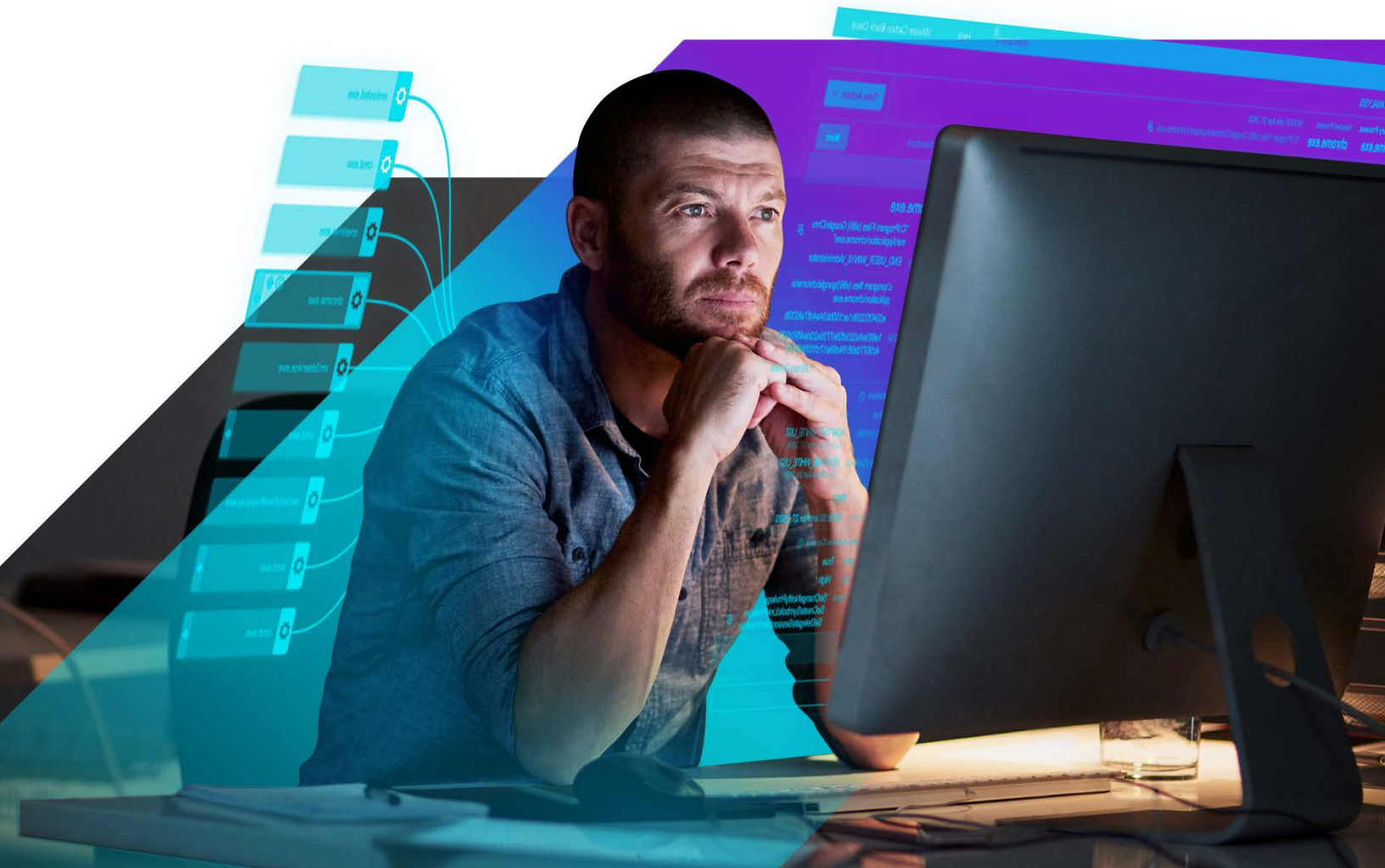
vmware®

España

Informe sobre seguridad en España de VMware

2021



Introducción

Esta investigación se ha llevado a cabo para comprender los desafíos y los problemas a los que se enfrentan las empresas españolas en relación con el auge de los ciberataques. Identifica las tendencias en materia de piratería informática y ataques maliciosos, así como el impacto financiero y para la reputación que han tenido las vulneraciones de seguridad en un año sin precedentes. Además, analiza los planes que tienen las organizaciones para implantar nuevas tecnologías, adoptar una estrategia de seguridad con prioridad en la nube y abordar la complejidad del actual entorno de gestión de la ciberseguridad.

Lea este informe para conocer cómo los profesionales de ciberseguridad están planificando la manera de hacer frente a los desafíos que plantean los espacios de trabajo distribuidos y desarrollar defensas para dotar de seguridad intrínseca a la infraestructura y las operaciones.

Resumen ejecutivo:

Prólogo

PERSPECTIVAS ANTE EL PANORAMA DE CIBERSEGURIDAD EN ESPAÑA

Rick McElroy, Estratega Principal de Ciberseguridad, Unidad de Negocio de Seguridad de VMware

Todo ha cambiado…, y al mismo tiempo, todo sigue igual.

Los profesionales de ciberseguridad que han contribuido a la segunda edición de nuestro «Informe sobre seguridad en España» se encuentran en una posición muy distinta a la que tenían cuando respondieron a la encuesta de 2020. Tras un año en el que se ha producido la mayor y más rápida transformación de los patrones 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 han avanzado rápidamente a medida que la superficie sujeta a potenciales ciberataques se ampliaba a salones, cocinas, redes domésticas y dispositivos personales. El teletrabajador se comporta de manera muy diferente al que está en una oficina, pues accede a la red a horas imprevisibles mientras intenta mantener la productividad a la vez que cuida de su familia y cumple las restricciones impuestas por las autoridades. Por todo ello, el tráfico de la red ha cambiado de forma irreconocible. Los defensores deben adaptar los sistemas de monitorización y los puntos de activación para evitar que los ciberdelincuentes utilicen patrones atípicos para enmascarar sus intentos de acceso.

En un contexto tan cambiante como el que vivimos, hay cosas que se mantienen igual: un sector que no se ha visto afectado por la COVID-19 es el de la ciberdelincuencia.

La frecuencia de los ataques es elevada, su sofisticación no deja de aumentar y el resultado inevitable son las vulneraciones de seguridad.

Tres cuartas partes (75 %) de los 251 encuestados señalan que el número de ataques a los que se han enfrentado ha aumentado en el último año y, de ellos, el 61,5 % afirma que han aumentado porque hay más empleados que trabajan desde casa. El 83 % dice que los ataques han aumentado en sofisticación, lo que supone un ligero descenso respecto a los niveles encontrados en el informe de junio de 2020 (86 %).

Los directores de seguridad de la información no pueden llegar a todos los rincones

El volumen de ciberataques ha crecido, pero las empresas aún no tienen una imagen completa debido a la rápida implantación del teletrabajo. El comportamiento errático de los empleados y el uso de dispositivos personales y de la red doméstica reducen la visibilidad, lo que crea puntos ciegos y rincones oscuros en los no se detectan los ataques. En consecuencia:

61,5 %

afirma que los ataques han aumentado debido al teletrabajo.

1,6

Se producen 1,6 vulneraciones de media por organización y año.

92 %

afirma haber sufrido una infracción de seguridad importante.

¿Cuál es el resultado? El número de vulneraciones de seguridad ha aumentado, y los encuestados que han sufrido un ciberataque comunican **1,6 vulneraciones de media al año**. No se trata de incidentes menores; en nueve de cada diez casos se trató de un incidente grave que requirió la notificación a los reguladores o la intervención de un equipo de respuesta.

Sin duda, los equipos de seguridad están sometidos a grandes presiones y no hay margen para la complacencia: el 49 % de los directores de seguridad de la información encuestados temen que su organización experimente una vulneración de seguridad importante el próximo año.

El 49 % de los directores de seguridad de la información temen una infracción grave el próximo año.

Tecnología de seguridad obsoleta, debilidad de los procesos y aplicaciones de terceros, principales causas de las infracciones

Cuando se pregunta por las causas de las vulneraciones de seguridad, los tres vectores principales arrojan una imagen de amenazas externas y debilidades internas. La tecnología de seguridad obsoleta es la causa más común, en el origen del 18 % de las vulneraciones, seguida de cerca por la debilidad de los procesos y, por último, las aplicaciones de terceros.

La acelerada transición al trabajo desde cualquier lugar ha dejado al descubierto a las organizaciones que habían descuidado la seguridad y no habían implantado una autenticación multifactorial. De este modo, han pagado el precio por emplear tecnologías y procesos obsoletos.

Además de estas amenazas, el auge de los programas de secuestro ha añadido tensiones no deseadas. Las campañas en varias etapas que conllevan penetración, persistencia, robo de datos y extorsión aumentan la presión, ya que los atacantes aprovechan los cambios radicales a los que se enfrentan los teletrabajadores. En la mayoría de los ataques de programas de secuestro, el correo electrónico sigue siendo el vector de ataque más común para conseguir el acceso inicial.

Reaparición de los programas de secuestro

Los programas de secuestro vuelven a ser una de las principales causas de las vulneraciones, pues los atacantes lanzan sofisticadas y lucrativas campañas en varias fases.

7,5 % **de todas las vulneraciones de seguridad se deben a los programas de secuestro.**

Temor ante el desarrollo y el uso de aplicaciones

Las aplicaciones de terceros son una de las principales causas de las vulneraciones de seguridad, según los directores de seguridad de la información a los que hemos encuestado. Por ello, es lógico que los equipos de seguridad se centren en perfeccionar un procedimiento para su uso y desarrollo.

Dos quintas partes de los encuestados están de acuerdo[1] en que necesitan una mayor visibilidad de los datos y las aplicaciones para prevenir los ataques, y un número similar se muestra de acuerdo en la necesidad de mejorar la seguridad contextual para hacer un seguimiento de la seguridad de los datos a lo largo del ciclo de vida de la aplicación. Se reconoce el impacto que ha tenido la COVID-19, ya que dos de cada cinco encuestados están de acuerdo en la necesidad de cambiar su forma de ver la seguridad, debido a la ampliación de la superficie de ataque.

Las aplicaciones también encabezan la lista como el punto más vulnerable en el recorrido de los datos, pero no son en absoluto el único motivo de preocupación.

Cada vez se aprecia más que las cargas de trabajo son fuente de vulnerabilidad.

El 11 % de los encuestados afirman que las cargas de trabajo son el punto más vulnerable en el recorrido de los datos en su organización, algo que no ocurría hace 12 meses.

[1] «Está de acuerdo» es la combinación de las opciones «Está totalmente de acuerdo» y «Está algo de acuerdo».

Otro 6 % señala que han sido el punto más vulnerable durante más de 12 meses. Los equipos reconocen que los antivirus tradicionales no protegen las cargas de trabajo de los servidores y que los errores de configuración son un riesgo de vulneración importante. Esto suele deberse a una carencia en los conocimientos de los equipos de seguridad y los de infraestructura, pues los equipos de seguridad desconocen cuál es el comportamiento previsto de las cargas de trabajo de producción, mientras que a los equipos de infraestructura les falta experiencia para reconocer el comportamiento de los atacantes. Prevemos que este año las organizaciones tratarán de subsanar estas deficiencias y reforzar las defensas de las cargas de trabajo en la nube.

En cuanto a la nube, nuestra investigación revela que se está produciendo un cambio inexorable. Casi todos los directores de seguridad de la información encuestados siguen una estrategia de seguridad con prioridad en la nube o tienen previsto hacerlo en breve. Se trata de una evolución importante y muestra que las organizaciones están acelerando su hoja de ruta en materia de seguridad en la nube en respuesta a los retos de la COVID-19. Puede que se trate de un proceso que ya habían puesto en marcha, pero ahora están pisando el acelerador ante la imperiosa necesidad de tener seguridad completa con prioridad en la nube en un mundo que también da prioridad a la nube.

Esperamos que este segundo **Informe sobre seguridad en España de VMware** le resulte elocuente e informativo.

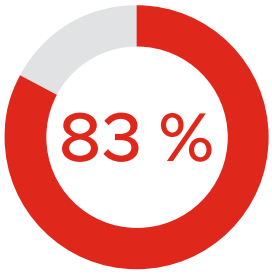
Principales conclusiones

La frecuencia de los ataques y el riesgo de vulneración siguen siendo elevados

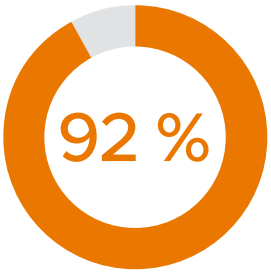
La frecuencia de los ataques es elevada, su sofisticación no deja de aumentar y el resultado inevitable son las vulneraciones de seguridad.

75 % de los encuestados afirman que el volumen de ataques ha aumentado en los doce últimos meses, con una media del 69 % en todas las organizaciones afectadas.

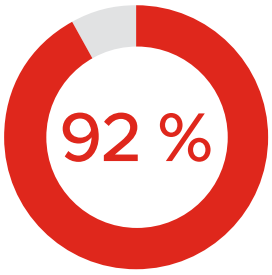
61,5 % de los que han sufrido un ciberataque creen que las vulneraciones aumentaron debido a que hay más personas que trabajan desde casa.



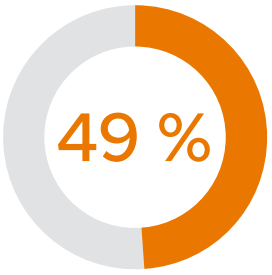
de los que han sufrido un ciberataque afirman que los ataques son más sofisticados.



ha sufrido una vulneración de seguridad en los doce últimos meses, con una media de 1,6 vulneraciones durante ese periodo.



cree que las vulneraciones que han sufrido son importantes.



teme que se produzca una vulneración importante en los doce próximos meses.

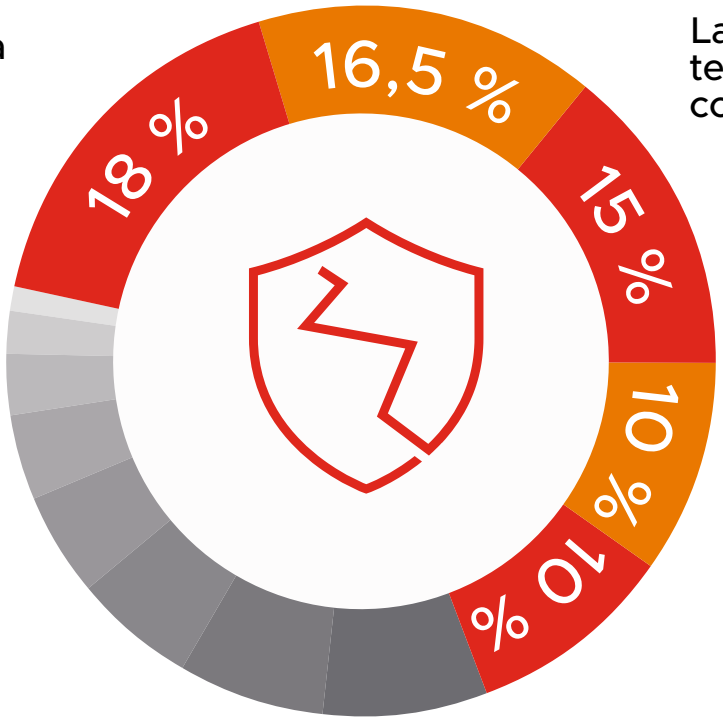
La tecnología obsoleta, la debilidad de los procesos y las aplicaciones de terceros son las principales preocupaciones de los directores de seguridad de la información

Los tres principales vectores que causan las vulneraciones arrojan una imagen completa de las amenazas externas y las debilidades internas.

Principales causas de vulneración entre quienes han sufrido un ciberataque:

La tecnología de seguridad obsoleta encabeza la tabla, con un 18 %.

La debilidad de los procesos ocupa la segunda posición, con un 16,5 %.



Las aplicaciones de terceros la tercera, con un 15 %.

Acceso mediante organizaciones más pequeñas, o «island hopping» (10 %) y vulnerabilidad del sistema operativo (10 %) completan los cinco primeros puestos.

Las aplicaciones y las cargas de trabajo también encabezan la lista como puntos más vulnerables en el recorrido de los datos, pero no son en absoluto el único motivo de preocupación.

La ampliación de la superficie de ataque obliga a los responsables a replantearse su metodología de seguridad tradicional

Un aspecto positivo es que se reconoce la necesidad de un cambio fundamental en la seguridad en una era digital altamente conectada en la que se presta apoyo al teletrabajo:

40 % está de acuerdo en que es necesario cambiar su concepto de seguridad, ya que se ha ampliado la superficie de ataque.

40 % se muestra de acuerdo en la necesidad de mejorar la seguridad contextual para poder hacer un seguimiento de los datos a lo largo del ciclo de vida.

41 % está de acuerdo en que necesita una mejor visibilidad de los datos y las aplicaciones para anticiparse a los ataques.

La simplificación, consolidación y necesidad de dar prioridad a la nube están en el orden del día para 2021

Los directores de seguridad de la información encuestados parecen estar siguiendo un proceso de consolidación tecnológica y de adopción de una metodología de seguridad más intrínseca, y el 35,5 % afirma estar aumentando su presupuesto de seguridad para lograr estos objetivos.

38 % está aumentando la seguridad de su infraestructura y sus aplicaciones y reduciendo el número de soluciones puntuales.

38 % ha adaptado su seguridad para mitigar los riesgos.

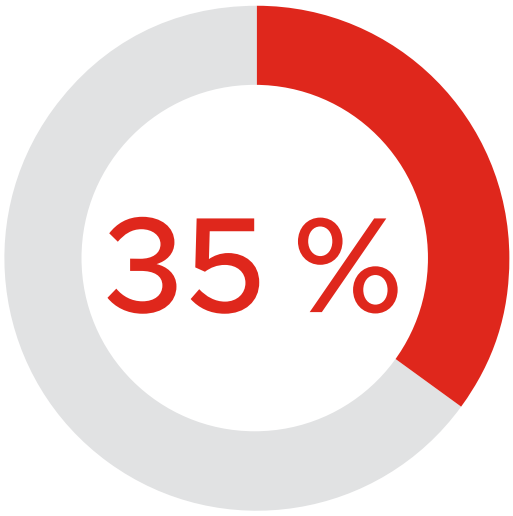
35 % ha actualizado su tecnología de seguridad para mitigar los riesgos.

31 % ha actualizado su política y metodología de seguridad para mitigar los riesgos.

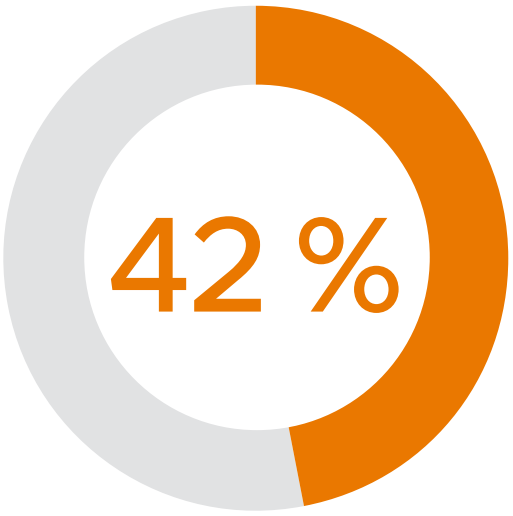
98 % ha cambiado o tiene previsto cambiar a una estrategia de seguridad con prioridad en la nube.

La inteligencia artificial es la nueva frontera de la innovación empresarial. Pero, ¿están frenando el progreso las preocupaciones por la seguridad?

La nueva frontera de la innovación empresarial es la inteligencia artificial, ya que las empresas quieren tomar la delantera para impulsar servicios a clientes y experiencias digitales más competitivas.

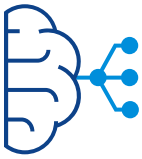


Sin embargo, más de un tercio de los encuestados (35 %) está de acuerdo en que las preocupaciones por la seguridad les impiden adoptar aplicaciones basadas en inteligencia artificial y aprendizaje automático para mejorar dichos servicios.



Y el 42 % de los encuestados están de acuerdo en que su capacidad de innovación depende de la creación de aplicaciones y de ponerlas a disposición de empleados y clientes de forma más segura.

La inteligencia artificial es la nueva frontera de la innovación empresarial. Pero, ¿están frenando el progreso las preocupaciones por la seguridad?



Muchos encuestados están preocupados por no poder responder a las oportunidades digitales.

40 % está de acuerdo en que hay demasiada complejidad en el sector de las soluciones de seguridad como para cambiar su política de seguridad, pese a que saben que la seguridad de TI no está funcionando actualmente.

42 % está de acuerdo en que los directivos de la empresa se sienten cada vez más preocupados en la comercialización de nuevas aplicaciones y servicios debido al aumento de las amenazas y los daños que provocan las filtraciones de datos y los ataques.

41 % está de acuerdo en que le gustaría utilizar más inteligencia artificial y aprendizaje automático en sus aplicaciones para mejorar la seguridad y los servicios.

41 % está de acuerdo en que necesita una mayor visibilidad de los datos y las aplicaciones para anticiparse a los ataques.

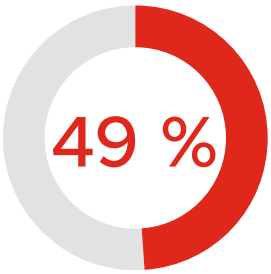
La protección de la marca y la reputación: ¿hace que sea más urgente el cambio?

La marca y la reputación siguen siendo el santo grial de las empresas, pero se pueden perder fácilmente. El impacto de las vulneraciones de seguridad sobre la reputación supera el impacto financiero.

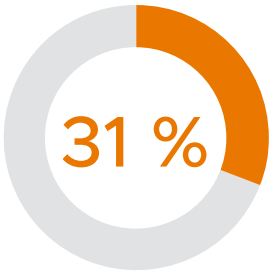
↗ 70 % de quienes sufrieron un ciberataque creen que su reputación se vio afectada negativamente.

↗ 92 % de los encuestados que sufrieron una vulneración de seguridad tuvieron que informar a los reguladores o contratar una empresa que se encargara de la recuperación de incidentes para solucionar los problemas para la reputación que les han causado las vulneraciones graves en los 12 últimos meses.

Los encuestados reconocen de forma muy diversa la gravedad de estas vulneraciones—y la falta de urgencia de cambio, a pesar de que el número de amenazas está creciendo.



teme que se produzca una vulneración importante el próximo año.



ha actualizado su política y metodología de seguridad para mitigar los riesgos.

Conclusiones completas del estudio

¿Se ha producido un incremento de los ciberataques a su empresa en los 12 últimos meses? Si es así, ¿de qué magnitud?

El 75 % de los directores de seguridad de la información encuestados señalan que han sufrido un aumento en el número de ciberataques en su organización en los 12 últimos meses. El aumento medio del volumen de ataques se sitúa en un 69 %, lo que supone un aumento considerable respecto al 41,5 % en junio de 2020.

A los encuestados del sector sanitario les fue mejor que a la media, con un 52 % que informa de un aumento en el volumen de los ataques.

Las organizaciones con plantillas entre 501 y 1000 empleados tuvieron que hacer frente a aumentos significativos, y una de cada cinco señala un incremento de más del 100 % en el volumen de ataques el último año.

Igualmente, los grandes equipos de sistemas informáticos sufrieron más ataques. Los equipos de sistemas informáticos con plantillas entre 41 y 50 empleados experimentaron un aumento en el volumen medio de ataques del 73 %, en comparación con el 65 % entre los equipos con plantillas entre 21 y 30 trabajadores.

¿Ha cambiado el número de ciberataques en general contra su sistema debido al incremento en el número de empleados que trabajan desde casa a causa de la pandemia de la COVID-19?

El 61,5 % de los encuestados que han sufrido ciberataques dicen que ha aumentado la frecuencia debido a que hay más empleados que trabajan desde casa.

Los encuestados del sector sanitario registraron un aumento superior a la media de los ataques debido al teletrabajo. Un 70,5 % manifestó que se había producido este aumento.

Los equipos de TI de 31 a 40 empleados señalan un aumento de los ataques por encima de la media, con un repunte del 64 % en frecuencia.

¿Ha aumentado o disminuido la sofisticación de los ciberataques a su empresa en los 12 últimos meses?

En cuanto a la sofisticación de los ataques, **el 83 % de los directores de seguridad de la información encuestados que han sufrido ciberataques creen que se han vuelto más sofisticados**. Esta cifra coincide en términos generales con el 86 % que declaró un aumento de la sofisticación de los ataques en el informe de junio de 2020.

> El 83 % de los directores de seguridad de la información encuestados creen que los ataques han aumentado en sofisticación.

El 42 % de los encuestados que han sufrido ataques creen que se han vuelto moderadamente más sofisticados, mientras que para el 8 % son significativamente más sofisticados. El crecimiento de la sofisticación de los ataques está por encima de la media en el sector de los servicios financieros, donde el 87 % de los encuestados consideran que los ataques a los que se han enfrentado son más complejos.

¿Cuál ha sido el tipo de ciberataque más frecuente que su empresa ha sufrido en los 12 últimos meses?

El entorno de los ataques en España es diverso. Hay pocos encuestados que experimenten la misma combinación de tipos de ataque y no predomina ningún tipo de ataque en concreto. Esta situación pone de relieve los retos a los que se enfrentan los directores de seguridad de la información españoles: deben crear respuestas estratégicas y tácticas contra una combinación increíblemente variada de vectores y técnicas de ataque.

Los programas maliciosos encabezan la tabla. Es el que ha afectado con mayor frecuencia al 10 % de los encuestados que han sufrido un ciberataque. Le siguen de cerca el vaciado de procesos y los ataques relacionados con la tecnología 5G, con un 8 % de los encuestados cada uno.

Los ataques sin archivos y los ataques a la cadena de suministro representan cada uno el 7 % de los ataques sufridos, seguidos de ataques a Google Drive (basados en la nube) y la piratería en formularios (formjacking), con un 6,5 % cada uno.

¿Cuántas veces ha sufrido su empresa una vulneración por ciberataque en los 12 últimos meses?

Nueve de cada diez directores de seguridad de la información que han participado en nuestro estudio afirman que su organización ha sufrido una vulneración debido a un ciberataque el último año (92 %). Esta cifra supone una bajada respecto al 100 % que declaraba haber sido víctima de una vulneración de seguridad en junio de 2020.

> El 92 % de las organizaciones encuestadas han sufrido una vulneración de seguridad el último año.

El número medio de vulneraciones sufridas por cada organización ha aumentado ligeramente, pasando de 1,52 en junio de 2020 a 1,6 en este informe. El 5 % de los encuestados señalan que su organización ha sufrido una vulneración cinco veces o más.

El sector de los servicios financieros sufrió un porcentaje menor de vulneraciones de media, con un 1,17.

¿Cuál fue la principal causa de estas vulneraciones de seguridad?

El 18 % de los directores de seguridad de la información encuestados que han sufrido un ciberataque se han enfrentado al desagradable descubrimiento de que el uso de tecnología de seguridad anticuada había sido la causante de la vulneración. Para agravar el problema, sus procesos no eran tan sólidos como creían y fueron la causa de la vulneración para el 16,5 %. La presión provocada por la adopción súbita del teletrabajo ha puesto claramente de manifiesto en qué áreas las políticas y las tecnologías no han sido capaces de mantener el ritmo de cambio del entorno.

Sin embargo, no toda la responsabilidad recae en la organización, pues el 15 % de las vulneraciones se originaron en aplicaciones de terceros. Otras causas significativas, aunque en puestos menos destacados, son las siguientes: el 10 % de las vulneraciones se atribuyen al island hopping, el 9,5 % a la vulnerabilidad del sistema operativo y el 7,5 % a los programas de secuestro. Una vez más, esta diversidad pone de manifiesto los numerosos frentes en los que los directores de seguridad de la información españoles tienen que luchar en defensa de su organización.

La debilidad de los procesos es un problema que afecta particularmente a las empresas de servicios financieros: son la causa de más de la quinta parte (23 %) de las vulneraciones. En el sector sanitario, las aplicaciones de terceros son responsables del 20,5 % de los incidentes.

¿Qué porcentaje de las vulneraciones por ciberataques en los 12 últimos meses cree que fueron graves, es decir, que tuvieron que comunicarlas a los reguladores o solicitar la presencia de un equipo de respuesta a incidentes para recuperar el sistema, etc.?

Cuando se produce una vulneración, es un asunto serio. **La mayoría de los encuestados (92 %) tuvo que informar a los reguladores o contratar una empresa de respuesta a incidentes para solucionar los problemas causados por las vulneraciones**.

El 52 % de los encuestados que han sufrido un ciberataque afirman que entre el 21 % y el 30 % de las vulneraciones fueron graves, mientras que para otro 24 % lo fueron entre el 31 % y el 40 % de las vulneraciones.

En la administración pública, el 27 % de los encuestados creen que entre el 31 % y el 40 % de las vulneraciones fueron graves, mientras que para el sector sanitario solo lo fueron el 16 %.

> El 92 % de las organizaciones han sufrido una vulneración de seguridad grave.

¿Cuáles fueron las consecuencias de estas vulneraciones de seguridad desde el punto de vista financiero y para la reputación de su empresa?

Una quinta parte (19,5 %) de los encuestados que han sufrido un ciberataque afirman haber experimentado un impacto financiero negativo debido a una filtración de datos sufrida por su organización. Esta cifra es inferior a la media mundial del 24 %, pero está en línea con el 19 % que dijo haber sufrido un impacto financiero en la encuesta de junio de 2020. El 55 % cree que su reputación no se ha visto afectada.

En general, el efecto sobre la reputación de la marca es mayor. El 35 % de los encuestados que han sufrido un ciberataque creen que su marca se ha visto afectada negativamente por una filtración de datos.

Solo el 22 % dice que no ha sufrido pérdida de reputación por la filtración.

¿En qué medida teme las vulneraciones graves que cree que sufrirá su organización en los 12 próximos meses?

Existe un importante factor de miedo asociado a la posibilidad de que se produzcan vulneraciones importantes el próximo año. Casi la mitad (49 %) tiene mucho o cierto temor a que una vulneración de seguridad afecte a su negocio.

El sector sanitario es el más preocupado, ya que el 56 % de los encuestados afirma temer una filtración. En la administración pública hay más confianza, pues solo el 26 % teme una filtración. El 52 % de las organizaciones de servicios financieros están preocupadas por un ataque.

¿Cómo se está abordando esta cuestión (la probabilidad de que se produzcan vulneraciones)?

Cuando se les pregunta por sus planes para mitigar el riesgo de vulneración, los encuestados dan prioridad a la simplificación y la consolidación de las soluciones de seguridad, así como a hacer que la seguridad sea intrínseca. También son importantes la adaptación de la tecnología, las políticas y la asignación de un presupuesto a este problema.

El 38 % de los encuestados afirman que tienen previsto **aumentar la seguridad de su infraestructura y sus aplicaciones y reducir el número de soluciones puntuales**. Esta cifra se eleva al 42 % en el sector sanitario.

Un 38 % tiene previsto aumentar la seguridad en su infraestructura y sus aplicaciones y reducir el número de soluciones puntuales.

El 37 % afirma haber **adaptado la seguridad para mitigar el riesgo**. El sector de servicios financieros es el que más ha recurrido a adaptar la seguridad (42 %), seguido de las organizaciones sanitarias (40 %).

El 35,5 % ha **aumentado su presupuesto de seguridad**.

El 35 % afirma **haber actualizado su tecnología de seguridad para mitigar los riesgos**, una inversión importante dados los importantes cambios que se han producido en el panorama de la seguridad durante el último año. El 50 % de las organizaciones sanitarias han seguido esta tendencia.

El 31 % ha **actualizado la política y la metodología de seguridad para mitigar los riesgos**. El sector de los servicios financieros (38 %) ha adoptado esta metodología en mayor medida que otros.

¿En qué grado está de acuerdo o en desacuerdo con las siguientes afirmaciones relativas al desarrollo y el uso de aplicaciones en su organización?

Cuando se les pregunta si han cambiado su forma de ver los retos de seguridad en torno al desarrollo y uso de aplicaciones en su organización, los encuestados ofrecen información sobre los problemas a los que se enfrentan. En general, los responsables de TI de España están menos preocupados que sus homólogos internacionales por muchos de los problemas relacionados con las aplicaciones.

La visibilidad es motivo de preocupación. El 41 % está de acuerdo en que **necesita una mayor visibilidad de sus datos y aplicaciones para poder anticiparse a los ataques. Esta cifra se eleva al 50 % en el sector sanitario**.

Un 41 % necesita una mayor visibilidad de datos y aplicaciones.

El 40 % de los encuestados en España están de acuerdo en que los cambios provocados por la COVID-19 requieren un replanteamiento de la seguridad, y están de acuerdo en que **deben plantearse la seguridad de una forma distinta a como lo han hecho hasta ahora, pues la superficie de ataque se ha ampliado**.

El 40 % está de acuerdo en que necesita mayor seguridad contextual para hacer un seguimiento de los datos y la seguridad durante todo su ciclo de vida.

Dos quintas partes (40 %) afirman que **necesitan mayor seguridad contextual para poder hacer un seguimiento de los datos y la seguridad durante todo su ciclo de vida**. Esto sugiere un entorno en el que la seguridad tiende a centrarse en las amenazas y a ser reactiva. Los responsables de TI reconocen que los entornos dinámicos requieren una metodología centrada en el contexto.

El 42 % de los encuestados están de acuerdo en que su **capacidad para innovar como empresa depende de la capacidad para crear, gestionar y distribuir aplicaciones de forma más segura**.

El 39 % de los encuestados **tienen confianza en la comercialización de nuevas aplicaciones porque saben que serán seguras**, porcentaje inferior a la media internacional. La confianza es mayor entre los encuestados del sector sanitario, donde el 46 % tiene confianza en la comercialización de nuevas aplicaciones y servicios, mientras que en el sector público el 38 % no la tiene.

Cuando se les pregunta por la inteligencia artificial en el desarrollo de aplicaciones seguras, los encuestados muestran indicios de conflicto. El 35 % está de acuerdo **en que los problemas de seguridad impiden adoptar aplicaciones basadas en inteligencia artificial y aprendizaje automático para mejorar los servicios, pero el 41 % está de acuerdo en que les gustaría utilizar más la inteligencia artificial y el aprendizaje automático en aplicaciones para mejorar la seguridad y los servicios**.

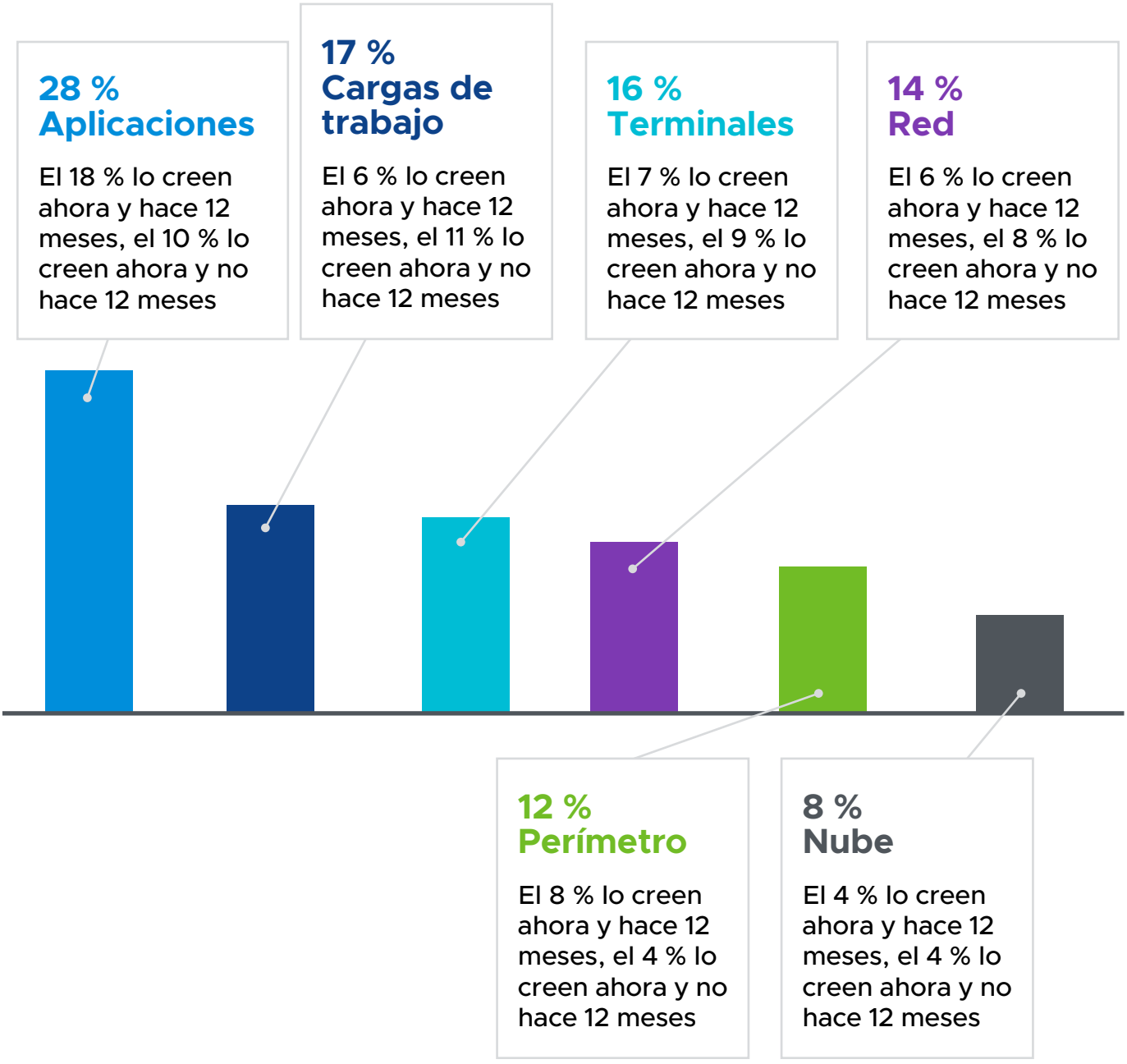
El 40 % coincide **en que hay demasiada complejidad en el mercado de las soluciones de seguridad como para cambiar nuestra política de seguridad, aunque seamos conscientes de que la seguridad informática actual no funciona**, lo que indica que los proveedores deben simplificar su propuesta y ofrecer una metodología unificada.

Por último, el 42 % está de acuerdo en que la seguridad de las aplicaciones está recibiendo atención en los directivos de la empresa, y que **los directivos se sienten cada vez más preocupados por la comercialización de nuevas aplicaciones y servicios debido al aumento de las amenazas y los daños que producen las filtraciones de datos y los ataques**.

> Un 42 % cree que el consejo de administración se siente cada vez más preocupado por los riesgos de seguridad en la comercialización de nuevas aplicaciones.

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

Las aplicaciones se consideran como el punto más vulnerable a vulneraciones en el recorrido de los datos y es obvio que han sido motivo de preocupación durante algún tiempo. Lo más interesante es que se percibe cada vez más que las cargas de trabajo representan una fuente de vulnerabilidad. Es probable que el año que viene las organizaciones se centren más en abordar este riesgo.



¿Cómo han abordado las organizaciones los retos de la implantación del teletrabajo?

Pedimos a los directores de seguridad de la información encuestados que valoraran si la implantación del teletrabajo se había realizado con éxito y si creían que una metodología que diera prioridad a la seguridad habría ayudado a realizar una transición más eficaz.

El 40 % cree que ha podido implantar el teletrabajo entre sus empleados y que la seguridad no ha sido un obstáculo. Esto demuestra la labor que han desarrollado los equipos de seguridad, que han estado más que nunca en el centro de las operaciones. Los encuestados del sector sanitario obtuvieron buenos resultados, pues el 46 % asegura no haber experimentado ninguna barrera de seguridad a la hora de implantar el teletrabajo. Por otro lado, los directores de seguridad de la información de servicios financieros han tenido más dificultades: un 24 % cree que no que ha podido implantar el teletrabajo sin problemas.

Los encuestados reconocen que siempre hay margen de mejora, y el 47 % está de acuerdo en que una metodología con prioridad en la seguridad habría aumentado su capacidad para permitir que los empleados trabajaran desde ubicaciones alternativas y siguieran siendo productivos. Este aspecto también se había confirmado en investigaciones anteriores de VMware, en las que se descubrió que la incapacidad de implementar la autenticación multifactorial era el mayor motivo de preocupación entre los profesionales informáticos en relación con la implantación del teletrabajo. Ahora que ha aumentado el perfil de la seguridad, debería ser más fácil para los directores de seguridad de la información conseguir el apoyo de los directivos para adoptar una metodología con prioridad en la seguridad.

> El 98 % ya utiliza o tiene previsto adoptar un enfoque con prioridad en la nube para proteger a la organización.

¿Utiliza o tiene previsto utilizar una estrategia de seguridad con prioridad en la nube?

Casi la totalidad de los encuestados declaran que están planeando cambiar a una estrategia de seguridad con prioridad en la nube. Aunque no de forma inmediata, esta estrategia se encuentra decididamente establecida en la hoja de ruta. El 98 % ya utiliza o tiene previsto adoptar un enfoque con prioridad en la nube para proteger a la organización.

El 36 % de los encuestados afirma que lleva más de un año siguiendo una metodología con prioridad en la nube, mientras que el 27,5 % indica que lleva menos de 12 meses. Otro 18 % tiene previsto adoptar este enfoque el próximo año, mientras que para el 17 % el cambio se producirá más adelante.

La madurez de la metodología con prioridad en la nube es alta entre las empresas de servicios financieros, donde el 30 % lleva siguiéndola más de 12 meses y otro 22 % menos de 12 meses. El 68 % de los encuestados del sector sanitario ya aplica una estrategia de seguridad con prioridad en la nube.

Datos y acciones clave

Nuestro segundo Informe sobre seguridad en España concluye que los profesionales de la ciberseguridad de alto nivel y las organizaciones para las que trabajan siguen enfrentándose a un gran volumen de amenazas sofisticadas. Estas se ven exacerbadas por el cambio a una plantilla muy dispersa geográficamente y, aunque la mayoría de las organizaciones han logrado implantar el teletrabajo, los directores de seguridad de la información reconocen que una metodología con prioridad en la seguridad habría facilitado la transición.

No cabe duda de que la COVID-19 ha cambiado significativamente el entorno de la ciberseguridad y seguirá influyendo en la estrategia en este ámbito. Por su parte, el sector de la ciberseguridad debe centrarse en ofrecer soluciones que reduzcan la complejidad operativa y, al mismo tiempo, protejan con solidez los entornos laborales distribuidos, que en el futuro se convertirán en la norma para la mayoría de las organizaciones.

El análisis de las respuestas a la encuesta revela importantes áreas en materia de ciberseguridad a las que habrá que prestar atención a lo largo del próximo año.

Priorizar la mejora de la visibilidad

Las organizaciones tienen un problema de visibilidad derivado de la rápida implantación del teletrabajo. Resulta difícil discernir la verdadera escala de los ataques, pues los defensores no pueden llegar a todos los rincones del ecosistema corporativo en los que se han introducido los dispositivos móviles personales y las redes domésticas. Si a esto añadimos los retos que implica la monitorización de las aplicaciones de terceros y de los proveedores, el número de puntos ciegos aumenta exponencialmente.

En pocas palabras, los defensores desconocen los puntos a los que no pueden llegar y, por tanto, las empresas quedan expuestas. Esta limitada visión contextual de los riesgos pone a los defensores en desventaja a la hora de proteger una superficie de ataque más amplia. Las organizaciones deben dar prioridad a la mejora de la visibilidad de todos los terminales y las cargas de trabajo para proteger el entorno de teletrabajo. Una inteligencia situacional robusta que ponga en contexto las amenazas ayudará a los defensores a dar prioridad y abordar los riesgos con confianza.

Responder a la reaparición de los programas de secuestro

La sofisticación de los ciberataques ha seguido aumentando y los programas de secuestro no son una excepción. Los atacantes consiguen acceder a las redes sin ser detectados, exfiltrando datos y estableciendo puertas traseras antes de lanzar peticiones de rescate o vender directamente los datos robados. Para evitar convertirse en víctimas de ataques repetidos, las organizaciones deben combinar una protección avanzada contra los programas de secuestro con una sólida reparación posterior al ataque que detecte la presencia de adversarios en el entorno.

Seguir subsanando la falta de eficacia de las tecnologías de seguridad obsoletas y la debilidad de los procesos

La seguridad obsoleta y la debilidad de los procesos siguen planteando un riesgo importante para las organizaciones, y la implantación del teletrabajo las ha expuesto aún más. A medida que salimos de la fase de respuesta inmediata y empezamos a vislumbrar el futuro, las organizaciones tendrán que identificar los cambios críticos que deberán darse en los procesos y la tecnología para ayudar a la plantilla remota e híbrida a trabajar de forma segura y reducir riesgos.

Ofrecer seguridad como servicio distribuido

En otros tiempos, los equipos de seguridad protegían los ordenadores de sobremesa propiedad de la empresa para empleados que trabajaban en las instalaciones conectándolos a aplicaciones corporativas que se ejecutaban en servidores de un centro de datos propiedad de la empresa. Hoy en día, el mundo es más complicado y los teletrabajadores se conectan a aplicaciones que se ejecutan en infraestructuras que quizá la empresa no gestione, posea ni controle. Con tantas superficies de ataque nuevas y distintos tipos de entornos que defender, la seguridad no puede ofrecerse como un catálogo de productos puntuales y puntos de control de la red. Los controles de los terminales y de la red deben realizarse como servicio distribuido. Esto implica proporcionar una seguridad que siga a los activos que se están protegiendo, independientemente del tipo de entorno.

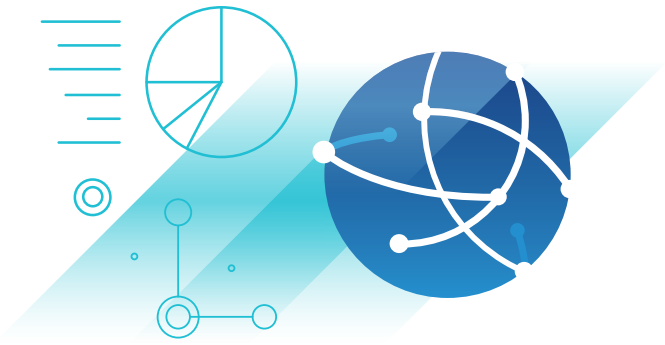
Adoptar una metodología de seguridad intrínseca con prioridad en la nube

El mayor cambio que hemos encontrado en nuestra investigación es la adopción de una estrategia de seguridad con prioridad en la nube. Sería difícil exagerar la magnitud del cambio que se ha producido en un periodo de tiempo tan corto; muy pocos directores de seguridad de la información antes de 2020 definían su estrategia de seguridad como una estrategia con prioridad en la nube. Es el resultado lógico de que las organizaciones hayan tenido que responder a las prácticas laborales altamente distribuidas que ha provocado súbitamente la COVID-19.

Pero la migración a la nube no es la panacea para la seguridad: no todas las nubes son iguales y las organizaciones deben investigar sus controles, porque si alguien quiere realizar un ataque a gran escala, la nube es el lugar idóneo. A medida que esta migración cobra impulso, la inversión en la seguridad de la nube pública será fundamental. Cuando uno se muda a una nube pública, cambia a un barrio muy difícil en el que la seguridad depende no solo de las propias acciones, sino de las de los vecinos. Puede que usted sea capaz de proteger sus propios recursos, pero no tiene ningún control sobre quiénes comparten ese entorno con usted. Las organizaciones deben dar prioridad a la protección de las cargas de trabajo en la nube en cada punto del ciclo de vida de la seguridad mientras realizan la gran migración a la nube.

En definitiva, el Informe sobre seguridad en España 2021 de VMware muestra un sector centrado en aprovechar los éxitos del año pasado y en responder a un entorno de amenazas que no para de cambiar. Los directores de seguridad de la información están muy convencidos del rumbo que deben seguir y las herramientas que tienen que emplear para mantenerse un paso por delante de los atacantes.

Metodología



En diciembre de 2020 VMware encargó un estudio que llevó a cabo una organización de investigación independiente, Opinion Matters. Se realizaron entrevistas a **251 directores de informática, directores de tecnología y directores de seguridad de la información** de diversos sectores, entre ellos, finanzas, sanidad, administración pública del estado y local, comercio minorista, fabricación e ingeniería, alimentación y bebidas, servicios públicos, servicios profesionales y medios de comunicación y entretenimiento. Este es el segundo Informe sobre seguridad en España que realiza VMware, y se basa en el estudio anterior, realizado en junio de 2020. Forma parte de un proyecto de investigación global realizado en **14 países**: 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 hace posible la compleja infraestructura digital del mundo actual. Las soluciones de nube, modernización de aplicaciones, red, seguridad y área de trabajo digital de la empresa ayuda a los clientes a ofrecer cualquier aplicación en cualquier nube y en cualquier dispositivo. Con sede en Palo Alto (California), VMware tiene el firme objetivo de servir para una buena causa, empezando por sus innovadoras tecnologías de vanguardia y 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 vmware.com
Copyright © 2021 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at vmware.com/go/patents. VMware is a registered trademark or trademark of VMware, Inc. and its subsidiaries in the United States and other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies. Item No: 863494aq-sec-insgt-rprt-es-es-uslet 5/21