vmware Carbon Black

España Threat Report

Una amenaza de mayor envergadura para la empresa

Junio de 2020

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. En ella se identifican las tendencias que se dan en la piratería informática y los ataques maliciosos y los efectos financieros y para la reputación que han tenido las violaciones de la seguridad. Se analizan los planes que tienen las organizaciones españolas para implantar nuevas tecnologías, adoptar marcos de ciberseguridad y abordar la complejidad del actual entorno de gestión de la ciberseguridad.

INDICE

METODOLOGÍA

En marzo de 2020, VMware Carbon Black encargó un estudio que llevó a cabo una organización de investigación independiente, Opinion Matters. Se realizaron entrevistas a 250 directores de sistemas de información (CIO), directores de tecnología (CTO) y responsables de seguridad informática (CISO) de empresas españolas de diversos sectores, entre ellos, finanzas, sanidad, Administración del Estado y autoridades locales, comercio minorista, fabricación e ingeniería, alimentación y bebidas, servicios públicos, servicios profesionales y medios de comunicación y entretenimiento. Este es el primer informe sobre amenazas en España de VMware Carbon Black. Forma parte de un proyecto de investigación global realizado en varios países, entre los que se incluyen España, Alemania, Australia, Canadá, Estados Unidos, Francia, Italia, Japón, Países Bajos, los países nórdicos, Singapur y el Reino Unido.

EL PANORAMA DE LOS CIBERATAQUES EN 2020 EN ESPAÑA

Rick McElroy
Responsable de estrategia de ciberseguridad, VMware Carbon Black

Prólogo

El panorama de las ciberamenazas está viviendo una escalada en España. En este primer informe sobre amenazas en España, encontramos que la frecuencia y la sofisticación de los ataques han alcanzado niveles sin precedentes. El 98 % de los profesionales de seguridad señalaron que se ha producido un aumento en el volumen de los ataques a los que se enfrentan. Los delincuentes están empleando una mayor variedad de tácticas y técnicas para intentar extorsionar, perturbar e infiltrarse en las organizaciones.

Por ello, los incidentes de seguridad son inevitables. Nuestra investigación concluye que:

El 99 % de las organizaciones españolas ha sufrido una filtración de datos por ciberataques en los 12 últimos meses y cada organización experimenta una media de 1,52 incidentes de seguridad.

Todos los profesionales de seguridad encuestados, salvo dos, indicaron que su organización había sufrido al menos una filtración de datos en los 12 últimos meses. Un encuestado prefirió no contestar y otro dijo que no había sufrido ningún ataque.

La considerable frecuencia y sofisticación de los ataques que revela este informe muestra que, por rápido que se adapten las empresas españolas a esta situación, las ciberamenazas evolucionan a un ritmo aún mayor. El 86 % de los profesionales de seguridad afirma que los ataques han aumentado en sofisticación y el 57 %, que se han vuelto moderada o significativamente más avanzados. Esto confirma las conclusiones de la investigación de la Unidad de Análisis de Amenazas de VMware Carbon Black: los adversarios están adoptando tácticas más avanzadas debido a que la generalización en el uso del malware facilita técnicas de ataque sofisticadas a un mayor número de ciberdelincuentes. No es de extrañar, por tanto, que el malware personalizado y de consumo sean tipos de ataque muy comunes.

98%

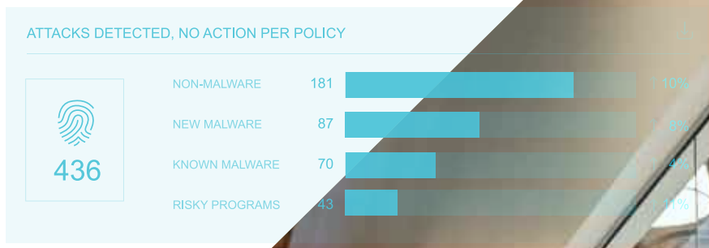
El 98 % de los profesionales de seguridad señalaron que se ha producido un aumento en el volumen de los ataques a los que se enfrentan

99%

El 99 % de las organizaciones españolas ha sufrido una filtración de datos por ciberataques en los 12 últimos meses y cada organización experimenta una media de 1,52 incidentes de seguridad

86%

El 86 % de los profesionales de seguridad afirma que los ataques han aumentado en sofisticación y el 57 %, que se han vuelto moderada o significativamente más avanzados



La reputación y los beneficios están en riesgo

A medida que aumenta la conciencia pública sobre los derechos de protección de datos y saltan a los titulares noticias sobre sanciones reglamentarias, no deja de incrementarse el impacto que tienen las infracciones de la seguridad. En España, los encuestados que trabajan para la **Administración del Estado y las autoridades locales** tienen más probabilidades de sufrir un impacto financiero grave por filtraciones de datos, mientras que quienes operan en **servicios financieros** indican que es probable que su reputación se vea gravemente afectada.

Los presupuestos aumentan pero ¿En gasto estratégico o táctico?

Los profesionales de seguridad españoles responden al repunte de las ciberamenazas con un incremento de los gastos en defensa. **Todos los encuestados salvo uno (más del 99 %) prevén un aumento del gasto.**

Un aspecto interesante es adónde va destinado ese gasto. La gran mayoría de los encuestados señaló inequívocamente que la caza de amenazas está dando sus frutos y que se reconoce cada vez más su valor a la hora de identificar a los agentes malintencionados que ya están en el sistema. Por ello, parece probable que esta inversión continúe. Pero ¿qué ocurre con los nuevos riesgos que están apareciendo?

La adopción del 5G en los 12 próximos meses está en la agenda de todos los encuestados, menos de dos. Sin embargo, la opinión está dividida en cuanto a la necesidad del gasto en seguridad. El 49 % cree que será necesario aumentar el gasto y los controles de seguridad, mientras que el 50 % no centrará el aumento presupuestario en la protección del 5G.

Un entorno complejo y abarrotado con múltiples tecnologías

Es posible que esta situación se deba al uso de múltiples tecnologías de seguridad. Los encuestados utilizan en la actualidad una media de más de **nueve consolas o agentes diferentes** para gestionar su estrategia de seguridad, lo que indica un entorno de seguridad que ha evolucionado de manera reactiva a medida que se han ido añadiendo herramientas para hacer frente a las amenazas emergentes, sin integrarlas de verdad. Esto ha dado lugar a entornos aislados y difíciles de gestionar que dan ventaja a los atacantes desde el principio. Está demostrado que los atacantes llevan la delantera cuando la seguridad no es un aspecto intrínseco del entorno. Ahora que el panorama de las ciberamenazas alcanza un punto de saturación, ha llegado el momento de la racionalización, del pensamiento estratégico y de la claridad en el despliegue de nuevas herramientas de seguridad.

99%
Todos los encuestados salvo uno (más del 99 %) prevén un aumento del gasto.

99.6%
Todos los encuestados salvo uno (el 99,6 %) prevén un aumento del gasto.

49%
El 49 % cree que será necesario aumentar el gasto en seguridad y los controles de ciberseguridad

División sobre la valía de los marcos de ciberseguridad

La visibilidad y la validación de las medidas de seguridad pueden mejorar significativamente mediante la aplicación del marco MITRE ATT&CK®. Aunque no es extraordinariamente elevado el conocimiento que se tiene de esta metodología, se aprecian de manera clara la relevancia y el valor que aporta. El 74 % de los encuestados lo conoce y el 55 % tiene previsto utilizarlo para reforzar sus medidas de seguridad, lo que demuestra que queda trabajo por hacer para establecer este marco como modelo de referencia entre las empresas.

Cargas de trabajo y aplicaciones como mayor riesgo para la ciberseguridad

La red está figura entre los prinicpales riesgos de infracción de seguridad entre los encuestados, y más de un tercio señalan que representa el mayor riesgo. Ligeramente por delante de la red se encuentran las cargas de trabajo y las aplicaciones, que algo más de la mitad de las organizaciones señalan como el mayor riesgo para la seguridad. Quizá no resulte sorprendente a la luz de las infracciones de seguridad relacionadas con aplicaciones de terceros. Dado que las empresas utilizan cada vez más aplicaciones en su apuesta por ofrecer flexibilidad y aumentar la productividad, garantizar su seguridad será de vital importancia.

Los encuestados utilizan en la actualidad una media de más de ocho cuadros de mando o agentes diferentes para gestionar su estrategia de seguridad

74% vs 55%
El 74 % de los encuestados lo conoce y el 55 % tiene previsto utilizarlo para reforzar sus medidas de seguridad

El impacto dela COVID-19

Cuando realizamos nuestra investigación primaria para esta edición del informe sobre amenazas de VMware Carbon Black, la COVID-19 apenas comenzaba a tener cierta repercusión en el mundo. Pero a medida que analizábamos los resultados quedó claro que la rápida escalada de la crisis nos obligaba a presentar la investigación procurando incluir un indicador del impacto que la situación está teniendo sobre la ciberseguridad y el ámbito de las ciberamenazas. Por tanto, volvimos a dirigirnos a los responsables de seguridad informática (CISO) para formularles preguntas complementarias que ayudaran a entender el impacto inmediato de la crisis y lo que los profesionales de la ciberseguridad están observando sobre el terreno en sus esfuerzos para adaptarse a un escenario en continuo cambio. Agradecemos a quienes se tomaron la molestia de responder en este difícil momento y creemos que la información obtenida será de gran valor para configurar la respuesta de ciberseguridad en el futuro.

Esperamos que encuentren útil e informativo nuestro primer informe sobre las amenazas en España.

Resultados dela investigación complementaria sobre la COVID-19

Con 1.002 encuestados en todo el mundo de marzo a abril de 2020, incluidos el Reino Unido, Estados Unidos, Singapur e Italia

Nuestra investigación sobre la COVID-19 ha revelado que la gran mayoría de las empresas se enfrentan a un aumento de los ciberataques debido a los empleados que trabajan desde casa, y el malware relacionado con la COVID-19 está haciendo sentir su dañina presencia.

Las principales carencias identificadas en la planificación de la recuperación frente a desastres giran en torno a la comunicación con interlocutores externos, como clientes, clientes potenciales y proveedores, así como a las propias operaciones informáticas y a los desafíos relacionados con el trabajo remoto de los empleados y la comunicación con ellos.

Las empresas que tardaron en adoptar la autenticación multifactorial han tenido motivos para lamentarlo, pues la incapacidad para implantarla constituye ahora la mayor amenaza a la que se enfrentan más de la cuarta parte de nuestros encuestados de todo el mundo. A medida que nos adaptamos a una nueva normalidad, con un aumento del teletrabajo y las amenazas que este implica, los departamentos informáticos se enfrentarán al reto de ampliar la protección de seguridad a los hogares de los empleados.

“Los delincuentes están empleando una mayor variedad de tácticas y técnicas para intentar extorsionar, perturbar e infiltrarse en las organizaciones.”

¿Ha cambiado el número total de ciberataques en su sistema a causa del teletrabajo?

Un asombroso 91 % de todos los encuestados a nivel mundial señala que se ha producido un aumento en el número total de ciberataques debido a que sus empleados trabajan desde casa.

El 7 % de los encuestados cree que han aumentado entre el 50 y el 100 %. Poco menos de un cuarto (24 %) señala que el volumen de ataques se ha incrementado entre el 25 y el 49 %.

Tres de los 1.002 encuestados indican que no tienen más empleados teletrabajando que antes.

De los cuatro países investigados, los encuestados de **Singapur** fueron los que más sufrieron un aumento de ataques, con un 93 %, seguidos de los del **Reino Unido**, con un 92 %, e **Italia**, con el 90,5 % y, por último, **EE. UU.,** con un 88 %. Además, **Italia** experimentó el mayor porcentaje de aumento de ataques (14 %) en la escala entre el 50 y el 100 % en comparación con el **Reino Unido,** que experimentó el más bajo en esta categoría (del 50 al 100 %) con un 2 %. **EE. UU.** ocupa el puesto más alto en la categoría del 25-49 %, pues el 28 % de los encuestados de este país indica que se ha producido un aumento en el número de ataques en esta escala.

El 14,5 % de las **empresas de medios de comunicación y entretenimiento** ha tenido un aumento de ataques de entre el 50 y el 100 %. El comercio minorista también puntúa alto, con un 13 % para esta categoría. El 45 % de los **comercios minoristas** también informa de aumentos de entre el 25 y el 49 %. A continuación se sitúa **fabricación e ingeniería**, con un 33 %.

El 41 % de las empresas con **501-1.000** empleados informan de un elevado incremento de los ataques, de entre el 25 y el 100 %.

Poco más de un cuarto (26 %) de las empresas que tienen departamentos informáticos de **más de 100 empleados** tuvieron un aumento de entre el 50 y el 100 %.

El 18 % de las que tienen departamentos informáticos de entre **41 y 50** empleados comunicaron aumentos del 50 al 100 %.

91%

Un asombroso 91 % de todos los encuestados a nivel mundial señala que se ha producido un aumento en el número total de ciberataques debido a que sus empleados trabajan desde casa.

48%

Casi la mitad (el 48 %) de los encuestados a nivel mundial indica que hubo carencias muy significativas en la comunicación con sus interlocutores externos

Un asombroso 91 % de todos los encuestados a nivel mundial señala que se ha producido un aumento en el número total de ciberataques debido a que sus empleados trabajan desde casa.

Casi la mitad (el 48 %) de los encuestados a nivel mundial indica que hubo carencias muy significativas en la **comunicación con sus interlocutores externos**, incluidos clientes, clientes potenciales y asociados. En general, el 84 % cree que hubo carencias que iban de graves a leves en la **comunicación con interlocutores externos.**

Más de un tercio (el 35 %) considera que hubo carencias muy significativas en la planificación de la recuperación frente a desastres en **operaciones informáticas,** incluido el despliegue de hardware y software. En términos generales, el 87 % cree que hubo carencias, fueran graves o leves, en **operaciones informáticas.**

Poco menos de un tercio (32 %) de los encuestados a nivel mundial cree que hubo carencias muy significativas en la **visibilidad de las amenazas para la ciberseguridad,** y otro 38 % considera que hubo carencias leves.

En cuanto al **teletrabajo de los empleados,** más de la cuarta parte (28 %) de los encuestados aprecia carencias graves y significativas, y en general, el 85 % de los encuestados considera que hubo carencias.

Más de un cuarto (27,5 %) admite haber tenido graves problemas a la hora de abordar la pandemia en lo relativo a la **comunicación con los empleados** y, en términos generales, el 78,2 % de los encuestados señala que estos problemas eran leves o muy significativos.

En cuanto a la planificación de la recuperación, un tercio (33 %) de los encuestados identifica lagunas muy significativas y un 88 % señala la existencia de disparidades de algún tipo.

Cinco de los 1.002 encuestados optaron por no responder a esta pregunta indicando de la COVID-19 no había revelado lagunas en la planificación de la recuperación frente a desastres en su empresa.

Las cifras de **Italia** son superiores a las de los otros tres países en identificación de carencias muy significativas en operaciones informáticas (41 %) visibilidad de las amenazas a la ciberseguridad (38 %) y teletrabajo (37 %). **Estados Unidos** tuvo la puntuación más alta en cuanto a carencias muy significativas (30 %) en la comunicación con los empleados, mientras que **Singapur** obtuvo la puntuación más alta (52 %) en la comunicación con interlocutores externos. Tanto **Italia** como **el Reino Unido** obtuvieron las puntuaciones más altas en carencias muy significativas en la planificación de la recuperación, con un 36 %.

29%

Más de la cuarta parte de los encuestados de todo el mundo (29 %) señala la incapacidad para implantar la autenticación multifactorial como la mayor amenaza para su empresa.

¿Cuáles de las siguientes amenazas asociadas con La COVID-19 han sido más importantes para su empresa hasta el momento?

Más de la cuarta parte de los encuestados de todo el mundo (29 %) señala la **incapacidad para implantar la autenticación multifactorial** como la mayor amenaza para su empresa. En segundo lugar, se encuentra el **malware relacionado con la COVID-19,** con un 15,5 %, y en tercer lugar, la **incapacidad para desplegar a tiempo parches de software** (13 %). El 10 % señala el **phishing** y el 6 %, el **spear phishing, la exposición del IoT** al ciberriesgo y la **falta de eficiencia en el acceso remoto.** Otras amenazas destacadas son el **enmascaramiento** (4,5 %), **el ransomware** (4 %) y la **ingeniería social** (4 %).

La **incapacidad para implantar la autenticación multifactorial** se aprecia con mayor intensidad en **Singapur** y Estados Unidos, con un 32 %. El **malware relacionado con la COVID-19** consigue una mayor puntuación en **Italia** (21 %), seguida de cerca por el **Reino Unido** (20 %), mientras que en **Singapur** es donde el **phishing** puntúa más alto (12 %).

La **incapacidad para implantar la autenticación multifactorial** es la mayor amenaza para las organizaciones de **servicios financieros**, con un 50 %. El **malware relacionado con la COVID-19** ha tenido un gran impacto en los sectores de **alimentación y bebidas** (49 %) y **servicios profesionales** (30 %). Los **medios de comunicación y el entretenimiento** han sido los más afectados por el **phishing** (29 %).

El **malware relacionado con la COVID-19** ha tenido una mayor repercusión en organizaciones pequeñas, en particular las que cuentan con 50-250 empleados (43 %). En el caso de empresas de entre 251 y 500 trabajadores, el mayor impacto lo ha tenido la **incapacidad para implantar la autenticación multifactorial** (46 %).

¿Cómo y en qué medida han cambiado las amenazas durante la COVID-19?

92%

Durante la pandemia, el mayor incremento de cambio en las amenazas se produjo con el malware relacionado con la COVID-19, que registró un incremento general del 92 %,

Durante la COVID-19, el mayor incremento de cambio en las amenazas se produjo con el **malware relacionado con la COVID-19**, que registró un incremento general del 92 %, y el 53 % de dicho incremento se produjo en las categorías del 51 a más del 100 %. El segundo es la **exposición del IoT al ciberriesgo,** con un incremento de cambio en la amenaza del 89 %, un 21 % del cual se dio en las categorías del 51 a más del 100 %. En tercer lugar, se encuentra el **phishing**, con el 89 %, un 24,5 % del cual corresponde a las categorías del 51 a más del 100 %. El **spear phishing** también arrojó un resultado significativamente alto, con un 88 % de incremento total de cambio en la amenaza, y poco menos de un cuarto (23 %) de este también corresponde a la categoría del 51 a más del 100 %.

De los cuatro países, **Italia** experimentó el mayor incremento general de **malware relacionado con la COVID-19** (del 96 %), con un asombroso aumento del 70 % en las categorías del 51 a más del 100 %. Le sigue el **Reino Unido**, con un 93 % en total, y un 54 % en las categorías del 51 % a más del 100 %.

Recientemente, ha aparecido una nueva familia de ransomware conocida como Coronavirus y se ha producido una tendencia al alza en este tipo de ataques. Lamentablemente, los ciberdelincuentes se encuentran en el mejor momento para la creación y distribución de **ransomware**. Sin embargo, el **ransomware** tiene una presencia menor que otras categorías, pues obtiene un 67 % de incremento total de cambio en la amenaza entre los encuestados.

El 29 % de los encuestados de todo el mundo señalan la **incapacidad para implantar la autenticación multifactorial** como la mayor amenaza para su empresa hasta el momento. En relación a los cambios que han experimentado las amenazas durante la COVID-19, se obtuvieron resultados relativamente altos, ya que el 87 % de los encuestados creen que se ha producido un incremento general y el 24 %, un incremento de entre el 51 y más del 100 %.

Conclusiones completas del estudio

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

Un asombroso 98 % de las organizaciones españolas han sufrido un aumento en el número de ciberataques en los 12 últimos meses.

Los encuestados informan de un incremento medio de frecuencia del 41,5 %, y el 56 % del total aseguran que se ha producido un aumento del volumen de ataques de entre el 26 % y el 100 %.

El 35 % de los encuestados del sector de **fabricación e ingeniería** creen que se ha producido un aumento del 51-100 %, mientras que el 34 % de los encuestados del sector de **medios de comunicación y entretenimiento** informan de un aumento del 26-50 %.

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

El 86 % de los encuestados dice que los ataques se han vuelto más sofisticados en los 12 últimos meses. De estos, el 57 % afirma que se han vuelto **moderada** o **significativamente** más sofisticados.

La mitad de los encuestados que trabajan en servicios financieros consideran que ha habido un incremento significativo en la sofisticación de los ataques a los que se enfrentan.

98%

Un asombroso 98 % de las organizaciones españolas han sufrido un aumento en el número de ciberataques en los 12 últimos meses.

56%

el 56 % del total aseguran que se ha producido un aumento del volumen de ataques de entre el 26 % y el 100 %

19% Google Drive™ (ataques basados en la nube) encabeza la tabla con un 19 %.

Todos los responsables de seguridad (CISO) y directores de sistemas de información (CIO) que participaron en nuestra investigación, menos uno, confirmaron que habían sufrido una infracción de seguridad tras un ciberataque en los 12 últimos meses.

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

Google Drive™ (ataques basados en la nube) encabeza la tabla con un 19 %. A continuación, se encuentran los **ataques sin archivo,** con un 18 %. El **malware de consumo** es el tercero más frecuente, con un 13 %, y el **malware personalizado** es el cuarto, con un 12 %.

El Island hopping se encuentra en una posición relativamente baja en la lista, con un 2 %, mientras que el **ransomware** no está mucho más arriba, con un 4 %, lo que indica que el panorama de amenazas puede estar cambiando a medida que los delincuentes abandonan vectores de ataque que antes eran muy frecuentes.

Los encuestados del sector de **fabricación e ingeniería** parecen estar a merced de los ataques a Google Drive (en la nube), puesto que el 29 % señalan que es el ataque más frecuente (en comparación con una media del 19 %). Los encuestados del sector de **medios de comunicación y entretenimiento** también se ven más afectados por el ataque a Google Drive (en la nube) que la media: el 24 %.

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

Todos los responsables de seguridad (CISO) y directores de sistemas de información (CIO) que participaron en nuestra investigación, menos uno, confirmaron que habían sufrido una infracción de seguridad tras un ciberataque en los 12 últimos meses. Un encuestado prefirió no contestar.

El número de infracciones de seguridad que sufrieron las organizaciones de media fue de 1,52. La mayor parte de los encuestados (el 69 %) asegura haber sufrido una infracción de seguridad, mientras que la cuarta parte dice haber sufrido 2 o 3.

Las organizaciones de servicios financieros fueron objeto del mayor número de infracciones de seguridad (2,13), y el 12,5 % de estas organizaciones sufrieron cinco. El 12,5 % de los encuestados del sector de fabricación e ingeniería afirman haber sufrido 3 infracciones de seguridad.

La causa de muchas de estas infracciones de seguridad parece ser la falta de planificación y de tecnología adecuada

18%
La principal causa se identifica como “nuestros procesos no eran tan fuertes como creíamos”, en el 18 % de los casos

87%
En general, más de cuatro de cada cinco encuestados (el 87 %) afirman haber sufrido un impacto en su reputación tras una infracción.

¿Cuál fuela lrincipal causa de estas infracciones de seguridad?

La causa de muchas de estas infracciones de seguridad parece ser la falta de planificación y de tecnología adecuada, lo que resulta preocupante. La principal causa se identifica como **“nuestros procesos no eran tan fuertes como creíamos”**, en el 18 % de los casos, seguido de cerca por **“nuestra tecnología de seguridad estaba desfasada”**, lo que permitió a los hackers aprovecharse y provocar el 17 % de las infracciones.

La **Administración del Estado y las autoridades locales** (21 %) y los **servicios profesionales** (22 %) ocupan los dos primeros puestos de la lista por contar con procesos que no eran tan fuertes como creían. **La Administración del Estado y las autoridades locales** (23,5 %) ocupan también posiciones destacadas en la lista porque **“nuestra tecnología estaba desfasada”**.

Frente a esta tendencia, los encuestados de **medios de comunicación y entretenimiento** fueron los más susceptibles a los ataques de aplicaciones web (20 %). Las aplicaciones de terceros (21 %) y la vulnerabilidad del sistema operativo (21 %) se encuentran en lo alto de la lista de los **encuestados de servicios financieros.**

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

El porcentaje de organizaciones que dicen haber sufrido un impacto financiero **grave** tras una infracción de seguridad se acerca a un quinto (el 19 %). Más de un cuarto (26,5 %) de las empresas del **sector de la Administración del Estado y las autoridades locales** señalan que han sufrido un grave impacto financiero como resultado de una infracción de seguridad, al igual que un cuarto de las empresas de **servicios financieros** y un quinto (21 %) de las de **fabricación e ingeniería.** Por el contrario, el 44 % de los encuestados de **servicios profesionales** afirman no haber tenido un impacto financiero negativo.

Casi un quinto (18 %) de los encuestados indican que han sufrido un **grave** impacto en su reputación como resultado de una infracción de seguridad. En general, más de cuatro de cada cinco encuestados (el 87 %) afirman haber sufrido un impacto en su reputación tras una infracción.

Los **servicios financieros** encabezan la lista de quienes han sufrido un impacto **grave** para la reputación, con un 33 %; el siguiente en la lista es la **Administración del Estado y las autoridades locales,** con un 23,5 %; le sigue el **sector de fabricación e ingeniería**, con un 21 %.

Fabricación e ingeniería fue el sector que más informa de daños de algún tipo a su reputación, con un 94 %.

En los 12 últimos meses, ¿La caza de amenazas que ha realizado su empresa ha logrado el objetivo de reforzar su defensa contra los ciberataques? ¿La caza de amenazas ha detectado ciberataques que no se habrían detectado de otro modo?

La caza de amenazas se está volviendo omnipresente —el 99 % de los encuestados la utiliza en el marco de su estrategia de ciberseguridad. También está demostrando ser eficaz: el 99 % de los encuestados señala que ha reforzado las defensas de su empresa, y el 25 % que las ha reforzado significativamente.

El porcentaje que ha encontrado **evidencias significativas** de actividad maliciosa es de cerca de un tercio (31 %), mientras que el 98 % ha encontrado algunas evidencias de actividad maliciosa gracias a la caza de amenazas.

Las organizaciones de **servicios financieros** han tenido particular éxito en la detección de actividades maliciosas, ya que el 58 % encontró evidencias significativas, mientras que el 100 % de los encuestados de **medios de comunicación y entretenimiento** y de **servicios profesionales** que realizaron caza de amenazas encontraron algún nivel de actividad maliciosa.

31%

El porcentaje que ha encontrado evidencias significativas de actividad maliciosa es de cerca de un tercio (31 %),

99%

La caza de amenazas se está volviendo omnipresente —el 99 % de los encuestados la utiliza en el marco de su estrategia de ciberseguridad

¿En qué cantidad tiene previsto aumentar su presupuesto de ciberdefensa en los 12 próximos meses?

Todos los responsables de seguridad (CISO) y directores de sistemas de información (CIO) que entrevistamos, menos uno, afirman que tenían previsto aumentar su presupuesto en ciberdefensa en los 12 próximos meses, con un aumento medio del 26 %. Un aumento del gasto presupuestario de entre 21-30 % es el más común entre los encuestados (57 %).

El 70 % de los encuestados de **medios de comunicación y entretenimiento** planean un aumento de estas proporciones, así como el 62 % de los encuestados de la **Administración del Estado y las autoridades locales.**

Todos los responsables de seguridad (CISO) y directores de sistemas de información (CIO) que entrevistamos, menos uno, afirman que tenían previsto aumentar su presupuesto en ciberdefensa

12

Todos los responsables de seguridad (CISO) y directores de sistemas de información (CIO) que encuestamos, menos dos, dijeron que planeaban adoptar el 5G en los 12 próximos meses

9,12

El promedio de tecnologías desplegadas es de 9,12,

74%

El conocimiento del marco MITRE ATT&CK® es relativamente alto en España: un 74 % de los encuestados lo conoce

¿Adoptará el 5g en un plazo de 6 a 12 meses y tendrá que aumentar el gasto en seguridad y controles para adoptarlo? es decir, ¿Realizará nuevas inversiones netas en función de este nuevo riesgo?

Todos los responsables de seguridad (CISO) y directores de sistemas de información (CIO) que encuestamos, menos dos, dijeron que planeaban adoptar el 5G en los 12 próximos meses, y el 62 % esperaba hacerlo en seis. Están divididos casi a partes iguales en cuanto a las implicaciones para la seguridad. El 49 % dice que será necesario aumentar el gasto y los controles de seguridad, mientras que el 50 % no cree que sea necesario invertir.

Los encuestados del sector de **servicios financieros** son los que más creen que adoptarán el 5G en los seis próximos meses y que invertirán en seguridad y controles relacionados (50 %). El 25 % de los encuestados de **servicios financieros** no necesitarán aumentar el gasto por la adopción del 5G en los seis próximos meses. El 50 % de los encuestados de la **Administración del Estado y las autoridades locales** adoptarán el 5G en los seis próximos meses, pero no creen que necesitarán aumentar el gasto para ello.

¿Cuántas tecnologías de seguridad diferentes utiliza en la gestión de su programa de seguridad (Por ejemplo, diversas consolas, agentes, herramientas)?

Casi tres cuartas partes (72 %) de las empresas tienen desplegadas entre 5 y 10 tecnologías distintas para gestionar su programa de seguridad. El 20 % utilizan entre 11 y 25 tecnologías.

El promedio de tecnologías desplegadas es de 9,12, cifra que aumenta hasta 9,66 en la **Administración del Estado y las autoridades locales.**

¿Conoce y tiene pensado utilizar el marco MITRE Att&Ck® para validar su postura de seguridad?

El conocimiento del marco MITRE ATT&CK® es relativamente alto en España: un 74 % de los encuestados lo conoce y un 55 % está preparándose para adoptarlo.

El sector de la **Administración del Estado y las autoridades locales** es el que muestra la actitud más positiva hacia el marco, pues un 59 % lo conoce y piensa utilizarlo, seguido de cerca por las organizaciones dedicadas a **fabricación e ingeniería** (58 %). Los más escépticos son los encuestados del sector de **servicios financieros**, donde el 58 % afirma que lo conoce pero no piensa utilizarlo.

En los 12 últimos meses, ¿Cuáles de las siguientes categorías han requerido una inversión al alza o a la baja (Es decir, un cambio en las prioridades del presupuesto)? (Marque todas las que correspondan)

Las **redes** se sitúan en cabeza, con un 83 %, seguidas por las **cargas de trabajo y aplicaciones,** con un 80 %, a continuación, **los móviles** (un 64 %) y, por último, los **terminales**, con un 31 %.

¿Cuál de los siguientes riesgos de infracción de seguridad es el principal en su programa de seguridad?

Las **cargas de trabajo y aplicaciones** se consideran el mayor riesgo, señalado por el 51 % de los encuestados, seguido de la **red,** identificada por poco más de un tercio (35 %). El siguiente riesgo que más se menciona son los **dispositivos móviles** —con el 10 %—, mientras que los **terminales**, como los ordenadores portátiles y de escritorio, llegan al 3 %.

En **servicios financieros** se aprecia un riesgo más alto que la media en los dispositivos móviles (21 %). El 65 % de los encuestados de la **Administración del Estado y las autoridades locales** considera que el mayor riesgo de infracción son las cargas de trabajo y aplicaciones.