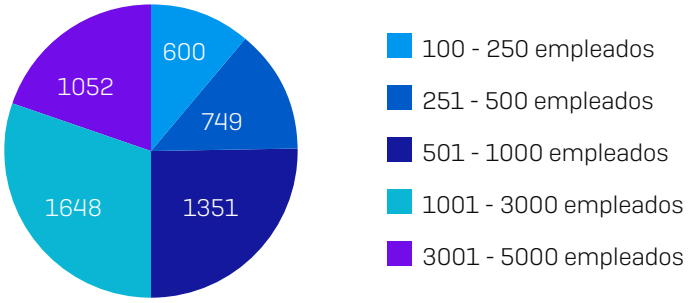
Acerca de la encuesta

Sophos encargó a la consultora independiente Vanson Bourne la realización de una encuesta a 5400 directores de TI de 30 países. La encuesta se llevó a cabo en enero y febrero de 2021.

País	N.º de encuestados	País	N.º de encuestados	País	N.º de encuestados
Australia	250	India	300	Arabia Saudita	100
Austria	100	Israel	100	Singapur	150
Bélgica	100	Italia	200	Sudáfrica	200
Brasil	200	Japón	300	España	150
Canadá	200	Malasia	150	Suecia	100
Chile	200	México	200	Suiza	100
Colombia	200	Países Bajos	150	Turquía	100
República Checa	100	Nigeria	100	EAU	100
Francia	200	Filipinas	150	Reino Unido	300
Alemania	300	Polonia	100	Estados Unidos	500

El 50 % de los encuestados de cada país procedían de organizaciones con entre 100 y 1000 empleados y el otro 50 %, de organizaciones con entre 1001 y 5000 empleados. Los encuestados también pertenecían a una amplia gama de sectores.

¿Cuántos empleados tiene su empresa en todo mundo? [5400]



¿A qué sector pertenece su empresa? [5400]

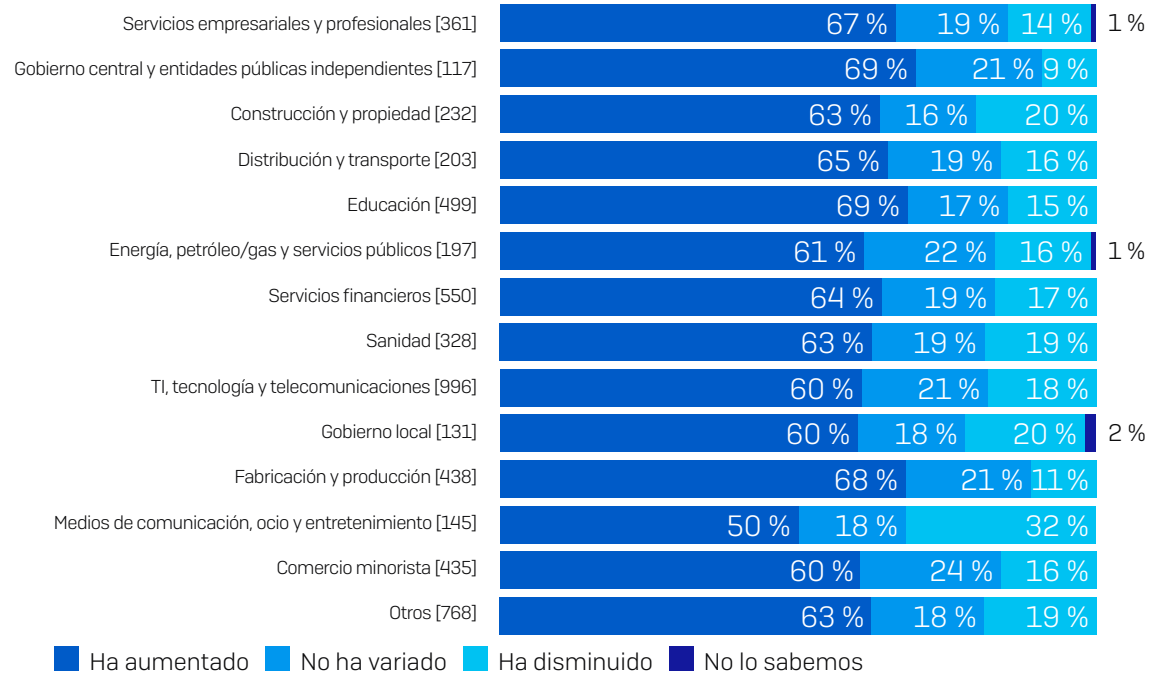
2020: un año de cambios

2020 fue un año como ningún otro, y los equipos de TI encabezaron la adaptación de las operaciones de las organizaciones en respuesta a la pandemia. Como es lógico, esto tuvo un impacto considerable en la carga de trabajo.

Aumentó la carga de trabajo de TI no relacionada con la seguridad...

El año 2020 supuso un gran volumen de trabajo nuevo para los equipos de TI: el 63 % de los directores de TI afirmó que su carga de trabajo no relacionada con la seguridad aumentó en el transcurso de 2020, y solo el 17 % experimentó un descenso. Los países más propensos a registrar un aumento de la carga de trabajo fueron Turquía (84 %), Austria (81 %) y Estados Unidos (75 %).

Cómo ha cambiado la carga de trabajo de TI (no relacionada con la seguridad) durante 2020



A lo largo de 2020, nuestra carga de trabajo de TI (no relacionada con la seguridad) ha disminuido/aumentado/se ha mantenido igual [números base en el gráfico], dividida por sector

Si observamos los datos por sector, vemos que los equipos de TI del **gobierno central y entidades públicas independientes** y de la **educación** fueron los más afectados: el 69 % de los encuestados manifestó que la carga de trabajo aumentó durante 2020, probablemente debido al papel fundamental que desempeñaron tanto las organizaciones gubernamentales como las educativas en la respuesta a la pandemia. En cambio, el sector de **medios de comunicación, ocio y entretenimiento** registró el mayor porcentaje de encuestados que experimentaron un descenso (32%), probablemente debido, al menos en parte, a que la pandemia obligó a muchos establecimientos a limitar sus servicios.

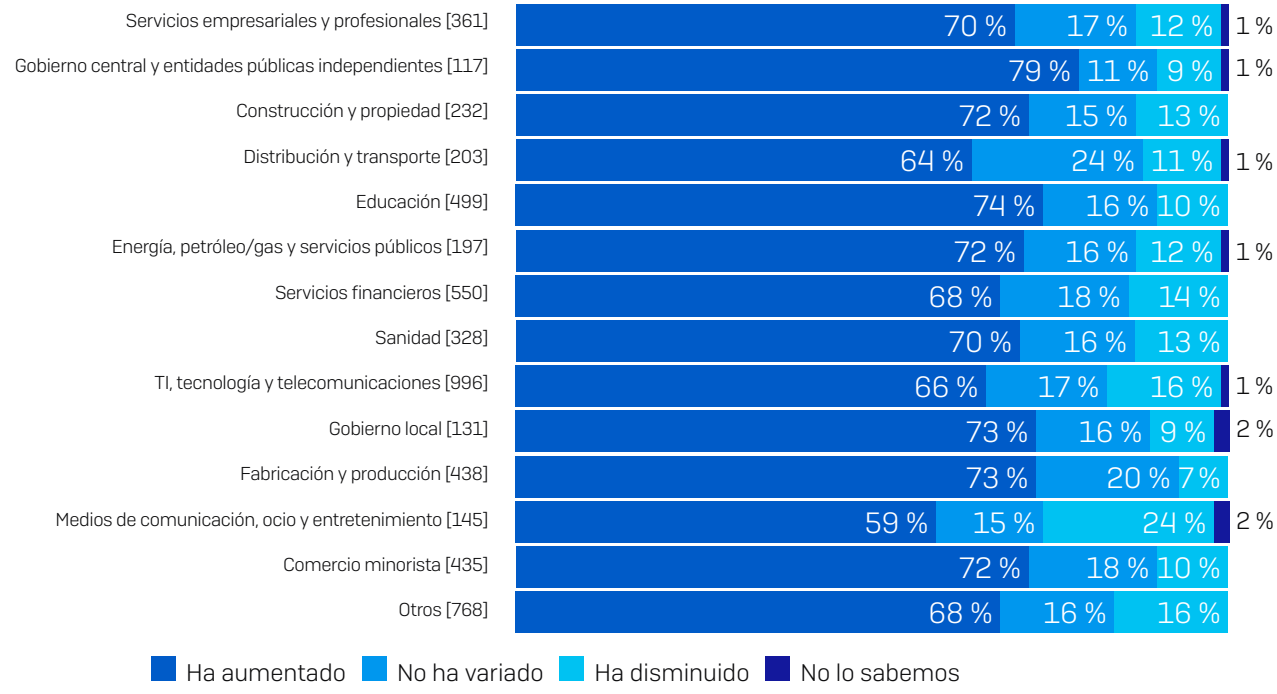
...y la carga de trabajo en ciberseguridad creció aún más

Cómo ha cambiado la carga de trabajo en ciberseguridad durante 2020

A lo largo de 2020, nuestra carga de trabajo en ciberseguridad ha disminuido/aumentado/se ha mantenido igual [5400], omitiendo "No lo sabemos"

El 69 % de los encuestados afirmó que su carga de trabajo en materia de ciberseguridad había aumentado con respecto al año anterior, el 13 % señaló que había disminuido y el 17 % dijo que su carga de trabajo había permanecido igual. De nuevo, Turquía (82 %) es el país que registró el mayor incremento, seguido de Suecia (80 %), Israel y Brasil (ambos con un 78 %). En el extremo opuesto, los encuestados de los Emiratos Árabes Unidos fueron los más propensos a experimentar una disminución de la carga de trabajo en ciberseguridad (26 %), seguidos por los de Suiza (22 %) y Nigeria y Filipinas (ambos con un 19 %).

Cómo ha cambiado la carga de trabajo en ciberseguridad durante 2020



Durante 2020, nuestra carga de trabajo en ciberseguridad ha disminuido/aumentado/se ha mantenido igual [números base en el gráfico], dividida por sector

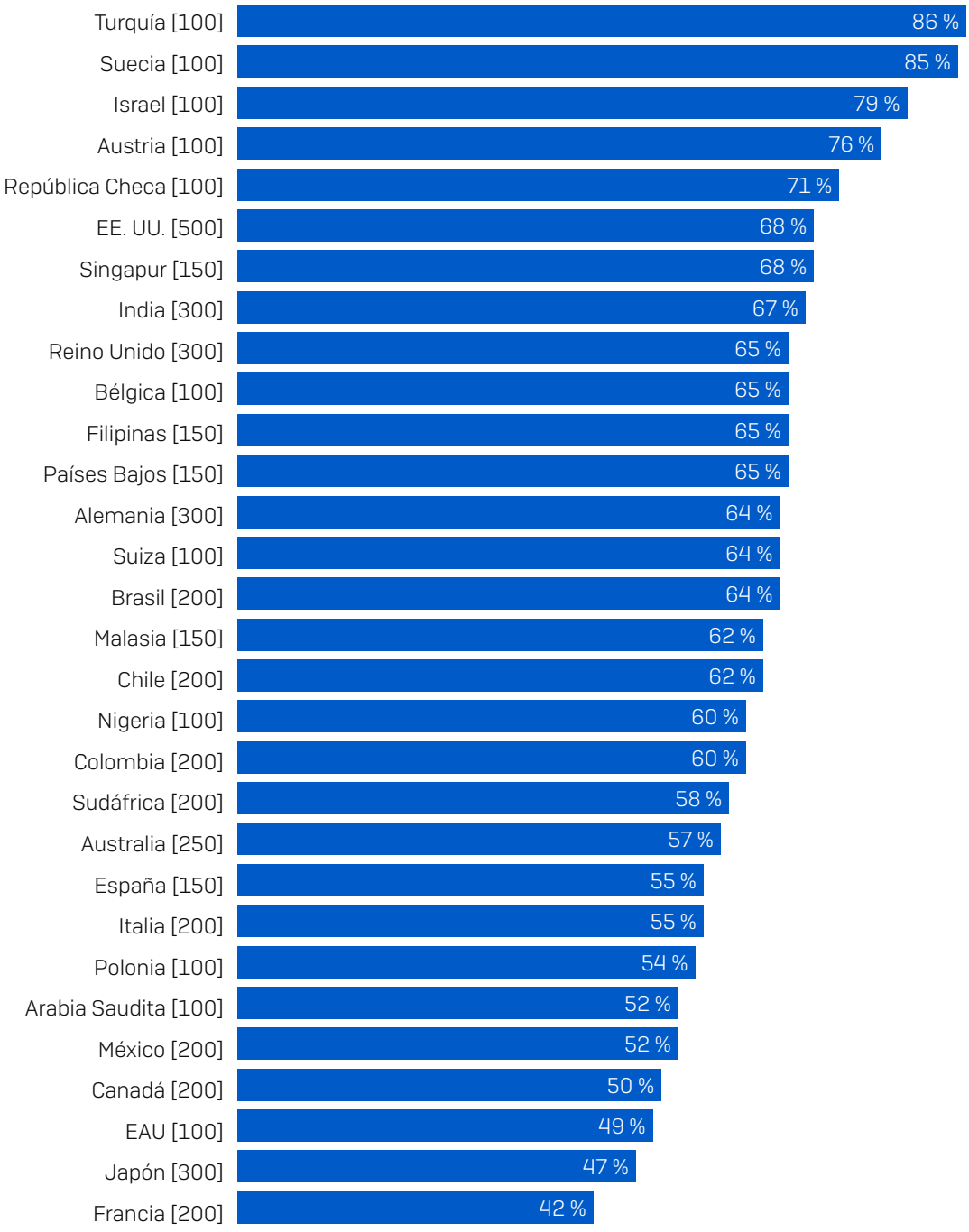
Coincidiendo con la tendencia que hemos visto anteriormente, los sectores más propensos a registrar un aumento de la carga de trabajo en ciberseguridad con respecto al año anterior fueron el del **gobierno central y entidades públicas independientes** (79 %) y el de la **educación** (74 %); el sector de **medios de comunicación, ocio y entretenimiento** fue el menos propenso a informar de un descenso (24 %). De nuevo, es probable que esto se deba a que estos sectores se encuentran entre los más afectados por la pandemia, aunque de forma muy diferente.

Aumento de la frecuencia de los ciberataques

El aumento de la carga de trabajo en materia de ciberseguridad en el transcurso de 2020 fue debido, en parte, al incremento de los ciberataques: más de seis de cada diez (61 %) encuestados registraron un repunte de los ataques a su organización el año pasado. Solo el 19 % afirmó haber experimentado un descenso.

Este crecimiento se produjo en todos los sectores, y la diferencia entre los que experimentaron el mayor aumento (**gobierno central y entidades públicas independientes**) y el menor (**TI, tecnología y telecomunicaciones**, y **medios de comunicación, ocio y entretenimiento**) fue de solo 16 puntos porcentuales (74 % frente a 58 %).

Porcentaje de organizaciones de los encuestados que experimentaron un aumento de los ciberataques durante 2020



Durante 2020, los ciberataques han aumentado [números base en el gráfico], omitiendo algunas opciones de respuesta, divididas por país

Sin embargo, cuando analizamos los datos por país, vemos una diferencia mucho mayor; por ejemplo, más del doble de los encuestados en Turquía registraron un aumento de los ataques en comparación con los de Francia (86 % frente a 42 %). Un porcentaje muy alto de encuestados en Suecia (85 %), Israel (79 %) y Austria (76 %) también informaron de un incremento de los ciberataques a su organización durante 2020. Por el contrario, en Francia, Japón y los Emiratos Árabes Unidos, menos de la mitad registraron un aumento.

Los ataques son cada vez más difíciles de detener

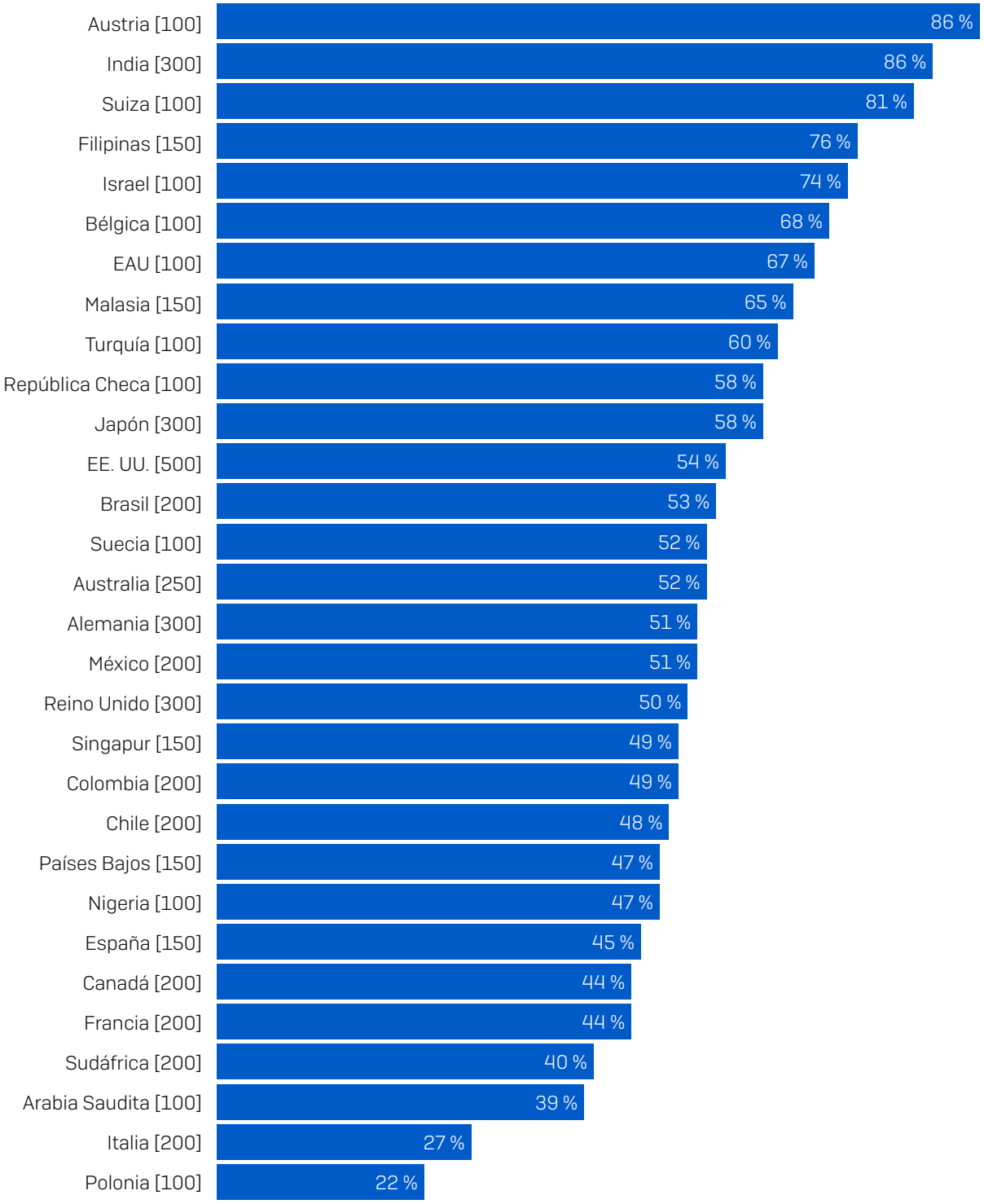
Los ciberataques avanzados son complejos y tienen varias fases, y los adversarios utilizan una gran cantidad de tácticas, técnicas y procedimientos (TTP) en el transcurso de un incidente. Hacer frente a estos ataques es un reto, y para más de la mitad de los encuestados (54 %), los ataques ahora son demasiado avanzados para que su equipo de TI se ocupe de ellos por su cuenta.

Afirma que los ciberataques ahora son demasiado avanzados para que el equipo de TI de su organización se ocupe de ellos por su cuenta

Este desafío es más grave en el sector de los **servicios empresariales y profesionales**, donde el 63 % de los encuestados cree que ya no es capaz de ocuparse de los ciberataques por su cuenta, seguido de cerca por el **gobierno central y entidades públicas independientes** (62 %) y la **sanidad** (60 %). Por el contrario, los sectores de la **construcción y la propiedad** y el **gobierno local** son los que menos de acuerdo están con esa afirmación (47 %). En el caso del gobierno local, este es un dato sorprendente, ya que, como se publicó en El estado del ransomware 2021, es el sector con más probabilidades de que se cifren sus datos en un ataque de ransomware.

Entre los países encuestados, observamos una considerable diferencia en el nivel de confianza para hacer frente a los ataques complejos.

Encuestados que opinan que los ciberataques ahora son demasiado avanzados para que su equipo de TI se ocupe de ellos por su cuenta



Encuestados que coinciden en que los ciberataques ahora son demasiado avanzados para que el equipo de TI de su organización se ocupe de ellos por su cuenta [números base en el gráfico], omitiendo algunas opciones de respuesta, divididas por país

Los encuestados de Austria y la India son los que menos confianza tienen a la hora de lidiar con los ataques, ya que el 86 % afirmó que son demasiado complejos para que su equipo de TI los resuelva por su cuenta, seguidos por los de Suiza (81 %), Filipinas (76 %) e Israel (74 %).

Reconocer la complejidad de los ataques e identificar cuándo se necesita experiencia externa es un paso clave para defenderse de los ciberataques avanzados de hoy día. Los equipos de SophosLabs y Sophos Managed Threat Response han observado un aumento constante del número de ataques que combinan la automatización con el hacking manual en vivo a fin de burlar las defensas de una organización. Para detener estos sofisticados ataques se necesitan expertos cualificados, y las organizaciones hacen bien en reconocer cuándo es necesario subcontratar estas capacidades.

En el extremo opuesto, Polonia es el país que menos dificultades tiene para hacer frente a los ciberataques a nivel interno, ya que solo el 22 % de los encuestados afirmó que los ataques son demasiado avanzados para su equipo de TI, seguido de cerca por Italia (27 %). Esta confianza ante el creciente número de ataques puede deberse a la inversión en la contratación y la formación de profesionales cualificados capaces de adelantarse a los adversarios. Sin embargo, también puede reflejar una confianza infundada ante los avanzados ataques actuales. En vista de la constante evolución de los enfoques de los adversarios, es importante ser realista en cuanto al nivel de conocimientos necesarios para detenerlos.

Los tiempos de respuesta han subido

Teniendo en cuenta el aumento generalizado de la carga de trabajo durante 2020, junto con los retos de adaptación a la pandemia, quizás no resulte sorprendente que una mayoría significativa de los encuestados (61 %) haya registrado un aumento del tiempo de respuesta a los casos de TI durante este periodo. El 20 % afirmó que el tiempo de respuesta disminuyó durante este periodo, mientras que para el 19 % se mantuvo igual.

Cambios en el tiempo de respuesta a los casos de TI durante 2020

Durante 2020, nuestro tiempo de respuesta a los casos de TI ha disminuido/aumentado/se ha mantenido igual [5400], omitiendo "No lo sabemos"

El aumento del tiempo de respuesta fue más generalizado en el sector de la **educación**, donde el 65 % de los encuestados registró un incremento. La necesidad de que los centros educativos de la mayoría de países se pasaran a la formación online durante 2020 creó un volumen de trabajo considerable para los equipos de TI, lo que repercutió en su capacidad para responder rápidamente a las incidencias.

El sector de **medios de comunicación, ocio y entretenimiento** fue el que más redujo el tiempo de respuesta, ya que casi un tercio (32 %) aseguró que pudo responder a las incidencias más rápidamente. De nuevo, es probable que la pandemia contribuyera en gran medida a este cambio, ya que al reducirse la actividad de estas empresas, el equipo de TI disponía de más tiempo para ofrecer una respuesta más rápida.

El impacto de 2020 en el equipo de TI

No todo son malas noticias. En lo que respecta al estado de los equipos de TI, hay mucho por lo que sentirse alentados. El 70 % de los responsables de TI afirmó que la capacidad de su equipo para seguir desarrollando sus habilidades y conocimientos en materia de ciberseguridad aumentó en el transcurso de 2020, y solo el 12 % manifestó que disminuyó.

Cambios en la capacidad de reforzar habilidades y conocimientos de ciberseguridad durante 2020

Durante 2020, la capacidad de reforzar nuestros conocimientos y habilidades en materia de ciberseguridad ha disminuido/aumentado/se ha mantenido igual [5400], omitiendo "No lo sabemos"
Por motivos de redondeo, los resultados no suman el 100 %

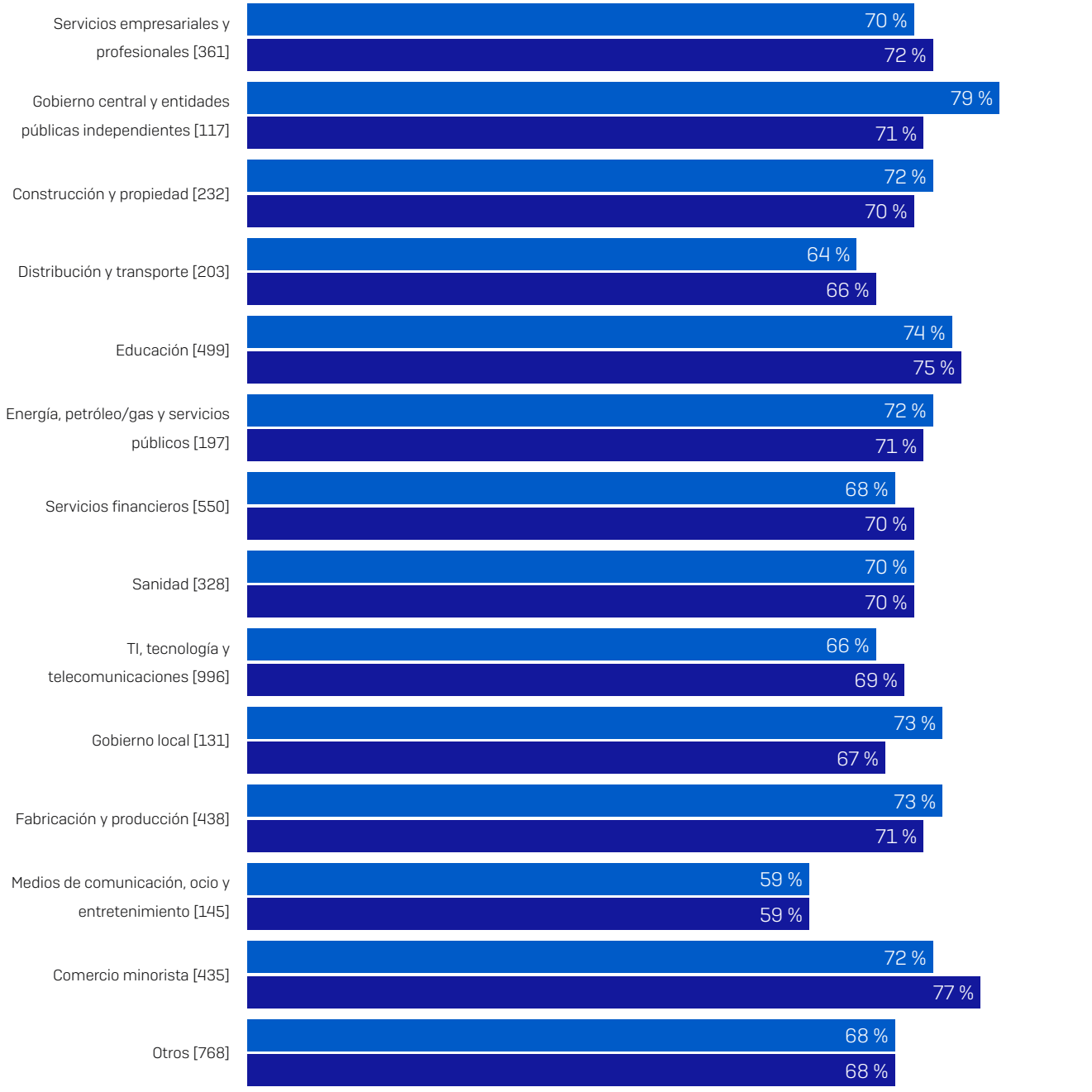
Curiosamente, varios sectores que se vieron especialmente afectados por la pandemia relataron experiencias opuestas:

- El **comercio minorista** fue el sector que más pudo mejorar sus habilidades y conocimientos en materia de ciberseguridad (77 %). Es probable que el gran giro hacia el comercio online durante el confinamiento supusiera nuevos retos y oportunidades para los equipos de TI de este sector.
- La **educación** fue el segundo sector que más mejoró sus aptitudes y conocimientos de ciberseguridad (75 %). Este es otro sector que experimentó una gran transformación durante el año pasado, y aunque el paso a la enseñanza y el aprendizaje online supuso sin duda un enorme reto para los equipos de TI, también creó una gran oportunidad de aprendizaje.
- El sector de **medios de comunicación, ocio y entretenimiento** registró el menor aumento (59 %). Este sector también registró el mayor descenso de las cargas de trabajo (tanto las no relacionadas con la seguridad como las relativas a la ciberseguridad), por lo que es probable que la reducción de la actividad limitara las oportunidades de desarrollo.

El aumento de la carga de trabajo conlleva un aumento de los conocimientos y habilidades

En general, los datos revelaron una clara correlación entre el aumento de la carga de trabajo en ciberseguridad y el aumento de la capacidad para desarrollar conocimientos y aptitudes en ciberseguridad en todos los sectores.

Aumento de la carga de trabajo en ciberseguridad y aumento de la capacidad para desarrollar conocimientos y habilidades de ciberseguridad



Durante 2020, se ha incrementado nuestra carga de trabajo en ciberseguridad / Durante 2020, se ha incrementado nuestra capacidad de ampliar los conocimientos y habilidades en ciberseguridad [números base en el gráfico], dividida por sector

Entre los encuestados que registraron un incremento de la carga de trabajo en ciberseguridad durante 2020, el 84 % también afirmó que aumentó su capacidad para desarrollar sus habilidades y conocimientos de ciberseguridad. Del mismo modo, más de ocho de cada diez (82 %) de los que registraron un aumento de los ciberataques en su organización también aseguraron que había incrementado su capacidad para desarrollar sus aptitudes y conocimientos en materia de ciberseguridad. Esto es lógico: aunque el aumento de la carga de trabajo y de los ciberataques añade presión, también ofrece oportunidades para desarrollar nuevas habilidades.

La moral del equipo ha mejorado

Más de la mitad de los responsables de TI encuestados (52 %) afirmaron que la moral del equipo aumentó durante 2020. El 26 % afirmó que disminuyó y el 22 % que se mantuvo igual.

Cambios en la moral del equipo durante 2020

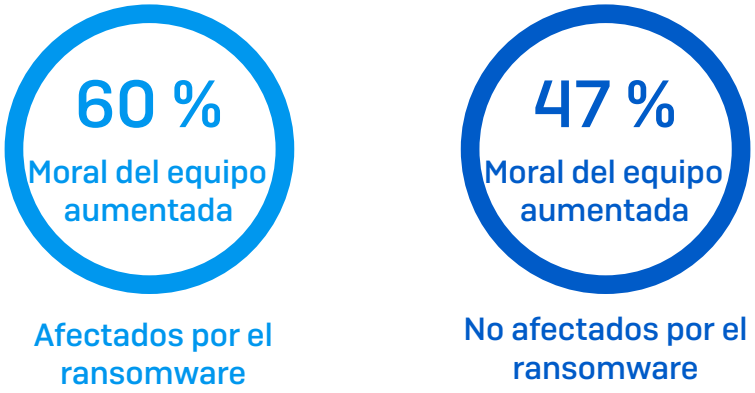
Durante 2020, la moral del equipo ha disminuido/aumentado/se ha mantenido igual [5400], omitiendo "No lo sabemos"

Desde el punto de vista geográfico, el mayor incremento de la motivación se registró en Turquía (75 %), Austria (71 %) e India y Sudáfrica (ambos con un 69 %). En el otro extremo, los equipos de TI de Israel (26 %), Francia (31 %), Italia (33 %) y Polonia (36 %) fueron los menos propensos a registrar una mejora de la moral del equipo.

Habrá observado que varios de los países destacados aquí también se han mencionado en secciones anteriores. Turquía y Austria, que tenían la mayor proporción de encuestados que afirmaron que la moral del equipo había aumentado, están entre los cuatro primeros países que registraron un aumento de los ciberataques. Del mismo modo, Francia presentó el segundo porcentaje más bajo de encuestados que registraron un aumento de la moral del equipo y también el menor aumento de ciberataques de todos los países encuestados. Esta correlación entre la experiencia de ciberataques y la moral del equipo es uno de los resultados más sorprendentes de la encuesta.

Un dato más que demuestra este punto es que el 60 % de los encuestados cuya organización se vio afectada por un ataque de ransomware en los 12 meses anteriores registraron un aumento de la moral del equipo, en comparación con el 47 % de los que no se vieron afectados.

Cambios en la moral del equipo durante 2020

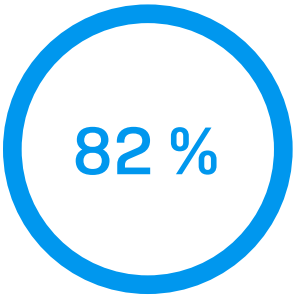


En el transcurso de 2020, la moral de nuestro equipo ha disminuido/aumentado/se ha mantenido igual [5400], omitiendo algunas opciones de respuesta, divididas por los encuestados cuya organización se vio afectada por el ransomware en el año anterior

Hay varios factores que podrían explicar esta correlación. La adversidad (en este caso, los ciberataques) a menudo brinda a las personas la oportunidad de unirse y trabajar en equipo hacia un objetivo común, lo que eleva la moral. Además, poder prestar apoyo a la organización frente a los crecientes ataques aporta una sensación de satisfacción. El mayor incremento de la moral lo registraron dos sectores muy afectados por la pandemia: la **educación** fue el sector más favorecido (58 %), seguido de cerca por la **sanidad** (57 %).

Al mismo tiempo, el papel fundamental que han desempeñado los equipos de TI para hacer posible la continuidad de la actividad frente a la pandemia puede haber dado lugar a una mayor concienciación y reconocimiento de su contribución, lo que también contribuye a elevar la moral. Si los equipos de TI no han sido debidamente reconocidos, ahora es el momento de hacerlo.

Los equipos de TI se sienten bien preparados para los retos que se avecinan



Afirma que dispone de las herramientas y los conocimientos necesarios para investigar a fondo las actividades sospechosas

Encuestados que coinciden en que si detectan actividades sospechosas en su organización, tienen las herramientas y los conocimientos necesarios para investigar a fondo [5400], omitiendo algunas opciones de respuesta

Ante el aumento de la carga de trabajo y la frecuencia de los ciberataques durante 2020, resulta alentador que el 82 % de los directores de TI afirme tener las herramientas y los conocimientos necesarios para investigar a fondo las actividades sospechosas si se detectan en su organización. Las oportunidades proporcionadas para desarrollar habilidades y conocimientos durante 2020 están preparando adecuadamente a los equipos para los desafíos que se avecinan. Seguir invirtiendo en herramientas y formación es esencial para que los equipos de TI puedan seguir el ritmo de la continua evolución de los ciberataques.

Sin embargo, si analizamos las respuestas a esta pregunta por sector, vemos dos atípicos claros: el **gobierno central y entidades públicas independientes** (67 %) y el **gobierno local** (64 %). En todo el mundo, el sector gubernamental se ha visto muy afectado por la pandemia. Ha tenido que garantizar la continuidad de los servicios esenciales durante un periodo de interrupción prolongado y, al mismo tiempo, proporcionar apoyo adicional tanto a los ciudadanos como a las organizaciones. Por otra parte, la financiación del sector público es un reto constante en muchos países, lo que puede limitar los recursos disponibles. Dado que los responsables del ransomware se centran en gran medida en las organizaciones gubernamentales, es esencial que cuenten con las aptitudes y los recursos necesarios para investigar las actividades sospechosas de forma eficaz.

El futuro del equipo de seguridad TI

Como hemos visto, el año pasado fue una ardua lucha para gran parte de los profesionales de TI. Sin embargo, los equipos de TI afrontaron los retos de 2020 de forma admirable y, como resultado, reforzaron tanto sus competencias como su moral. Estas experiencias, junto con una serie de cambios más amplios en el panorama de TI, como el aumento del trabajo flexible y el uso de la nube, repercutirán directamente en el equipo de seguridad TI del futuro.

Los equipos de seguridad TI crecerán, y rápidamente

Ante las crecientes exigencias a los equipos de TI, los encuestados prevén un crecimiento considerable del personal de seguridad TI, tanto interno como subcontratado, sobre todo en los próximos dos años:

- El 68 % prevé que el personal interno se incremente en los próximos dos años, y el 76 % espera un aumento en los próximos cinco años
- El 56 % prevé que el personal de TI subcontratado aumente en los próximos dos años, y el 64 % anticipa un aumento en los próximos cinco años
- Solo el 8 % prevé que el número de empleados internos disminuya en un plazo de cinco años

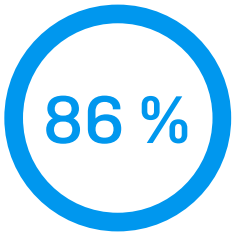
Dotación de recursos de seguridad TI	Cambio previsto	Para 2023	Para 2026
Personal interno de seguridad TI	Aumento	68 %	76 %
	Disminución	11 %	8 %
Personal subcontratado de seguridad TI	Aumento	56 %	64 %
	Disminución	14 %	10 %

¿Cómo cree que cambiará el tamaño del equipo de seguridad TI de su organización de aquí a 2023 y a 2026? [5400], excluyendo algunas opciones de respuesta

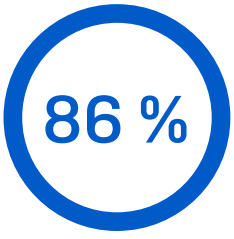
Curiosamente, el aumento del personal de TI subcontratado no se produce a expensas de los equipos internos. Casi la mitad (46 %) de los encuestados prevén que el personal de seguridad TI, tanto interno como subcontratado, crezca de aquí a 2023, y el 55 % estima un aumento para 2026.

En general, el 77 % de los encuestados prevé un incremento en al menos un área de contratación (interna o externa) en los próximos dos años, y el 85 % prevé un aumento de aquí a 2026.

La inteligencia artificial es clave



Confía en que la IA ayude a afrontar el creciente número de ataques



Confía en que la IA ayude a afrontar la creciente sofisticación de los ataques

Encuestados que confían en que las tecnologías de IA ayudarán a hacer frente al creciente número de ataques o confían en que las tecnologías de IA ayudarán a hacer frente a la creciente sofisticación de los ataques [5400], omitiendo algunas opciones de respuesta

Casi de forma universal, los equipos de TI están recurriendo a las tecnologías de inteligencia artificial para ayudarles a combatir el aumento de las ciberamenazas. El 86 % prevé que las tecnologías de IA ayuden a hacer frente al creciente número de ataques, mientras que el mismo porcentaje confía en que las tecnologías de IA ayuden a abordar la creciente sofisticación de los ataques, habiendo seleccionado el 92 % al menos una de estas opciones.

Cree ahora el equipo de seguridad TI del futuro

Para crear el equipo de TI del futuro hay que empezar ahora. Las organizaciones pueden servirse de esta información, que procede directamente de la primera línea de batalla, a fin de prepararse para afrontar con éxito los retos de ciberseguridad en 2023 y más allá. A partir de las conclusiones de este informe, Sophos ofrece cinco recomendaciones:

1. Implemente herramientas y enfoques que reduzcan la carga de trabajo de los administradores de seguridad TI

El aumento de la carga de trabajo, tanto la relacionada con la seguridad como otra, ha sido muy evidente en el último año. Las organizaciones deben procurar aplicar herramientas y enfoques que reduzcan la carga de trabajo de la seguridad TI, a fin de que los equipos puedan dedicar tiempo a otras actividades.

- **Automatice.** Saque partido de la automatización para reducir la carga de las tareas diarias que absorben el valioso tiempo y energía de los profesionales de TI y los desvían de los proyectos de estrategia. Las máquinas son invariablemente capaces de reaccionar más rápido que los operadores humanos, lo que acelera el tiempo de respuesta y reduce la exposición.
- **Consolide.** Simplifique la administración diaria gestionando todas sus soluciones de ciberseguridad a través de una sola consola unificada. Tener todo en un único lugar elimina la necesidad tanto de ir de consola en consola para gestionar la seguridad como de correlacionar los datos entre los distintos sistemas, lo que supone un gran ahorro de tiempo y esfuerzo para los equipos de TI. Consolidar la seguridad TI también reduce los gastos de gestión de proveedores.
- **Integre.** Elija soluciones que se integren y estén diseñadas para funcionar de forma conjunta. Esto aumenta la capacidad de automatizar tareas y facilita la realización de investigaciones entre productos, además de ofrecer datos más detallados de su posición de seguridad.

2. Invierta en herramientas y formación que permitan a los equipos de TI aprovechar sus nuevas habilidades

Los equipos de TI han desarrollado notablemente sus habilidades y conocimientos en el último año. Sería conveniente que las organizaciones invirtieran en las herramientas y la formación que les permitan utilizar estas nuevas habilidades, y que sigan aprendiendo. Estos recursos también ayudarán a contratar talento nuevo para el equipo.

3. Combine los conocimientos de equipos de TI internos y externos

Las ciberamenazas ya son demasiado complejas para que más de la mitad de los directores de TI puedan hacer frente a ellas por su cuenta, y cada vez lo serán más. Al combinar los conocimientos internos y externos en sus equipos de seguridad, puede obtener lo mejor de ambos mundos: profesionales que conozcan en profundidad las amenazas y su organización. Esta estructura combinada también facilita la adaptación y la respuesta a los cambios, recurriendo a las personas más adecuadas para cada situación. Las organizaciones deben buscar partners de seguridad que puedan completar su equipo de TI con habilidades y capacidades que no estén disponibles a nivel interno, a la vez que proporcionan la flexibilidad necesaria para adaptarse a su modelo operativo preferido.

4. Prepárese para atraer a los mejores talentos mundiales

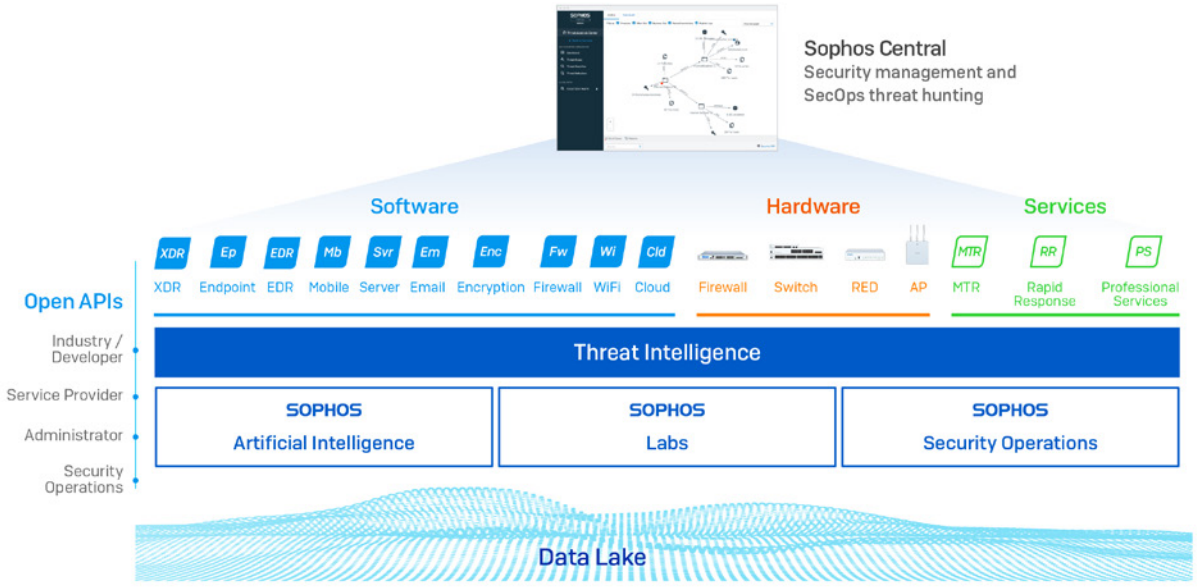
Dado que la mayoría de las organizaciones desean ampliar sus equipos de TI, la competencia por los mejores talentos será feroz. Adoptar tecnologías innovadoras que puedan gestionarse desde cualquier lugar le ayudará a aumentar su reserva de talento. La pandemia nos ha enseñado que casi todas las funciones de TI pueden realizarse a distancia si es necesario. Además, ofrecer herramientas de alta calidad incrementará su atractivo para los candidatos más capacitados.

5. Desarrolle el flujo de trabajo de su equipo de seguridad TI interno

Ya hay escasez de expertos en seguridad TI. Además de ampliar su reserva de talento, las organizaciones también deben buscar programas internos para promover y desarrollar el flujo de trabajo de su equipo de TI, como prácticas y formación en el puesto. Aunque la imagen de un joven con capucha encorvado delante de un ordenador en su habitación es un estereotipo, también es un recordatorio de que muchas personas adquieren conocimientos de ciberseguridad avanzados sin seguir las vías de formación tradicionales.

Cómo puede ayudar Sophos

Sophos ayuda a los equipos de TI de más de 500 000 organizaciones y 150 países a defenderse de las ciberamenazas.



Sophos Adaptive Cybersecurity Ecosystem (ACE), o ecosistema de ciberseguridad adaptativa de Sophos

- Ofrecemos un completo catálogo de **tecnologías next-gen** con **inteligencia artificial**. Nuestros productos están diseñados para funcionar de forma conjunta, automatizando las tareas manuales y reduciendo la exposición a las amenazas: es lo que llamamos Seguridad Sincronizada. Los clientes que cuentan con nuestra protección para endpoints y firewalls observan sistemáticamente una reducción de al menos el 50 % en la administración diaria, así como menos incidentes de seguridad.
- La **detección y respuesta ampliadas (XDR) de Sophos** y la **detección y respuesta para endpoints (EDR) de Sophos** ofrecen a los equipos de TI las herramientas que necesitan para identificar y remediar rápidamente las amenazas y los problemas de higiene de TI. Sophos EDR es la primera solución EDR diseñada tanto para administradores de TI como para analistas de seguridad que permite a los equipos de TI ampliar sus conocimientos sin aumentar la plantilla.
- Todas las tecnologías next-gen de Sophos se gestionan a través de la plataforma de seguridad **Sophos Central**, una herramienta basada en Internet que permite emplear a los mejores profesionales en materia de seguridad, independientemente de su ubicación.
- Los equipos de **Sophos Managed Threat Response (MTR)** y **Sophos Rapid Response** son servicios totalmente administrados que ofrecen experiencia en la búsqueda de amenazas avanzadas y en la respuesta a incidentes para apoyar a los equipos internos. Usted controla cómo y cuándo se derivan los incidentes potenciales y qué acciones de respuesta (si procede) desea que tomemos en su nombre.
- Toda nuestra protección se sustenta en la información sobre amenazas colectiva de **SophosLabs, las operaciones de seguridad de Sophos** y el equipo de **Sophos AI**, además de **Sophos Data Lake**.
- Nuestras **API abiertas** permiten a todos los clientes beneficiarse de los conocimientos y la telemetría de nuestros partners de todo el mundo.

Para saber más sobre lo que hacemos y analizar los retos a los que se enfrenta su equipo, visite nuestro sitio web o hable con un representante de Sophos.

Para saber más sobre lo que hacemos y analizar los retos a los que se enfrenta su equipo, visite nuestro sitio web o hable con un representante de Sophos.

Sophos ofrece soluciones de ciberseguridad líderes en la industria a empresas de todos los tamaños a fin de protegerlas en tiempo real de amenazas avanzadas como el malware, el ransomware y el phishing. Gracias a nuestras funcionalidades next-gen probadas, los datos de su empresa estarán protegidos de forma eficiente por productos con tecnologías de inteligencia artificial y Machine Learning.

20-05-2021 (WP-NP)

SOPHOS