SOPHOS

El rompecabezas imposible de la ciberseguridad

Resultados de una encuesta independiente patrocinada por Sophos a 3100 directores de TI

Monográficos de Sophos Junio de 2019

Contenido

El rompecabezas imposible de la ciberseguridad 2

La encuesta 3

2 de cada 3 empresas fueron víctimas de un ciberataque en 2018 4

- Los ciberataques conllevan preocupaciones en distintos ámbitos 4

Por qué las empresas aún tienen dificultades para reducir los ciberriesgos 5

- N.º 1 Los ataques proceden de múltiples direcciones 5
- N.º 2 Los ciberataques son coordinados, mixtos y constan de varias fases 7
- N.º 3 La tecnología, el talento y el tiempo escasean 8

El reto imposible de la ciberseguridad 10

- Un enfoque distinto: la ciberseguridad como sistema 10
- Seguridad Sincronizada: la clave para resolver el rompecabezas imposible 11

Conclusión 12

El rompecabezas imposible de la ciberseguridad

Resultados de una encuesta independiente patrocinada por Sophos a 3100 directores de TI

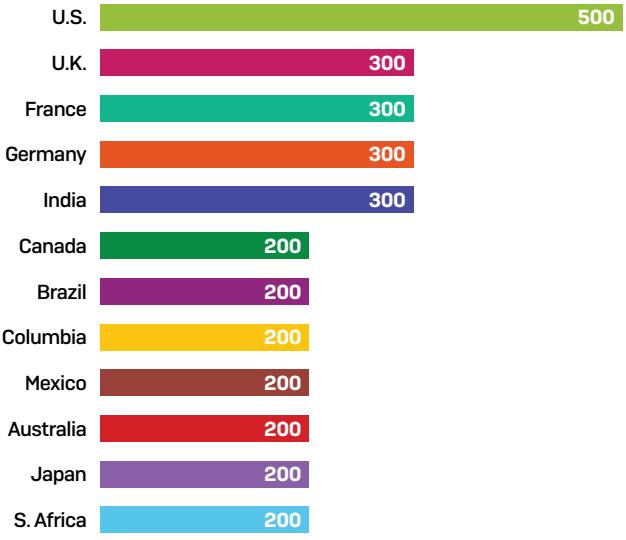
La ciberseguridad está lejos de simplificarse. Si bien las tecnologías de protección siguen avanzando a gran velocidad, también lo hacen los ciberdelincuentes que tratan de eludirlas. Al mismo tiempo, la creciente complejidad de las amenazas hace que controlarlas sea una ardua tarea para los equipos de TI desbordados.

Para comprender estos retos, Sophos encargó un estudio independiente sobre las experiencias de 3100 directores de TI de 12 países. La encuesta, realizada por la firma de investigación Vanson Bourne, aporta revelaciones esclarecedoras sobre los niveles y tipos de ciberataques, así como sobre las dificultades para gestionar la ciberseguridad.

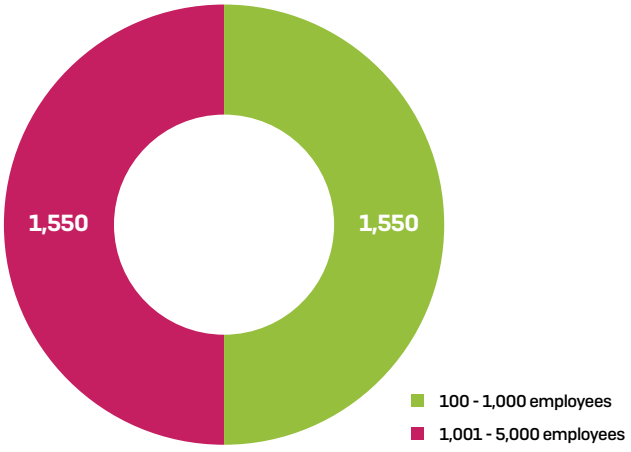
La encuesta

La consultora británica Vanson Bourne entrevistó a 3100 responsables de TI entre diciembre de 2018 y enero de 2019. Para proporcionar un tamaño representativo dentro de cada país, los encuestados se dividieron a partes iguales entre empresas de 100-1000 usuarios y empresas de 1001-5000 usuarios.

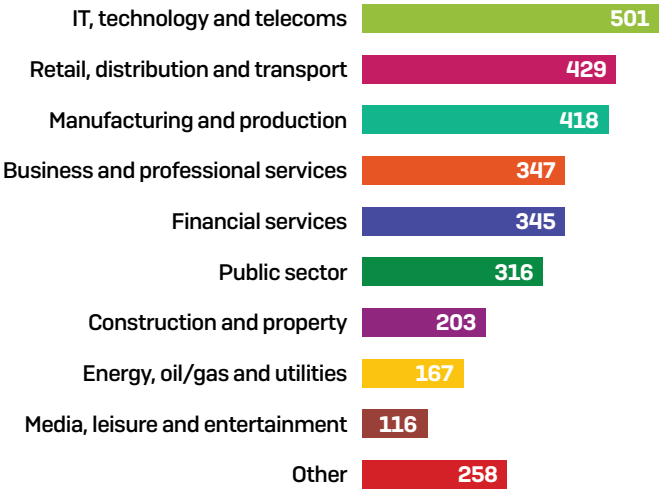
Número de encuestados por país



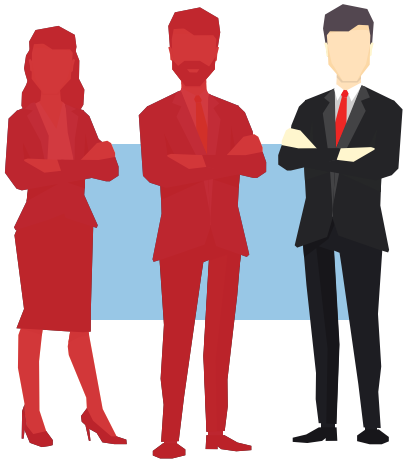
Distribución de los encuestados por tamaño de la empresa



Distribución de los encuestados por sector



2 de cada 3 empresas fueron víctimas de un ciberataque en 2018



A todos los encuestados se les preguntó si habían sufrido un ciberataque en el último año, entendiendo por tal que su empresa no había podido impedir que entrara en la red o los endpoints. El 68 % dijo que sí. De esas empresas afectadas, el promedio de ataques había sido de dos, aunque el 10 % había sufrido cuatro ataques o más.

Es especialmente preocupante que 9 de cada 10 encuestados (90,5 %) dijeron que su empresa contaba con una solución actualizada de protección de ciberseguridad en el momento del ataque o, en el caso de las empresas que se habían visto afectadas varias veces, en el momento del ataque más significativo. De todos los países participantes, los encuestados de Francia eran los más propensos a tener protección actualizada (97,5 %), mientras que los de Colombia eran los menos propensos, ya que solo 7 de cada 10 (70,9 %) tenían protección actualizada.

El 91 % de las empresas contaban con una solución de seguridad actualizada en el momento del ataque

Estos datos revelan que, a pesar de las buenas intenciones y las buenas conductas, las amenazas se abren paso. Esto puede producirse a través de vulnerabilidades de ciberseguridad o porque hay brechas de seguridad que no se han solventado o la protección de las mismas presenta carencias; si bien es posible que una empresa haya estado usando una protección para endpoints actualizada, esto no significa que todos los demás dispositivos fueran seguros.

Los ciberataques conllevan preocupaciones en distintos ámbitos

El riesgo de ciberataques suscita preocupación entre los administradores de TI en varios ámbitos, entre ellos:

Pérdida de datos La cuestión que más preocupa a los encuestados; el 31 % la calificó como su principal preocupación y más de dos tercios (68 %) la consideraron una de sus tres principales preocupaciones.

Coste El 21 % de los encuestados consideraron que el coste (tanto económico como en términos de tiempo y esfuerzo) de hacer frente a un ciberataque era su principal preocupación.

Daños a la empresa Esta cuestión fue una de las tres principales preocupaciones para más de la mitad de los directores de TI (56 %) y la preocupación número uno para el 21 %.

Curiosamente, en el sector de TI impera el espíritu de equipo: los directores de TI anteponen el bienestar del departamento a su situación personal. El 13 % de los encuestados afirmaron que lo que más les preocupaba de sufrir un ciberataque era el daño que causaba a la imagen de TI en toda la empresa, casi el doble de la cifra (7 %) que puso la seguridad de su puesto de trabajo en el primer lugar de la lista.

Por qué las empresas aún tienen dificultades para reducir los ciberriesgos

Como muestran estos resultados, a pesar de las inversiones en tecnologías de seguridad, ahora la norma es sufrir un ciberataque. La encuesta reveló tres razones principales por las que a las empresas les cuesta reducir los ciberriesgos.

N.º 1 Los ataques proceden de múltiples direcciones

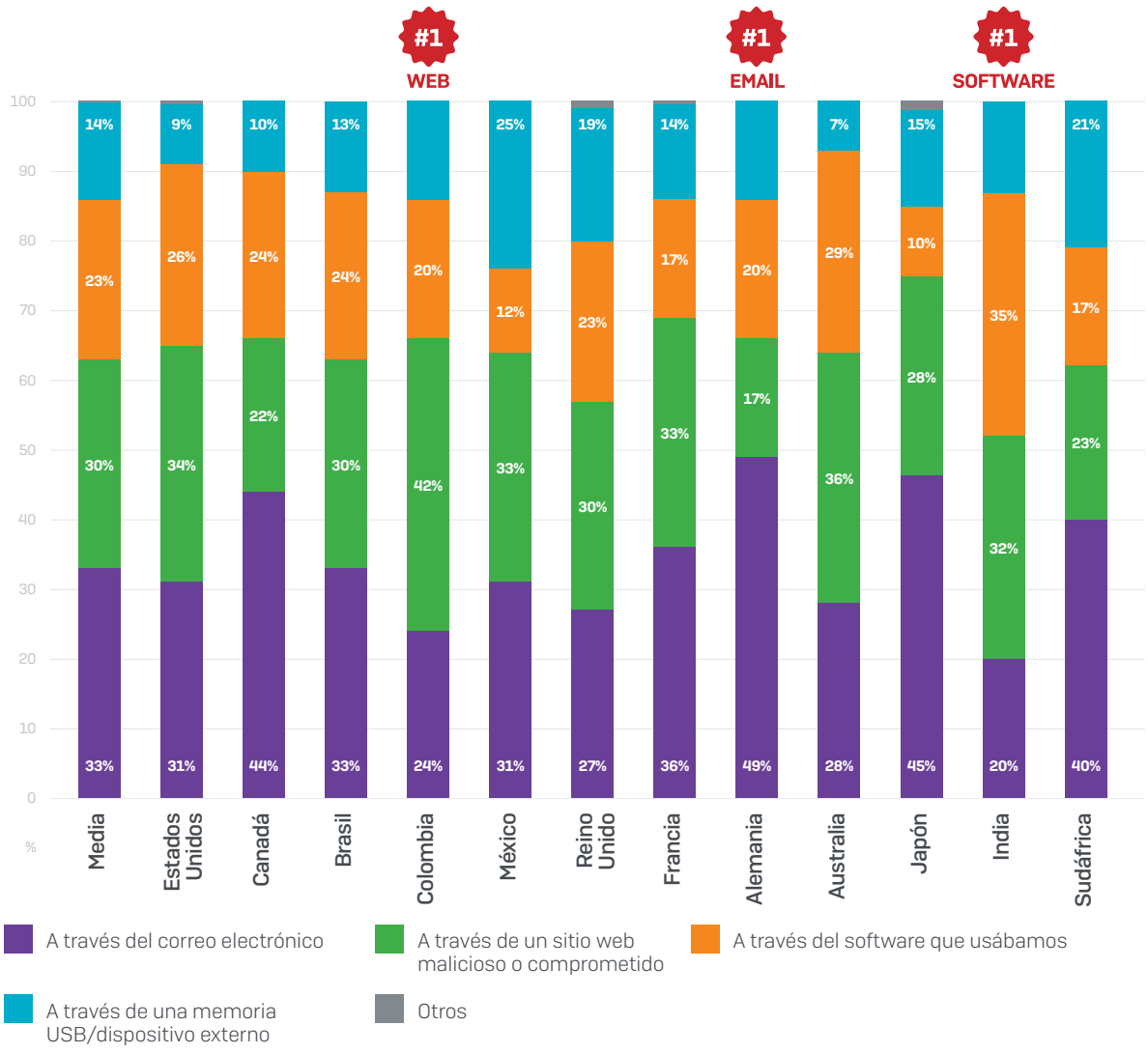
A los encuestados que habían sido víctimas de un ciberataque en el último año se les preguntó cómo había accedido a su entorno el ciberataque más significativo. Los resultados revelaron que, en los casos en que los encuestados saben cómo había entrado el ataque, el correo electrónico es el vector de ataque más habitual, habiendo sido utilizado en el 33 % de los ataques. Dada la prevalencia del phishing (tema que trataremos más adelante), este dato no resulta tan extraño. Internet también es un vector importante, ya que se usa en 3 de cada 10 ataques. En conjunto, el correo electrónico e Internet representan casi dos tercios de los ataques que entran en las empresas.

Sin embargo, los directores de TI no pueden centrarse solo en el correo electrónico e Internet. El 23 % de los ataques se produjo a través de una vulnerabilidad de software y el 14 % a través de una memoria USB o un dispositivo externo. Además, el 20 % de los directores de TI no sabían cómo había entrado el ataque más significativo; si no se sabe qué puerta de seguridad se ha dejado abierta, es difícil cerrarla.

¿Cómo entró en el entorno de su empresa el ciberataque más significativo que ha sufrido en el último año? (redondeado al número entero más cercano)
Base: *encuestados que saben cómo entró el ataque (1685)*

Si se examinan los datos con más detenimiento, queda claro que los vectores de amenazas varían enormemente en todo el mundo. Internet es el vector de ataque más habitual en Colombia, mientras que el correo electrónico es el número 1 en Alemania y las vulnerabilidades de software encabezan la lista en la India. Las memorias USB y los dispositivos externos son el origen de 1 de cada 4 ataques en México.

Esto plantea la interesante cuestión de si esta variación es el resultado de que los ciberdelincuentes utilicen diferentes vectores de ataque en diferentes países o de diferentes vulnerabilidades de seguridad en las distintas zonas geográficas estudiadas.



¿Cómo entró en el entorno de su empresa el ciberataque más significativo que ha sufrido en el último año?

Base: *encuestados que saben cómo entró el ataque (1685)*

Los equipos de TI tienen que gestionar una amplia gama de riesgos en lo que a ciberseguridad se refiere. Preguntamos a los encuestados cuáles creían que eran sus mayores riesgos de seguridad. Teniendo en cuenta los vectores de ataque que acabamos de ver, no es de extrañar que el phishing (n.º 1) y los exploits de software (n.º 2) ocupen un lugar destacado en la lista.

Sin embargo, en tercer lugar están las personas, incluido el personal interno, los contratistas y los visitantes. El 44 % de los encuestados considera que los humanos somos una de las tres principales preocupaciones en materia de seguridad, y claramente suponemos un tipo de desafío de ciberseguridad muy diferente para los equipos de TI.

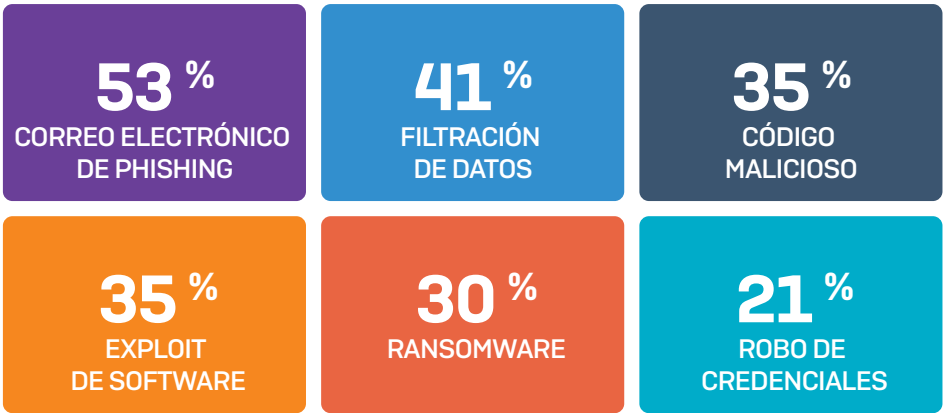
La seguridad Wi-Fi también está muy presente en la mente de los directores de TI, ya que más de un tercio (36 %) la clasifica como una de las tres principales preocupaciones, seguida de los dispositivos desconocidos, que son una de las principales preocupaciones para 3 de cada 10 encuestados (31 %).

¿Cuáles cree que son los principales riesgos de seguridad de su empresa? (combinación de respuestas clasificadas como n.º 1, 2 y 3):

1. Correos electrónicos de phishing **50 %**
2. Exploits de software **45 %**
3. Personas (personal, contratistas, visitantes) **44 %**
4. Redes inalámbricas no seguras **36 %**
5. Dispositivos desconocidos **31 %**

N.º 2 Los ciberataques son coordinados, mixtos y constan de varias fases

Los encuestados cuyas empresas habían sido víctimas de un ciberataque revelaron que habían sufrido una amplia gama de ataques durante el último año.



¿Qué tipo de ciberataques ha sufrido su empresa durante el último año? ***Base:*** *encuestados de empresas que han sufrido un ciberataque o más en el último año (2109)*

Estas cifras suman claramente más del 100 %, lo que indica que ahora los ataques de varias fases son la norma. Por ejemplo, un correo electrónico de phishing podría instalar código malicioso que aprovecha una vulnerabilidad de software para instalar ransomware. Las elevadas cifras implicadas también confirman la magnitud del reto al que se enfrentan los equipos de TI.

Phishing: el ciberataque más frecuente

De las 2109 empresas afectadas por un ciberataque en 2018, más de la mitad (53 %) fueron víctimas del phishing. De hecho, el phishing fue también el ataque más frecuente en todos los países estudiados, con la excepción de Colombia, donde fue la segunda amenaza más común. De los 3100 encuestados, más de un tercio (36 %) habían sido víctimas de correos electrónicos de phishing.

Exploits de software: diferentes repercusiones en todo el mundo

De las empresas afectadas por un ciberataque, más de un tercio (35 %) fueron víctimas de un exploit que se aprovechaba de una vulnerabilidad en el software que utilizaban. Existen variaciones regionales significativas en cuanto a la tendencia a verse afectado por los exploits. En México, más de la mitad de las empresas que sufrieron un ciberataque fueron víctimas de un exploit de software (51 %). Esto es más del doble del número de afectados en Brasil (22 %), Sudáfrica y Japón (ambos 23 %).

Ransomware: vivo y coleando

A pesar de los rumores sobre su desaparición, el ransomware sigue vivo y coleando. 3 de cada 10 (30 %) de las empresas que sufrieron un ciberataque se vieron afectadas por el ransomware. Sin embargo, esta media mundial oculta algunas variaciones significativas según la región:

- La mitad (49 %) de los encuestados japoneses afirmaron que sufrieron un ataque de ransomware, seguidos por el Reino Unido con un 43 %.
- Solo el 5 % de los encuestados mexicanos se vieron afectados por el ransomware, y solamente el 13 % en Colombia.

N.º 3 La tecnología, el talento y el tiempo escasean

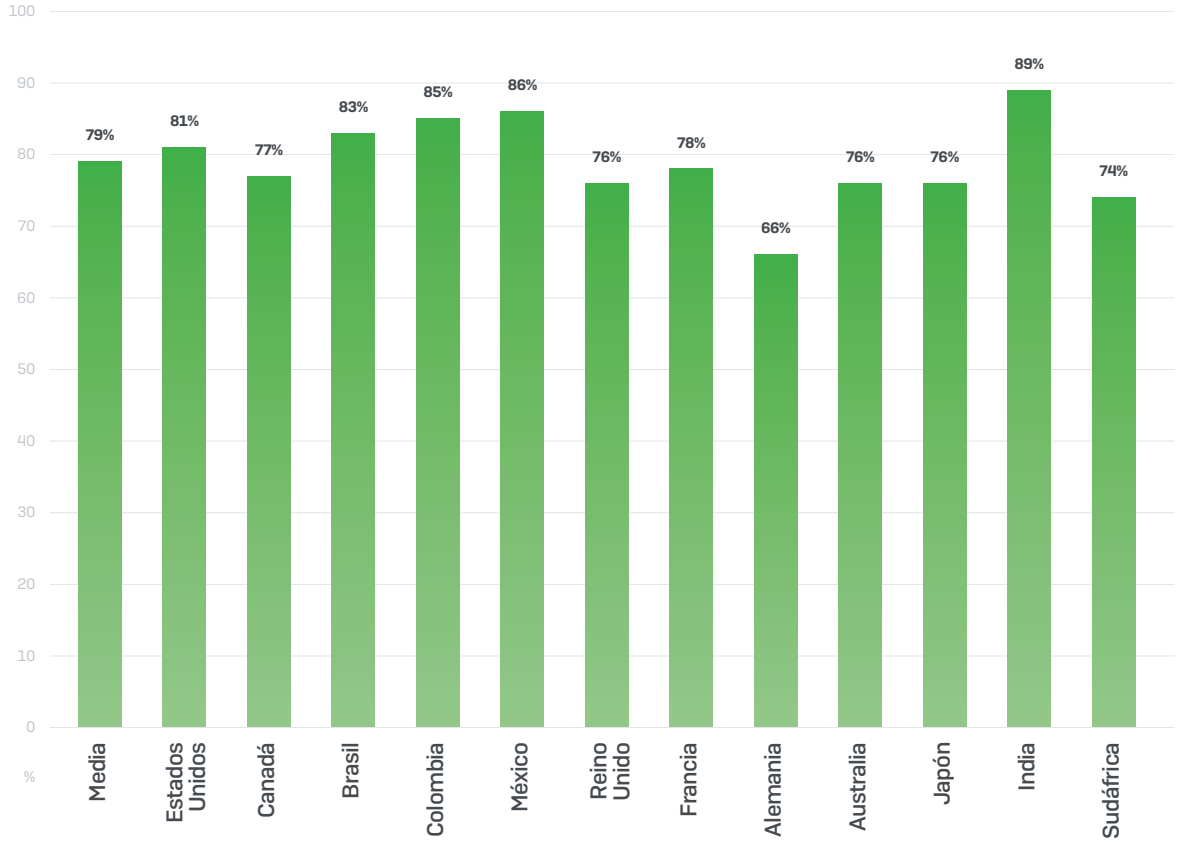
Como hemos visto, las empresas se enfrentan a una amplia gama de ataques y necesitan proteger múltiples vectores de amenazas. La encuesta reveló que, de media, los equipos de TI dedican el 26 % de su tiempo a la gestión de la ciberseguridad. Para la mayoría de los encuestados, esta no es la proporción correcta.

El 26 % del tiempo del equipo de TI se dedica a la ciberseguridad

Las empresas indias son las que dedican más tiempo (32 %) y las japonesas las que menos (19 %). Las empresas que han sufrido un ciberataque dedican un poco más de tiempo a la seguridad TI (28 %) que las que no han sufrido ningún ataque (23 %).

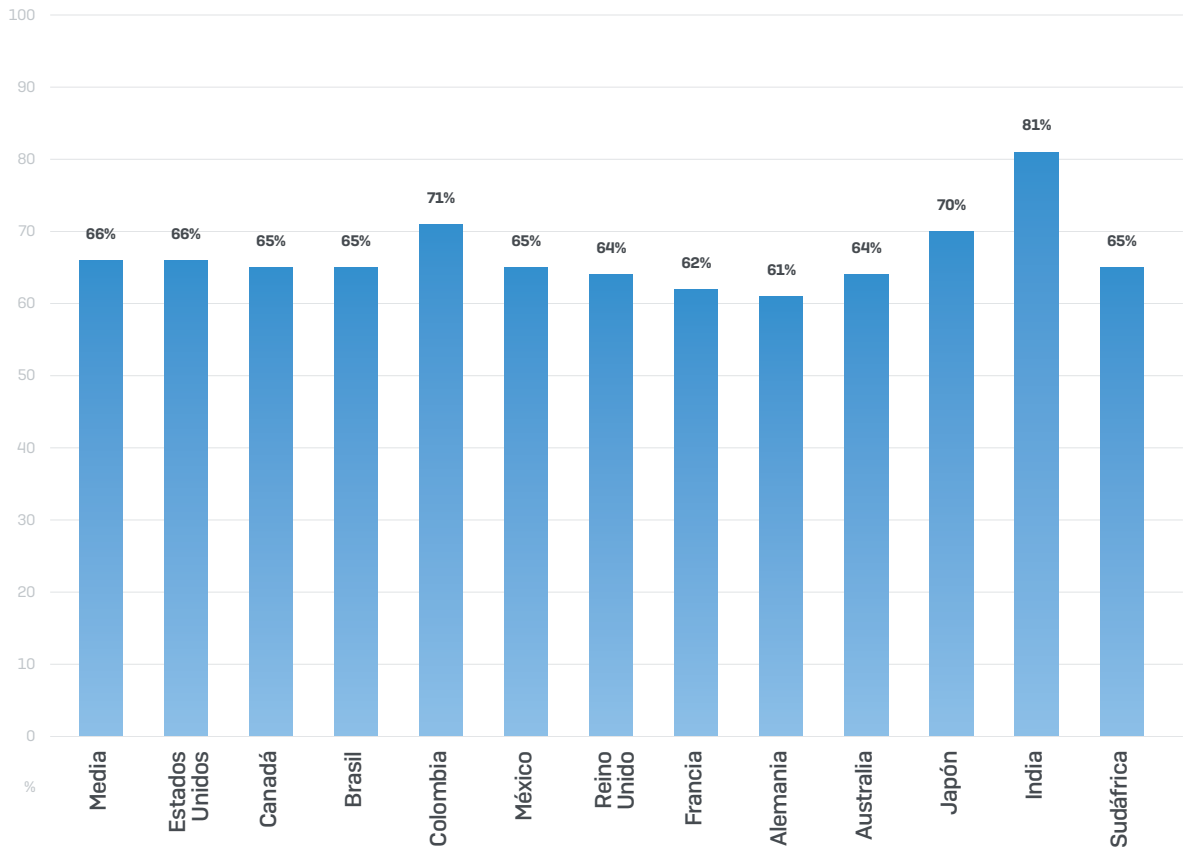
Dada la variedad y complejidad de las amenazas, no es de extrañar que el 86 % de los encuestados afirmen que necesitan mayores conocimientos de ciberseguridad en su empresa. Las empresas que han sufrido un ataque necesitan más conocimientos sobre ciberseguridad que las que no se han visto afectada(un 89 % frente a un 79 %). Esto podría deberse a que tienen más problemas de seguridad que necesitan solucionarse o a una mayor concienciación de la complejidad de los ataques de hoy en día.

Sin embargo, aportar los conocimientos necesarios para solucionar esas carencias es un gran desafío. A 8 de cada 10 empresas les resulta difícil contratar a personas con las habilidades adecuadas. En lo que respecta a la contratación de personal, India es el país que se enfrenta al mayor reto (89 %) y Alemania el que menos, pero aun así, 2 de cada 3 directores de TI alemanes afirman que tienen problemas para contratar a personas con los conocimientos adecuados.



Porcentaje de encuestados que están de acuerdo con la afirmación siguiente: Contratar a personas con los conocimientos de ciberseguridad que necesitamos es un reto. ***Base:*** *todos los encuestados (3100)*

Al mismo tiempo, los presupuestos de ciberseguridad no son suficientes, ya que 2 de cada 3 encuestados (66 %) afirman que su presupuesto para personal y tecnología es demasiado bajo. Este porcentaje aumenta ligeramente hasta el 70 % en las empresas que sufrieron un ciberataque en 2018.



Porcentaje de encuestados que están de acuerdo en que su presupuesto de ciberseguridad (incluidos personal y tecnología) está por debajo de lo necesario. ***Base:*** *todos los encuestados (3100)*

Existen claros paralelismos entre la escasez de presupuesto y la contratación en el ámbito de la ciberseguridad. Alemania, el país con menos dificultades en materia de contratación, es también el que menos carencias presupuestarias tiene. En el otro extremo, la India es el país con más dificultades en cuanto al presupuesto y la contratación.

Este dato refleja la oferta limitada y la gran demanda de conocimientos en materia de ciberseguridad, lo que da lugar a que los profesionales de la ciberseguridad puedan exigir salarios más altos y paquetes de prestaciones.

El reto imposible de la ciberseguridad

Las empresas de tecnología han estado desarrollando productos de ciberseguridad durante décadas, y las empresas siguen invirtiendo tiempo, esfuerzo y dinero en ciberseguridad. Sin embargo, a pesar de años de innovación e inversión, la encuesta ha revelado que la ciberseguridad sigue siendo un verdadero desafío y que las empresas todavía no tienen los recursos que necesitan.

¿Quizás es hora de un enfoque diferente?

Un enfoque distinto: la ciberseguridad como sistema

Como hemos visto, las ciberamenazas funcionan como un sistema que utiliza múltiples técnicas y tecnologías interconectadas en sus ataques. Al mismo tiempo, nuestra infraestructura de TI también es un sistema: una red compleja e interconectada de PC, Mac, servidores, impresoras, dispositivos móviles, aplicaciones, cargas de trabajo en la nube, conmutadores, firewalls, sistemas inalámbricos... y todo el software que se ejecuta en ellos. Si la infraestructura de TI y las ciberamenazas funcionan como un sistema, tiene sentido que la ciberseguridad también funcione como un sistema y no como productos independientes y aislados.

La Seguridad Sincronizada es el galardonado sistema de ciberseguridad de Sophos. Productos para endpoints, redes, dispositivos móviles, redes inalámbricas, correo electrónico y cifrado que comparten información en tiempo real y responden automáticamente a los incidentes. Y al tenerlo todo controlado mediante una sola consola web, la gestión es muy sencilla.

Seguridad Sincronizada: la clave para resolver el rompecabezas imposible

La Seguridad Sincronizada permite a las empresas abordar los complejos desafíos que pone de manifiesto la encuesta.

Múltiples vectores de ataque:

- La completa cartera de soluciones de protección le permite detener las amenazas de todos los vectores de ataque: correo electrónico, Internet, vulnerabilidad de software o dispositivos USB.
- Los productos están diseñados para trabajar juntos, con lo que se eliminan las brechas de seguridad y se evitan problemas de compatibilidad.
- Gracias a una aportación de datos sin precedentes, es posible identificar riesgos desconocidos hasta la fecha, como aplicaciones maliciosas en el tráfico de red.

Ataques complejos, coordinados y de varias fases:

- La protección integrada por capas maximiza sus defensas contra amenazas avanzadas al bloquearlas en varias fases y utilizar varias tecnologías.
- La respuesta automatizada a incidentes reduce drásticamente su exposición a las amenazas al detener y aislar los ataques en cuestión de segundos.
- La información de múltiples entornos le permite identificar y abordar la causa raíz de cualquier problema.

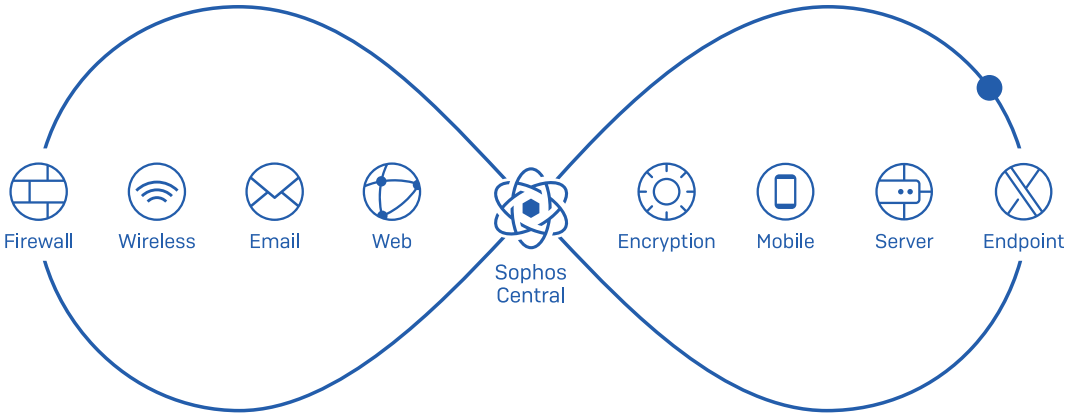
El tiempo, el talento y la tecnología escasean:

- Gestionarlo todo a través de una única consola web reduce considerablemente los gastos diarios, al tiempo que aligera la carga de trabajo de los miembros de equipo.
- La respuesta automatizada a incidentes también reduce la carga administrativa de TI al eliminar la necesidad de identificar y reparar los equipos infectados de forma manual.
- La interfaz uniforme y familiar en todos los productos hace que sea más rápido y fácil comenzar a usar nuevos productos.

Conclusión

A pesar de las grandes y continuas inversiones en tecnología de ciberseguridad, el trabajo de los equipos de TI de todo el mundo está lejos de simplificarse. En lugar de seguir con el mismo enfoque a la ciberseguridad, es hora de pasarse a la ciberseguridad como sistema. Al permitir que los productos de seguridad compartan información y trabajen juntos en tiempo real, puede anticiparse a las amenazas y, al mismo tiempo, liberar valiosos recursos de TI.

La Seguridad Sincronizada de Sophos es el galardonado sistema de ciberseguridad en el que confían miles de empresas de todo el mundo. Para obtener más información y verlo en acción, visite es.sophos.com/synchronized.



Para obtener más información y probarlo, vaya a es.sophos.com/synchronized

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

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

21-06-19 WP-ES (RP)

SOPHOS