vmware®

Informe sobre seguridad global

Las amenazas a las que se enfrenta la empresa geográficamente dispersa

2021

Introducción

Este estudio se realizó para entender los desafíos y problemas que deben abordar las empresas de todo el mundo ante una cantidad cada vez mayor de ciberataques. En él se identifican tendencias en la piratería y los ataques malintencionados, así como el efecto que han tenido las vulneraciones en la economía y la reputación en este último año sin precedentes. Se examinan los planes de las organizaciones para proteger la nueva tecnología, adoptar una estrategia de seguridad que dé prioridad a la nube y hacer frente a la complejidad del entorno actual de gestión de la ciberseguridad.

Se encuestaron 3542 directores de tecnología, directores de informática y directores de seguridad de la información de empresas de distintos sectores a fin de elaborar este informe, que forma parte de un proyecto de investigación que abarca 14 países.

Lea el informe para averiguar cómo los profesionales sénior de la ciberseguridad planean adaptarse a los desafíos de seguridad que supone un lugar de trabajo distribuido y modificar las defensas para lograr una seguridad intrínseca en la infraestructura y las operaciones.

Resumen de gestión:

Introducción

INFORMACIÓN SOBRE EL PANORAMA DE CIBERSEGURIDAD GLOBAL

Rick McElroy, estratega principal de ciberseguridad de la unidad de negocio de seguridad de VMware

Todo ha cambiado, pero sigue igual.

Los profesionales de ciberseguridad que contribuyeron a la cuarta edición de nuestro «Informe sobre seguridad global» se encuentran en una situación muy diferente a la de los que participaron en la encuesta de 2020. Tras un año en el que vimos la mayor y más rápida transformación de los modelos de trabajo de la historia, los equipos de seguridad son responsables ahora de un ecosistema más distribuido y heterogéneo que nunca.

Los programas de transformación digital avanzaron rápidamente a medida que la superficie de los ciberataques llegaba a salas de estar, cocinas, redes domésticas y dispositivos personales. El comportamiento de los empleados en la oficina es muy distintos al de los teletrabajadores, que acceden a la red a horas impredecibles en su intento de conciliar la vida laboral con la familiar. Como consecuencia, el tráfico de red ha cambiado tanto que es casi irreconocible. Los defensores deben adaptar los sistemas de supervisión y los factores desencadenantes, o corren el riesgo de que los atacantes recurran a patrones atípicos para enmascarar sus intentos de infiltración.

Pese a que la situación cambia a toda velocidad, hay cosas que siguen igual: un sector que no se ha visto afectado por la COVID-19 es el de la ciberdelincuencia.

La frecuencia de los ataques es alta y la sofisticación sigue evolucionando y, por lo tanto, las vulneraciones son inevitables.

Tres cuartas partes (el 76 %) de los 3542 participantes en nuestra encuesta dijeron que la cantidad de ataques que han sufrido ha aumentado en los últimos doce meses. De ellos, el 78 % afirmaron que el aumento de los ataques se debía a que hay más empleados trabajando desde casa. El 79 % dijeron que los ataques eran cada vez más sofisticados.

En consecuencia, la cantidad de vulneraciones ha aumentado. Los participantes que sufrieron un ciberataque indicaron una **media de 2,35 vulneraciones al año**. Estos incidentes no fueron de poca importancia. En ocho de cada diez casos, la vulneración fue un incidente importante que hubo que comunicar a los organismos reguladores o que requirió la intervención de un equipo de respuesta a incidentes.

No hay duda de que los equipos de seguridad están sometidos a mucha presión, y no pueden ceder a la autocomplacencia: el 56 % de los directores de seguridad de la información encuestados temen que su organización sufrirá una vulneración importante durante el próximo año.

Los directores de seguridad de la información no pueden vigilar los rincones

La cantidad de ciberataques ha aumentado, pero el rápido cambio hacia el teletrabajo significa que las empresas siguen sin ver el panorama completo. El comportamiento imprevisible de los empleados, los dispositivos personales y el uso de la red doméstica reducen la visibilidad, y se crean puntos ciegos y rincones oscuros en los que los ataques pasan desapercibidos. Por lo tanto:

El 78 %

dijeron que los ataques han aumentado con el teletrabajo.

2,35

es la media de vulneraciones al año según las organizaciones.

El 82 %

dijeron que han sufrido una vulneración importante.

Las aplicaciones de terceros y los programas de secuestro son las principales causas de las vulneraciones

Al preguntar por las causas tras las vulneraciones, hubo casi un empate entre los tres primeros vectores de ataque, lo que describe una situación en la que abundan las amenazas externas y los puntos débiles internos. Las aplicaciones de terceros son el culpable más habitual, seguidas muy de cerca por los programas de secuestro y la tecnología de seguridad anticuada.

El rápido cambio hacia el teletrabajo ha dejado desprotegidas a las organizaciones que han dejado que empeore la integridad de la seguridad y que no han implementado la autenticación multifactor. También fueron causas comunes de las vulneraciones los procesos deficientes y las vulnerabilidades de los sistemas operativos.

Además de estas amenazas, la proliferación de los programas de secuestro ha aumentado las tensiones. Las campañas formadas por fases de intrusión, persistencia, robo de datos y extorsión están incrementando la presión, y los atacantes sacan partido a las interrupciones que sufren los teletrabajadores. En casi todos los ataques de programas de secuestro, el correo electrónico sigue siendo el vector de ataque más frecuente para obtener el acceso inicial.

Resurgimiento de los programas de secuestro

Los programas de secuestro han reaparecido como una de las causas principales tras las vulneraciones, ya que los atacantes lanzan campañas de varias fases sofisticadas y lucrativas.

El 14 % de las vulneraciones en todo el mundo fueron causadas por programas de secuestro.

El secuestro del sector sanitario

El 19 % de las vulneraciones del sector sanitario en todo el mundo fueron causadas por programas de secuestro.

Preocupación en torno al desarrollo y el uso de aplicaciones

Las aplicaciones de terceros son la primera causa de vulneraciones, según los directores de seguridad de la información encuestados. Por lo tanto, no sorprende que los equipos de seguridad se centren en perfeccionar su enfoque de desarrollo y uso de aplicaciones.

Casi dos tercios de los participantes están de acuerdo[1] en que necesitan una mayor visibilidad de los datos y las aplicaciones para evitar ataques. Una cifra parecida está de acuerdo en que se necesita una mejor seguridad contextual para realizar un seguimiento de la seguridad de los datos a lo largo del ciclo de vida de las aplicaciones. Los efectos de la COVID-19 también se hacen notar. Tres de cada cinco participantes creen que deben enfocar la seguridad de forma diferente que en el pasado, ya que la superficie de ataque se ha ampliado.

Las aplicaciones también se consideran el punto más vulnerable del recorrido de los datos, pero no son las únicas que causan preocupación.

Las cargas de trabajo están subiendo considerablemente como una fuente de vulnerabilidad percibida.

El 15 % de los participantes dijeron que las cargas de trabajo eran el punto más vulnerable en el recorrido de los datos en su organización, y señalaron que no era así hace un año.

[1] En los que «están de acuerdo» se incluye a los que están «totalmente de acuerdo» y a los que lo están «algo de acuerdo».

Otro 4 % afirmaron que habían sido su punto más vulnerable durante más de un año. Los equipos admiten que los antivirus tradicionales no protegen las cargas de trabajo de los servidores y que las configuraciones erróneas acarrean un riesgo de vulneración importante. El motivo suele ser la falta de conocimientos de los equipos de seguridad y los de infraestructura. Los primeros no saben cuál es el comportamiento que se espera de las cargas de trabajo de producción, y los segundos no tienen experiencia en cómo se comportan los atacantes. Este año, creemos que las organizaciones tratarán de solucionar estas carencias y reforzar las defensas de las cargas de trabajo en la nube.

En cuanto a la nube, nuestro estudio revela que se está produciendo una transición inexorable. Casi todos los directores de seguridad de la información encuestados tienen una estrategia de seguridad que da prioridad a la nube o planean implementarla muy pronto. Se trata de un cambio importante e indica que las organizaciones están acelerando su plan de seguridad de la nube como respuesta a los desafíos de la COVID-19. Es posible que ya hubieran iniciado la transición, pero ahora dan mucha más importancia a la necesidad de contar con una seguridad exhaustiva que dé prioridad a la nube en un mundo que ya prioriza la nube.

Esperamos que el cuarto **informe de seguridad global de VMware** le parezca interesante e informativo.

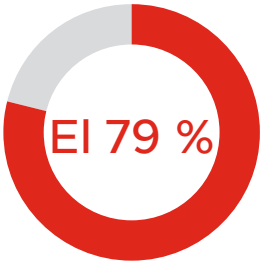
Principales conclusiones

La frecuencia de los ataques y el riesgo de vulneraciones siguen siendo altos

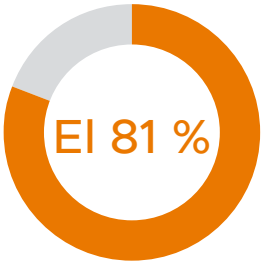
La frecuencia de los ataques es alta, su sofisticación sigue aumentando y, por lo tanto, las vulneraciones son inevitables.

El 76 % dijeron que la cantidad de ataques había aumentado en los últimos 12 meses en un 52 % de promedio en las organizaciones afectadas.

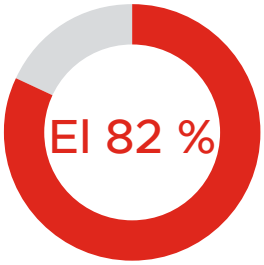
El 78 % de los encuestados que han sufrido un ciberataque afirmaron que los ataques habían aumentado porque había más empleados trabajando desde casa.



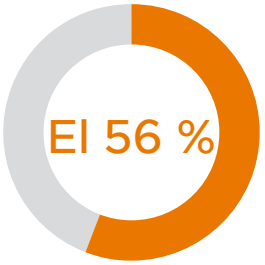
de los encuestados que han sufrido un ciberataque afirmaron que los ataques eran más sofisticados.



han sufrido vulneraciones en los últimos 12 meses. Este grupo sufrió un promedio de 2,35 vulneraciones durante este periodo.



dijeron que las vulneraciones que sufrieron fueron importantes.



temen que sufrirán una vulneración importante en los próximos 12 meses.

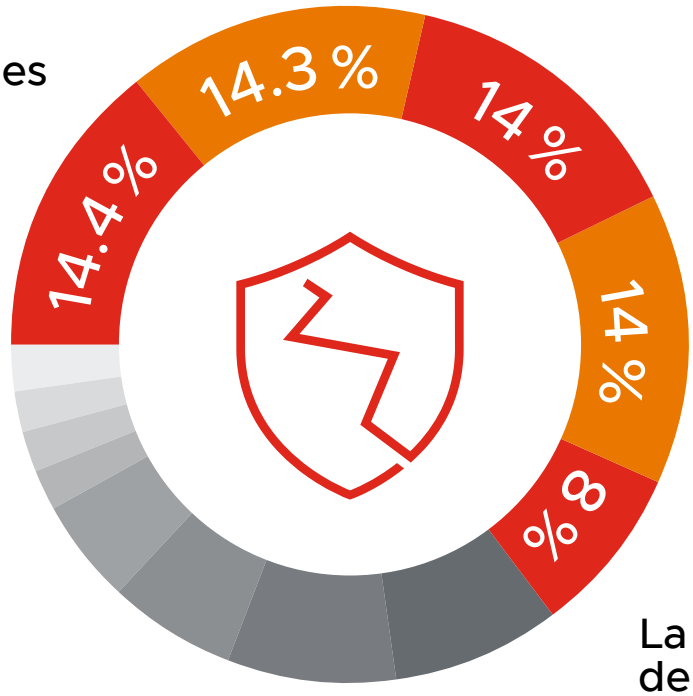
Las aplicaciones, las cargas de trabajo y los programas de secuestro son las principales preocupaciones de los directores de seguridad de la información

Los tres principales vectores que causan vulneraciones describen una situación en la que abundan las amenazas externas y los puntos débiles internos.

Principales causas tras las vulneraciones de quienes sufrieron un ciberataque:

Los programas de secuestro fueron la segunda, con un 14,3 %.

Las aplicaciones de terceros fueron la primera causa, con un 14,4 %.



La tecnología de seguridad anticuada y los puntos débiles de los procesos empataron en tercer lugar, con un 14 %.

La vulnerabilidad de los sistemas operativos es la quinta causa, con un 8 %.

Las aplicaciones y las cargas de trabajo se consideran el punto más vulnerable del recorrido de los datos, pero no son las únicas que causan preocupación.

La ampliación de las superficies de ataque está obligando a los directivos a replantearse el enfoque tradicional de la seguridad

Afortunadamente, ya se admite la necesidad de cambiar fundamentalmente la seguridad para adaptarla a una era digital, altamente conectada y en la que debe tener cabida el teletrabajo.

El 61 % de los encuestados, casi dos tercios, coinciden en que es necesario cambiar su percepción de la seguridad ahora que la superficie de ataque se ha expandido.

El 63 % coinciden en que necesitan una mejor seguridad contextual para hacer un seguimiento de los datos a lo largo de su ciclo de vida.

El 63 % coinciden en que necesitan una mayor visibilidad de los datos y las aplicaciones para prevenir ataques.

Simplificar, consolidar y dar prioridad a la nube forma parte del plan para 2021

Parece que los directores de seguridad de la información encuestados buscan consolidar la tecnología y adoptar un enfoque de seguridad más intrínseco. Además, están aumentando los presupuestos de seguridad para lograr esos objetivos.

↗ El 43 % están integrando una mayor seguridad en las infraestructuras y aplicaciones, y reduciendo la cantidad de soluciones puntuales.

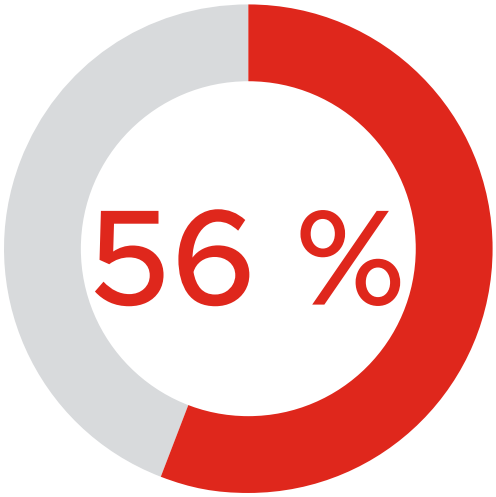
↗ El 42 % han actualizado la tecnología de seguridad para mitigar el riesgo.

↗ El 41 % han actualizado las políticas y el enfoque de seguridad para mitigar el riesgo.

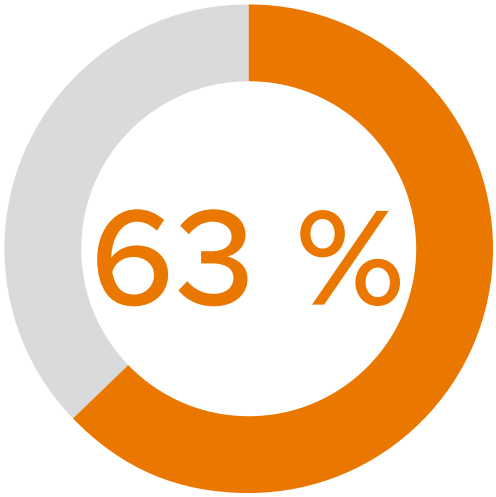
El 98 % ya utilizan una estrategia de seguridad que da prioridad a la nube o planean hacerlo.

La IA es el siguiente paso en la innovación empresarial, pero ¿siguen los problemas de seguridad ralentizando su avance?

Ahora que las empresas buscan la ventaja que les permita ofrecer servicios y experiencias digitales más competitivos al cliente, el paso siguiente en la innovación empresarial es la inteligencia artificial (IA).



Sin embargo, más de la mitad de los participantes de todo el mundo (el 56 %) coinciden en que los problemas de seguridad les impiden adoptar aplicaciones basadas en la IA y el aprendizaje automático para mejorar estos servicios.



El 63 % de los participantes coinciden en que su capacidad para innovar depende de poder desarrollar aplicaciones y ofrecérselas a empleados y clientes con mayor seguridad.

La IA es el siguiente paso en la innovación empresarial, pero ¿siguen los problemas de seguridad ralentizando su avance?

A muchos participantes les preocupa no poder aprovechar las ventajas de la transformación digital.

El 57 %

coinciden en que la complejidad excesiva del sector de las soluciones de seguridad les impide cambiar las políticas de seguridad, aunque son conscientes de que la seguridad de TI actual no funciona.

El 60 %

coinciden en que a los directivos y los responsables sénior les preocupa cada vez más lanzar aplicaciones y servicios al mercado, porque las amenazas están aumentando y por los daños que causan las vulneraciones de datos y los ataques.

El 62 %

coinciden en que les gustaría emplear más IA y aprendizaje automático en las aplicaciones, con el fin de mejorar la seguridad y los servicios.

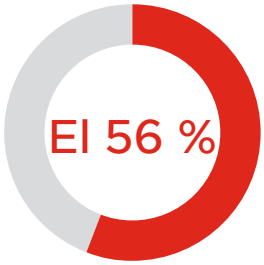
¿Es posible que proteger la marca y la reputación motive acelerar los cambios?

La marca y la reputación siguen teniendo una importancia enorme para las empresas, y se pueden perder fácilmente. Sin embargo, las vulneraciones de seguridad tienen un impacto mayor en la reputación que en las finanzas.

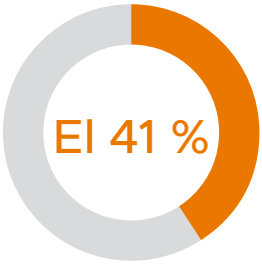
El 75 % de encuestados que sufrieron un ciberataque afirman que causó un impacto negativo en la reputación de la empresa. Este porcentaje era del 70 % en junio de 2020.

El 82 % de los encuestados tuvieron que informar a organismos regulatorios o contratar a una empresa de respuesta a incidentes para lidiar con los daños a su reputación causados por vulneraciones importantes en los últimos 12 meses.

Los participantes tienen opiniones diversas sobre la gravedad de las vulneraciones y no creen que los cambios sean urgentes a pesar del aumento de las amenazas.



temen que sufrirán una vulneración importante durante el próximo año.



han actualizado las políticas y el enfoque de seguridad para mitigar el riesgo.

Conclusiones completas de la encuesta

¿Ha observado un aumento de los ciberataques contra su empresa en los últimos 12 meses? Si es así, ¿en qué medida?

El 76 % de los directores de seguridad de la información encuestados indicaron que observaron un aumento de los ciberataques contra su organización en los últimos 12 meses. La cifra sube hasta el 89 % en el sector de los servicios financieros.

Por regiones, más participantes de Arabia Saudí observaron una mayor cantidad de ataques: el 92 % afirmaron que habían aumentado. En el otro extremo, solo el 64 % de los participantes de Singapur observaron un aumento.

El aumento medio de la cantidad de ataques sufridos fue del 52 %. El 37 % de los participantes indicaron que el aumento fue de entre el 51 % y el 300 %. El mayor aumento medio, del 69 %, se dio en España.

El tamaño de las organizaciones influye en la cantidad de ataques que sufren. De las empresas que tienen entre 251 y 500 empleados, solo el 69 % indicaron que la cantidad de ataques aumentó; de las que tienen entre 5001 y 10 000, un 93 % indicaron un aumento.

La pandemia de COVID-19 ha provocado un aumento en el teletrabajo, en consecuencia, ¿ha cambiado la cantidad total de ciberataques típicos contra su sistema?

El 78 % de los encuestados que sufrieron ciberataques afirmaron que habían observado un aumento en la frecuencia debido a que más empleados trabajan desde casa.

El mayor incremento de los ataques como consecuencia del teletrabajo se observó en Francia, con un 96 %. También en el Reino Unido (86 %) y en Australia (89 %) se observó un aumento. El teletrabajo representó un problema algo menor en Estados Unidos y en los países nórdicos, donde solo un 63 % de los encuestados observaron más ataques.

Una vez más, el tamaño es un factor de riesgo. El 76 % de las organizaciones pequeñas (entre 251 y 500 empleados) indican que el teletrabajo dio lugar a una mayor cantidad de ataques, pero la cifra es del 89 % en organizaciones que tienen entre 5001 y 10 000 empleados.

En los últimos 12 meses, ¿la sofisticación de los ciberataques contra su empresa ha aumentado o disminuido?

Al hablar de la sofisticación de los ataques, **el 79 % de los directores de seguridad de la información que sufrieron un ciberataque han observado que los ataques son más sofisticados.** Esta cifra es muy parecida al 80 % que afirmaron lo mismo en el informe sobre seguridad de junio de 2020. El 49 % afirman que los ataques son bastante o mucho más sofisticados.

Los directores de seguridad de la información encuestados en Francia tienen mayores probabilidades de ver un aumento en la sofisticación; el 89 % afirmaron que los ataques son más complejos. En Italia, la cifra es de solo el 66 %.

Los adversarios dirigen sus tácticas, técnicas y procedimientos (TTP) más sofisticados contra las organizaciones de gran tamaño. De las empresas que tienen entre 5001 y 10 000 empleados y que sufrieron un ciberataque, un 90 % observaron un aumento en el nivel de sofisticación, mientras que solo el 78 % de las organizaciones que tienen entre 251 y 500 empleados observaron lo mismo. Esto refleja el hecho de que, cuanto mayor es una organización, mayor es el volumen y el valor de sus datos, y mayor es la probabilidad de que los ciberdelincuentes obtengan un beneficio económico.

> El 79 % de los directores de seguridad de la información que sufrieron un ciberataque han observado que los ataques son más sofisticados.

¿Cuál ha sido el tipo de ciberataque más prolífico (es decir, el más frecuente) que ha sufrido su empresa en los últimos 12 meses?

Los ataques basados en la nube son los que se han sufrido con mayor frecuencia, pero la proporción de ataques que representan se ha reducido casi a la mitad en los últimos 12 meses, del 18 % al 10 %. Su lugar lo ocupan ahora los ataques de programas de secuestro, que han aumentado respecto a junio de 2020 y representan el 9 % de los ataques, en lugar del 4,5 % que representaban en nuestro informe sobre seguridad anterior. Este dato coincide con lo que ha constatado VMware Threat Analysis Unit™, que observó un aumento de los programas de secuestro del 900 % en la primera mitad de 2020 y destaca las tácticas de extorsión doble que se hicieron famosas el mismo año.

Los ataques de programas de secuestro fueron el tipo de ataque más habitual en Alemania, Francia, Estados Unidos, Reino Unido, los países nórdicos y Japón.

Los ataques a aplicaciones de terceros ocuparon el tercer lugar y representaron el 9 % de los ataques. Representaron el 15 % en los Países Bajos y fueron el tipo de ataque más habitual en Canadá y Australia.

¿Con qué frecuencia ha logrado un ciberataque vulnerar su empresa en los últimos 12 meses?

De las organizaciones que participaron en el estudio, más de ocho de cada diez sufrieron una vulneración en el último año. La cifra ha descendido desde el 94 % que notificaron una vulneración en junio de 2020.

La cifra media oculta importantes diferencias regionales. El 97 % de las organizaciones francesas y el 93 % de las del Reino de Arabia Saudí indicaron que habían sufrido una vulneración. En el otro extremo, solo el 66 % de los encuestados de Singapur y el 69 % de los del Reino Unido sufrieron vulneraciones.

Por lo general, los que sufrieron alguna vulneración, tuvieron una mayor cantidad de estas.

> De las organizaciones que participaron en el estudio, más de ocho de cada diez sufrieron una vulneración en el último año.

De media, los directores de seguridad de la información indican que tuvieron 2,35 vulneraciones el año pasado, frente a las 2,17 de junio de 2020. El 59 % afirmaron que tuvieron una sola vulneración, pero es preocupante que el 14 % tuvieron al menos cinco vulneraciones.

La mayor cifra media de vulneraciones se dio en Estados Unidos, con 3,44, y la menor se observó en España, con 1,6 vulneraciones.

¿Cuál fue la principal causa de las vulneraciones?

La primera causa de las vulneraciones son las aplicaciones de terceros, que representan el 14 % de los incidentes. A continuación están los programas de secuestro y la tecnología de seguridad anticuada, ambas causas con un porcentaje algo menor del 14 %.

El problema de las aplicaciones de terceros destaca en los Países Bajos, donde el 36 % de las organizaciones lo nombran como la causa más común de las vulneraciones. En cuanto a sector vertical, el 16 % de los encuestados de la administración pública y el 21 % de las empresas de comunicación y entretenimiento indicaron que las aplicaciones de terceros fueron la principal causa de las vulneraciones.

Los programas de secuestro son la principal causa de vulneraciones en Francia, Alemania, los países nórdicos, Australia y Japón.

El sector sanitario es la principal víctima de los programas de secuestro. Casi una quinta parte de los encuestados (el 19 %) de este sector indican que son la primera causa de las vulneraciones.

La seguridad anticuada es el problema más grave para el 19 % de los encuestados de los sectores de fabricación y automoción.

¿Qué porcentaje de las vulneraciones debidas a ciberataques sufridas durante los últimos 12 meses cree que constituyeron una vulneración importante (es decir, tuvo que notificarlas a los organismos regulatorios, recurrir a un equipo de respuesta a incidentes, etc.)?

Las vulneraciones, cuando suceden, son un problema grave. **La mayoría de los encuestados, el 82 %, tuvieron que comunicarlas a los organismos regulatorios o recurrir a un equipo de respuesta a incidentes para recuperarse de lo problemas causados.**

> La mayoría de los encuestados, el 82 %, tuvieron que comunicarlas a los organismos regulatorios o recurrir a un equipo de respuesta a incidentes para recuperarse de lo problemas causados.

Los mayores porcentajes de vulneraciones que se consideraron importantes se obtuvieron en el Reino de Arabia Saudí (94 %), España (92 %) y Estados Unidos (90 %). Los resultados fueron mejores en Singapur, donde solo el 68 % de los encuestados informaron de vulneraciones importantes.

¿Cómo repercutieron estas vulneraciones en la economía y la reputación de la empresa?

Menos de la cuarta parte (24 %) de los encuestados que sufrieron un ciberataque indicaron que sufrieron un impacto económico negativo como consecuencia de una vulneración de datos en su organización. La cifra representa un descenso respecto al 30 % que dieron la misma respuesta en junio de 2020. El porcentaje de los que no observaron ningún efecto económico negativo descendió del 56 % al 51 %. Hubo un aumento considerable de los que no saben cuáles fueron los efectos económicos de las vulneraciones. El 20 % indicaron que no lo sabían, frente al 9 % de junio de 2020.

También en este sentido hubo grandes diferencias regionales. Los efectos económicos negativos de las vulneraciones se hicieron notar más en los Emiratos Árabes Unidos, con un 47 % de los encuestados, y en los Países Bajos, con un 40 %. En el extremo opuesto están Canadá, Italia y Reino Unido, donde un 6 %, un 9 % y un 10 %, respectivamente, indicaron que sus empresas habían sufrido efectos económicos adversos como consecuencia de una vulneración.

Las empresas de servicios profesionales tienen una mayor probabilidad de sufrir repercusiones económicas debidas a una vulneración: el 32 % indicaron que han tenido pérdidas. Además, el 83 % de este sector indicaron también que su reputación se vio afectada.

En general, los efectos en la reputación de la marca fueron mayores. Tres cuartas partes de los encuestados indicaron que su marca se había visto afectada negativamente por una vulneración de datos, un porcentaje sube hasta el 89 % en Japón y el 83 % en Francia y Singapur.

Solo el 19 % afirmaron no haber sufrido ningún efecto negativo sobre su reputación cuando se produjo una vulneración, un descenso desde casi la cuarta parte que afirmó lo mismo en 2020.

¿En qué medida le preocupan las vulneraciones importantes que opina que sufrirá su organización en los próximos 12 meses?

Las posibles vulneraciones importantes que pueden ocurrir en el próximo año generan una preocupación considerable. Más de la mitad de los participantes (el 56 %) sienten mucho o cierto temor a que su organización sea víctima de una vulneración. La cifra sube hasta el 74 % en Francia, mientras que la más baja se observa en los Países Bajos, con un 37 %.

Los servicios financieros y el comercio minorista son los sectores en los que la preocupación es mayor. El 67 % de los encuestados de estos sectores indican que temen una vulneración importante. Solo la mitad de las organizaciones de la administración pública y del sector sanitario comparten esta preocupación.

¿Está tomando medidas para abordar la probabilidad de sufrir una vulneración? ¿Cuáles?

Al hablar de sus planes para mitigar el riesgo de vulneraciones, los encuestados dieron prioridad a simplificar y consolidar las soluciones de seguridad, así como a adoptar un enfoque de seguridad intrínseca. También dieron importancia a actualizar la tecnología y las políticas, y a asignar recursos económicos al problema.

El 43 % de los encuestados afirmaron que planean **integrar una mayor seguridad en la infraestructura y las aplicaciones, y reducir la cantidad de soluciones puntuales**. La cifra sube hasta el 48 % en los sectores del comercio minorista y de la alimentación.

Más de la mitad de los participantes de Italia, Alemania, Singapur y Japón planean adoptar la seguridad intrínseca y reducir la cantidad de soluciones puntuales. Este enfoque no está tan extendido en los Países Bajos (32 %), Canadá (34 %) y los Emiratos Árabes Unidos (37 %).

El 42 % afirmaron que han **actualizado la tecnología de seguridad para mitigar el riesgo**. Los encuestados de los sectores de viajes y transporte son lo que tienen más probabilidades de haber adoptado este enfoque (54 %).

Las actualizaciones de tecnología son más habituales en Singapur (51 %), Japón (50 %) y Australia (48 %). Los participantes con menor probabilidad de adoptar este enfoque son los de Canadá (30 %), los Emiratos Árabes Unidos (33 %) y España (35 %).

El 41 % afirmaron que han **actualizado las políticas de seguridad para mitigar el riesgo**, una táctica importante a la vista de los grandes cambios en el panorama de la seguridad durante el último año. Las empresas de comunicación y entretenimiento son las que más han adoptado esta táctica, con un 44 %.

Los países con mayor probabilidad de actualizar las políticas de seguridad para gestionar el riesgo de vulneración son Japón (50 %), los países nórdicos (49 %) y Alemania (47 %).

El 40 % **modificaron la seguridad para mitigar el riesgo**, y el 39 % **aumentaron el presupuesto de seguridad**. Los sectores del comercio minorista (44 %), sanitario (42 %) y de servicios financieros (41 %) son en los que con mayor probabilidad se aumentarán los presupuestos.

Los encuestados de Japón (48 %) son los que con mayor probabilidad aumentarán los presupuestos, y los de Italia (32 %) son los que con menor probabilidad lo harán.

Es interesante ver que las organizaciones dan más importancia a la estrategia que a sencillamente asignar más recursos económicos, y que aumentar los presupuestos se considera menos prioritario en general.

¿En qué medida está de acuerdo con las siguientes afirmaciones en relación con el desarrollo y el uso de aplicaciones en su organización?

Cuando se les preguntó por el cambio en el enfoque de los desafíos de seguridad en lo relativo al desarrollo y uso de aplicaciones en la organización, los encuestados ofrecieron información sobre los problemas a los que se enfrentan.

La visibilidad es una preocupación clara. El 63 % coinciden en que **necesitan una mayor visibilidad de los datos y las aplicaciones para prevenir ataques**. La cifra sube hasta el 73 % en los sectores de **viajes y transporte** y de **servicios públicos**. Es una preocupación importante en Francia, donde el 84 % de los encuestados se mostraron de acuerdo o totalmente de acuerdo.

El 61 % de los encuestados de todo el mundo se mostraron de acuerdo en que los cambios en el panorama de los ataques que ha supuesto la COVID-19 exigen replantearse la seguridad. Coinciden en que es **necesario cambiar su percepción de la seguridad ahora que la superficie de ataque se ha expandido**. También en este ámbito es más probable que los encuestados de los sectores de **viajes y transporte** y de **servicios públicos** compartan esta opinión.

Casi dos tercios (63 %) se mostraron de acuerdo en que **necesitan una mejor seguridad contextual para hacer un seguimiento de los datos y la seguridad a lo largo de su ciclo de vida**. Esto indica la prevalencia de entornos en los que la seguridad suele ser reactiva y centrarse en las amenazas. Los directores de seguridad de la información admiten que los entornos dinámicos exigen un enfoque centrado en el contexto.

Los directores de seguridad de la información encuestados entienden perfectamente que la seguridad de las aplicaciones es esencial para las empresas. El 63 % coinciden en que su **capacidad para innovar como empresa depende de poder desarrollar aplicaciones, gestionarlas y ofrecérselas a empleados y clientes con mayor seguridad**. No resulta sorprendente que esta percepción esté más extendida en sectores en los que hay contacto directo con los clientes. El 74 % de los encuestados del sector del comercio minorista y el 75 % de los del sector de viajes y transporte están de acuerdo con esta afirmación.

El 62 % de los encuestados **creen que pueden lanzar aplicaciones nuevas al mercado con confianza, porque saben que serán seguras**. Los encuestados de los Emiratos Árabes Unidos y de Arabia Saudí son los que sienten más confianza al lanzar aplicaciones al mercado, con el 82 % y el 83 % de acuerdo, respectivamente. Por su parte, los directores de seguridad de la información son los que sienten menos confianza: solo el 39 % afirman sentir confianza, y el 23 % afirman no sentir confianza en poder lanzar aplicaciones seguras.

Cuando pedimos a los encuestados su opinión sobre la IA en el desarrollo de aplicaciones seguras obtuvimos respuestas dispares. El 56 % coinciden en que los **problemas de seguridad les impiden adoptar aplicaciones basadas en la IA y el aprendizaje automático para mejorar los servicios**, pero el 62 % indicaron **que les gustaría emplear más IA y aprendizaje automático en las aplicaciones, con el fin de mejorar la seguridad y los servicios**.

Más de la mitad de los encuestados (57 %) coinciden en que **la complejidad excesiva del mercado de las soluciones de seguridad les impide cambiar las políticas de seguridad, aunque son conscientes de que la seguridad de TI actual no funciona**. Este dato sugiere que los proveedores deben simplificar sus productos con un enfoque unificado.

Por último, el 60 % coincidieron en que los directivos se interesan por la seguridad de las aplicaciones, y que a los **directivos y los responsables sénior les preocupa cada vez más lanzar aplicaciones y servicios al mercado, debido al aumento en amenazas y por los daños que causan las vulneraciones de datos y los ataques**. Los consejos de administración con mayor probabilidad de mostrar preocupación son los de las empresas de servicios públicos: tres cuartas partes de sus directores de seguridad de la información afirman que los consejos muestran preocupación. A continuación vuelven a estar los sectores que tienen contacto directo con los clientes: el comercio minorista y viajes y transporte.

Los consejos de administración con mayor probabilidad de mostrarse preocupados por los lanzamientos al mercado de aplicaciones y servicios son los de Arabia Saudí y los Emiratos Árabes Unidos, con un 83 % y un 74 %, respectivamente.

¿Cuál cree que es el punto más vulnerable del procesamiento de los datos en su infraestructura de seguridad? ¿Ha cambiado en los últimos 12 meses?

Las aplicaciones ocupan el primer lugar en este aspecto, que lleva cierto tiempo siendo una preocupación clara. Cabe destacar que las cargas de trabajo se perciben cada vez más como una vulnerabilidad.

35 % Aplicaciones

El 21 % lo indican ahora y lo indicaban hace 12 meses; el 14 % lo indican ahora y no lo indicaban hace 12 meses.

21 % Red

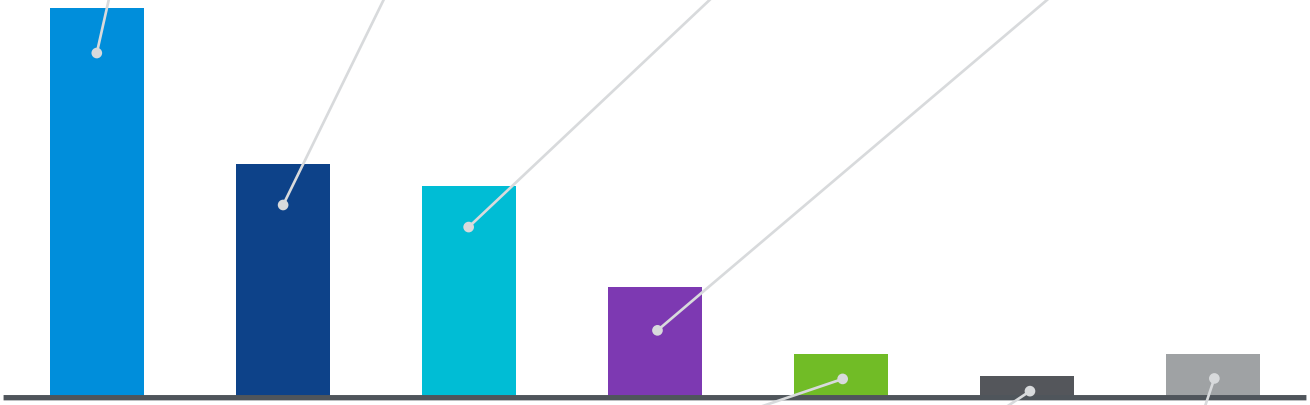
El 13 % lo indican ahora y lo indicaban hace 12 meses; el 8 % lo indican ahora y no lo indicaban hace 12 meses.

19 % Cargas de trabajo

El 4 % lo indican ahora y lo indicaban hace 12 meses; el 15 % lo indican ahora y no lo indicaban hace 12 meses.

10 % Terminales

El 6 % lo indican ahora y lo indicaban hace 12 meses; el 4 % lo indican ahora y no lo indicaban hace 12 meses.



4 % Nube

El 2,5 % lo indican ahora y lo indicaban hace 12 meses; el 1,9 % lo indican ahora y no lo indicaban hace 12 meses.

2 % Contenedores

El 1,7 % lo indican ahora y lo indicaban hace 12 meses; el 0,6 % lo indican ahora y no lo indicaban hace 12 meses.

4 % Desconocido

¿Cómo han superado las organizaciones los desafíos del cambio al teletrabajo?

Pedimos a los directores de seguridad de la información encuestados que calificaran el éxito de la transición hacia el teletrabajo. También les preguntamos si un enfoque que dé prioridad a la seguridad hubiera contribuido a una transición más efectiva.

El 54 % se muestran de acuerdo en que han podido adoptar el teletrabajo y en que la seguridad no ha supuesto un obstáculo. Esto pone de manifiesto que el trabajo de los equipos de seguridad ha sido un componente esencial de las operaciones. Las variaciones regionales son considerables. Solo el 33 % de los encuestados del Reino Unido coinciden en que adoptaron el teletrabajo sin problemas y el 22 % se muestran en desacuerdo. Por el contrario, el 76 % de los directores de seguridad de la información encuestados en Francia apenas tuvieron problemas.

Los participantes admiten que siempre se puede mejorar, y el 60 % se muestran de acuerdo en que un enfoque que dé prioridad a la seguridad hubiera facilitado la transición hacia el teletrabajo y habría ayudado a mantener la productividad. Este hecho se confirmó en un estudio de VMware anterior, que indicó que la imposibilidad de implementar la autenticación multifactor fue la mayor preocupación de los profesionales de TI como consecuencia de la transición hacia el teletrabajo. Ahora que el perfil de la seguridad ha cobrado mayor importancia, a los directores de seguridad de la información debería resultarles más fácil conseguir que los consejos de administración apoyen un enfoque que dé prioridad a la seguridad.

¿Utiliza o piensa utilizar una estrategia de seguridad que dé prioridad a la nube?

> El 98 % ya utilizan o planean utilizar un enfoque que dé prioridad a la nube para proteger su organización.

Casi todos los encuestados indicaron que piensan adoptar una estrategia de seguridad que dé prioridad a la nube con toda probabilidad, aunque no sea inmediatamente. **El 98 % ya utilizan o planean utilizar un enfoque que dé prioridad a la nube para proteger su organización.**

El 100 % de los encuestados de Estados Unidos van a adoptar la nube, frente al relativamente bajo porcentaje del 87 % de los que piensan hacerlo en los Países Bajos.

El 46 % afirman que llevan más de un año utilizando un enfoque que da prioridad a la nube, y el 30 % indican que llevan haciéndolo menos de 12 meses. El 11 % piensan dar prioridad a la nube durante el año próximo, y otro 11 % piensan hacerlo más adelante.

La mayor priorización de la nube se constata en Australia, donde el 63 % de los encuestados llevan más de 12 meses con este tipo de enfoque. Canadá está en el extremo opuesto, con solo un 25 %.

Aspectos y pasos clave

Nuestro cuarto informe sobre seguridad global indica que los profesionales sénior de la ciberseguridad y las organizaciones en las que trabajan siguen enfrentándose a muchas y muy sofisticadas amenazas. El problema se agrava como consecuencia de la transición hacia el trabajo geográficamente disperso. Asimismo, a pesar de que muchas organizaciones han conseguido adoptar el teletrabajo, los directores de seguridad de la información admiten que un enfoque que dé prioridad a la seguridad hubiera facilitado la transición.

No cabe duda de que la COVID-19 alteró el entorno de la ciberseguridad enormemente y seguirá influyendo en las estrategias de seguridad. Por su parte, el sector de la ciberseguridad debe centrarse en proporcionar soluciones que reduzcan la complejidad operativa y protejan eficazmente los entornos de teletrabajo que pasarán a ser la norma en casi todas las organizaciones.

El análisis de las respuestas a la encuesta revela áreas importantes a las que la ciberseguridad debe prestar atención durante el próximo año.

Priorizar la mejora de la visibilidad

La rápida transición hacia el teletrabajo ha creado un problema de visibilidad en las organizaciones. El volumen de los ataques es difícil de precisar, ya que los defensores no tienen visibilidad de los recovecos del ecosistema corporativo que han surgido al incorporar los dispositivos móviles personales y las redes domésticas. Si a esto le añadimos los desafíos que supone supervisar aplicaciones de terceros y proveedores, la cantidad de puntos ciegos se dispara.

En pocas palabras, los defensores no saben cuánto ignoran y, como consecuencia, las empresas se encuentran en una situación vulnerable. Dada la escasa información contextual de la que disponen, los defensores están en desventaja a la hora de proteger una superficie de ataque ampliada. Una de las prioridades de las organizaciones debe ser mejorar la visibilidad de todos los terminales y cargas de trabajo para proteger el entorno del teletrabajo. Una sólida información sobre el contexto de las amenazas ayudará a los defensores a priorizar y corregir los riesgos con confianza.

Responder ante el resurgimiento de los programas de secuestro

Los ciberataques son cada vez más sofisticados, y los programas de secuestro no son una excepción. Los atacantes acceden a las redes sin ser detectados, exfiltran datos y crean entradas ocultas antes de pedir rescate o beneficiarse directamente de los datos robados. Para no ser víctimas de ataques continuos, las organizaciones deber combinar la protección contra programas de secuestro avanzada y las soluciones posteriores a los ataques que detecten la constante presencia de adversarios en sus entornos.

Continuar buscando soluciones a una tecnología de seguridad heredada poco efectiva y a los puntos débiles de los procesos

La seguridad anticuada y los puntos débiles de los procesos siguen representando riesgos importantes para las organizaciones, y la adopción del teletrabajo ha agravado el problema. A medida que salimos de la fase de respuesta inmediata y empezamos a ver el panorama del futuro a largo plazo, las organizaciones deben identificar los cambios esenciales necesarios en los procesos y la tecnología para proporcionar un modelo de teletrabajo o híbrido seguro, con menos riesgos.

Ofrecer la seguridad como un servicio distribuido

En el pasado, los equipos de seguridad protegían los ordenadores de las empresas que los empleados utilizaban en las instalaciones; estos se conectaban a aplicaciones corporativas alojadas en los servidores de un centro de datos propiedad de la empresa. El mundo es ahora más complejo. Los teletrabajadores se conectan a aplicaciones alojadas en una infraestructura cuya gestión, propiedad o control puede estar en manos de terceros. Con tantas nuevas superficies y distintos tipos de entornos que hay que proteger, la seguridad no puede consistir en una serie de productos puntuales y cuellos de botella en la red. Los controles de los terminales y la red se deben proporcionar como un servicio distribuido. Esto quiere decir que se debe ofrecer una seguridad que acompañe a los recursos que protege en todo tipo de entornos.

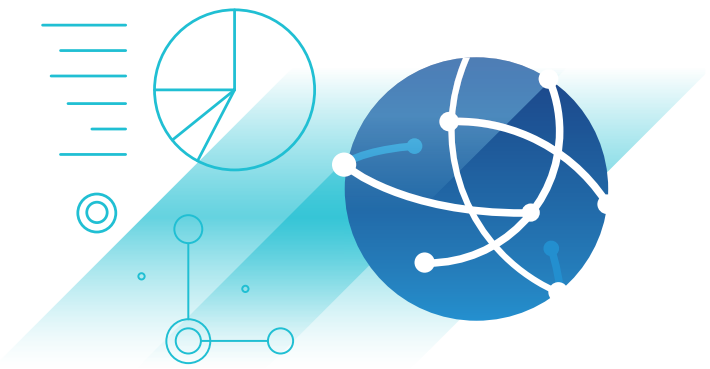
Adoptar un enfoque intrínseco de la seguridad que dé prioridad a la nube

El cambio más profundo que reveló nuestra investigación es la transición hacia una estrategia de seguridad que da prioridad a la nube. Es muy importante destacar la magnitud del cambio que se ha producido en un espacio de tiempo muy breve. Antes de 2020, muy pocos directores de seguridad de la información afirmaban que su estrategia de seguridad daba prioridad a la nube. Es una consecuencia lógica de que las organizaciones hayan tenido que responder a prácticas de trabajo muy geográficamente disperso por culpa de la COVID-19.

Sin embargo, la transición a la nube no es la panacea de la seguridad. No todas las nubes son iguales y las organizaciones de usuarios deben aprobar los controles, ya que, si los adversarios quieren atacar a gran escala, la nube es lugar idóneo para hacerlo. A medida que la transición va tomando impulso, será esencial invertir en la seguridad de la nube pública. Al realizar la transición a la nube pública, se está trasladando a un lugar muy complicado, en el que la seguridad depende de sus propias acciones y de las de los demás. Es posible que pueda proteger sus recursos, pero no controla las acciones de quienes comparten el mismo entorno que usted. Las organizaciones deben priorizar la protección de las cargas de trabajo de nube durante todo el ciclo de vida de la seguridad y mientras dure la gran transición a la nube.

En última instancia, el informe sobre seguridad global de VMware de 2021 revela que el sector está centrado en aprovechar el éxito obtenido durante el último año y en responder a un entorno de amenazas que cambia constantemente. Los directores de seguridad de la información saben muy bien qué camino deben seguir y qué herramientas deben utilizar para poder ir un paso por delante de los atacantes.

Metodología



En diciembre de 2020, VMware encargó la elaboración de una encuesta a la organización de investigación independiente Opinion Matters. Participaron en la encuesta **3542 directores de tecnología, directores de informática y directores de seguridad de la información** de empresas de distintos sectores: financiero, sanitario, administración pública y autoridad local, comercio minorista, fabricación e ingeniería, alimentación, servicios públicos, servicios profesionales, y comunicación y entretenimiento. Es el cuarto informe de seguridad global de VMware y continua lo estudiado en los anteriores, que se elaboraron en febrero de 2019, octubre de 2019 y junio de 2020. Forma parte de un proyecto de investigación internacional que abarca **14 países y regiones:** Australia, Canadá, Arabia Saudí, Oriente Medio, Reino Unido, Francia, Alemania, España, Países Bajos, países nórdicos, Italia, Japón, Singapur y Estados Unidos.

Acerca de VMware

El software de VMware es la base de la infraestructura digital más compleja del mundo. Las soluciones de nube, modernización de aplicaciones, red, seguridad y áreas de trabajo digitales de la empresa ayudan a los clientes a distribuir cualquier aplicación en cualquier nube y dispositivo. VMware es una empresa con sede en Palo Alto (California) y tiene el firme objetivo de servir para una buena causa, desde sus innovadoras tecnologías de vanguardia hasta su repercusión internacional. Para obtener más información, visite vmware.com/es/company.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com
C/ Rafael Botí, 26 - 2.ª planta, 28023 Madrid, España. Tel. +34 914125000 Fax +34 914125001 www.vmware.es