Las ciberamenazas pulverizan récords

En los últimos meses, estamos viviendo la consolidación de la industria de la ciberdelincuencia basada en una proliferación de ciberataques diarios a nivel mundial. El común de los mortales ya tiene en sus conversaciones del día a día la ciberseguridad como tema recurrente, gracias, entre otras cosas, a que 2021 ha sido un año histórico en términos de ciberataques registrados, lo que nos hace estimar, con estos indicadores adelantados, que en 2022 se volverán a batir nuevos récords.

El informe 'Digital Trust 2022', elaborado por PwC a partir de una encuesta con 3.602 responsables de ciberseguridad (CISO), CEO y altos directivos de 66 países (141 españoles), adelanta un nuevo incremento de los ciberataques a empresas en 2022, con más del 50% de las compañías entrevistadas que espera que aumenten por encima de los niveles récord de 2021. Una amenaza que se está viendo reflejada en sus presupuestos, ya que el 69% de las compañías (el 71% en España) prevé aumentar sus inversiones en ciberseguridad, frente al 55% del año pasado, y un 26% -el mismo porcentaje en nuestro país- espera que este incremento sea del 10% o esté, incluso, por encima.

Estrategia de ciberseguridad

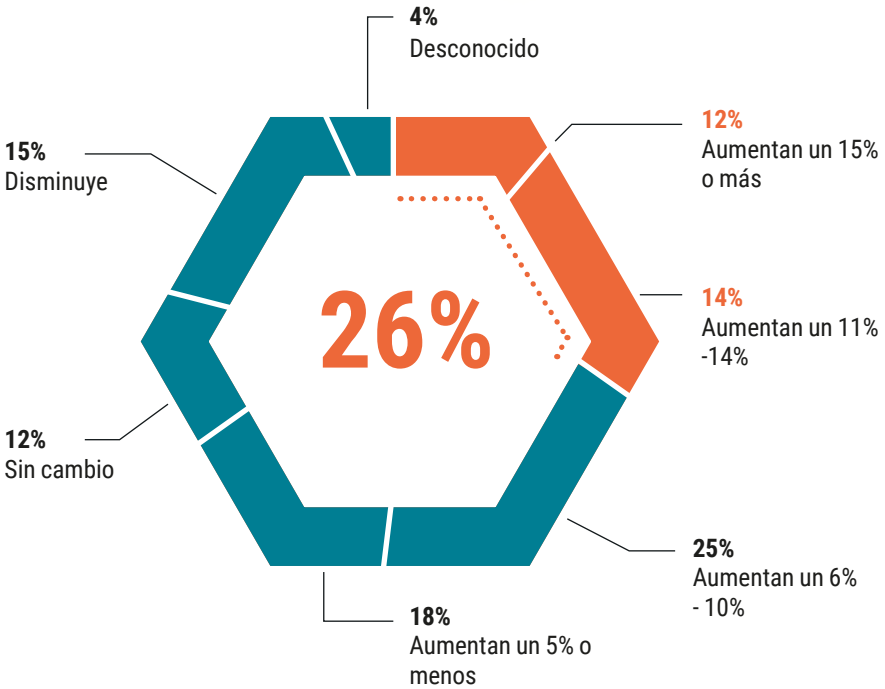
En general, los CEO encuestados se consideran implicados y comprometidos en la mitigación de los riesgos relacionados con la ciberseguridad como parte de su modelo operativo y estrategia futura, definiendo objetivos similares en sus planes estratégicos de ciberseguridad en los próximos tres años. En estos objetivos, la prevención ante ciberataques es la línea más importante; el incremento de la resiliencia y la rapidez en la respuesta a incidentes e interrupciones de servicio es la siguiente, seguida de la mejora de la capacidad de las organizaciones para gestionar las amenazas presentes y futuras. En el caso de España, se destaca de forma muy notable la mejora del grado de cumplimiento con reguladores.

Mario Benavente, Director de Soluciones de Seguridad de Negocio en PwC

Crecimiento de los ciberataques

Pero ¿cuáles son los ciberataques que más van a crecer en 2022? ¿De dónde vendrán y por dónde es más probable que entren en las empresas? Según el conjunto los directivos participantes en

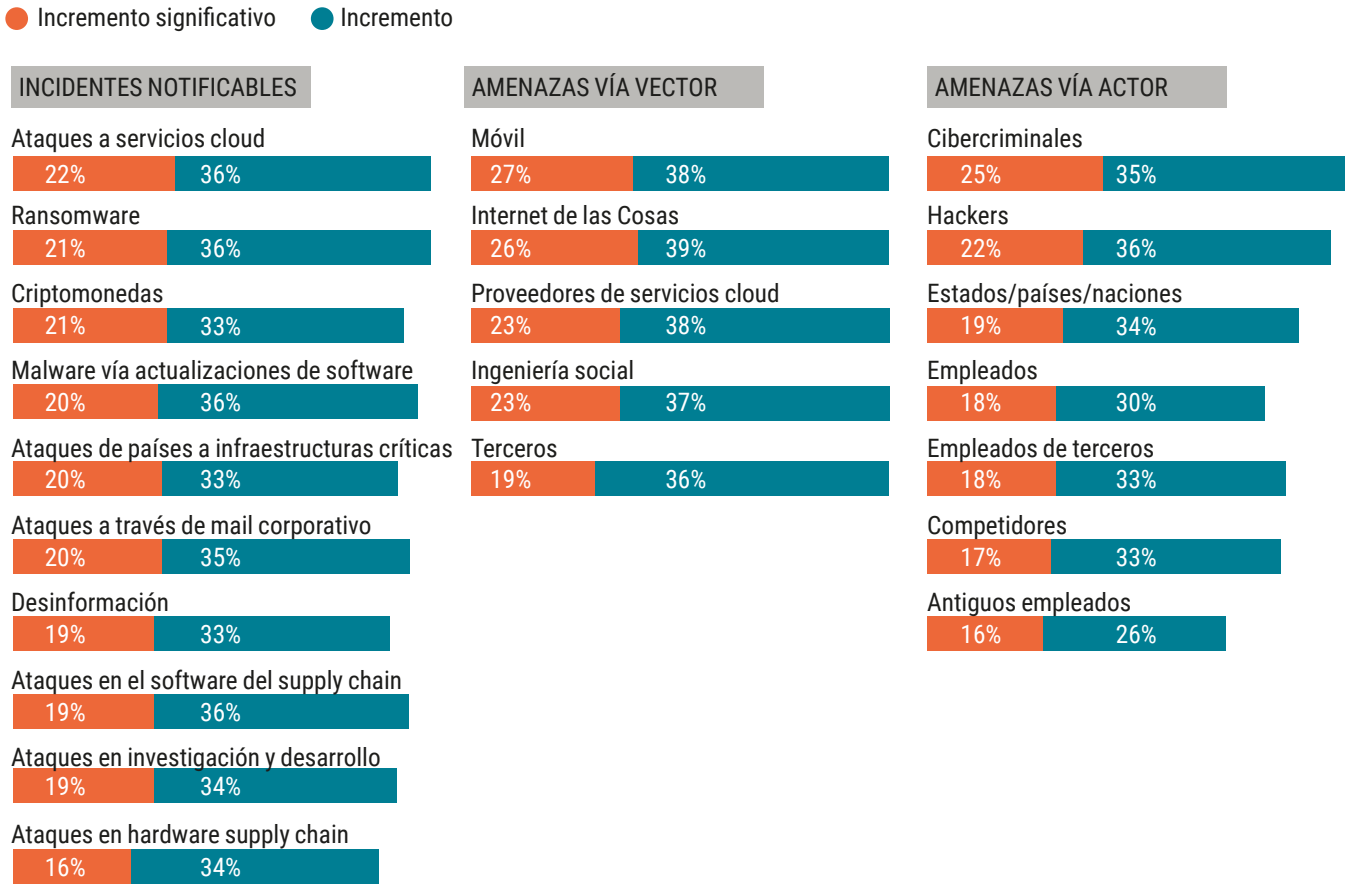
Previsión de los presupuestos en ciberseguridad



Objetivos de ciberseguridad de las empresas en los próximos 3 años

	Global (3602)	Europa Occidental (1203)	España (141)
Incremento de la prevención ante ciberataques efectivos	1st	1st	2nd
Mejora de los tiempos de respuesta ante incidentes y caída de servicios	2nd	2nd	1st
Mejora de la capacidad de gestión de amenazas presentes y futuras	3rd	3rd	4th
Obtención de mejores resultados en los procesos de transformación	4th	4th	9th
Mejora de la experiencia de usuario	5th	7th	5th
Mejor cumplimiento con requerimientos de reguladores	6th	8th	3rd

Previsión para 2022 de incidentes de ciberseguridad, vectores y actores



el estudio, los ataques que más van a crecer el próximo año son los que tienen como objetivo los servicios en la nube y los ransomware, seguidos del malware descargado a través de las actualizaciones de software y los ataques al correo corporativo y al software de terceras partes.

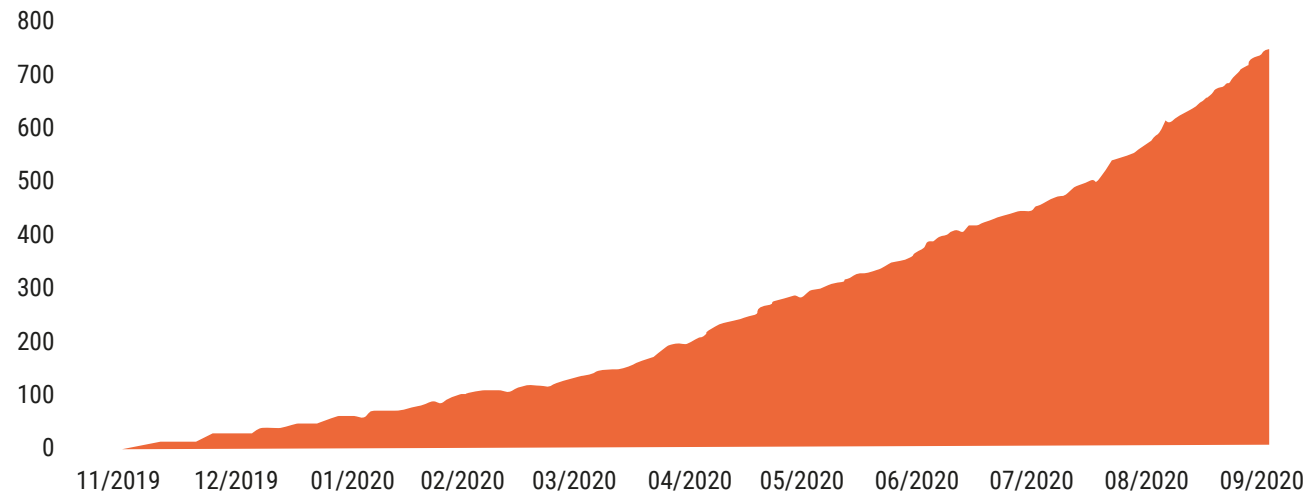
El 57% de los responsables de seguridad encuestados coinciden en afirmar que su principal preocupación y gran reto a combatir durante los próximos años son los ataques a servicios cloud y los ransomware. Sin ir más lejos, durante el primer semestre de 2021 el volumen global de ransomware alcanzó los 304,7 millones de ataques, superando el total de todo el año 2020, lo que supone un aumento del 151% hasta la fecha.

Aquellas organizaciones que todavía no han dado los pasos necesarios para entender y reducir su nivel de vulnerabilidad frente a estos ataques deberían actuar ya. Esto es especialmente importante, puesto que se han visto afectadas empresas de todos los sectores y la frecuencia de estos ataques se prevé que continúe en aumento durante los próximos años.

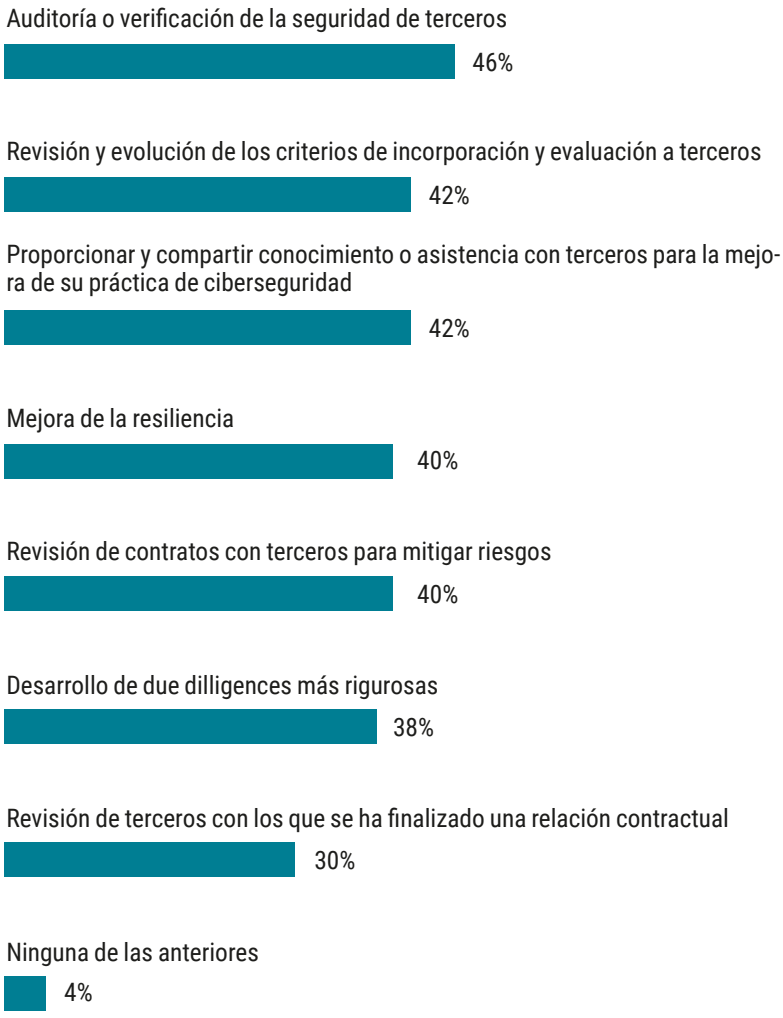
Los atacantes de ransomware a menudo trabajan con otros grupos criminales que utilizan técnicas automatizadas y a escala masiva para obtener acceso a las redes de las empresas. Este tipo de ataques permiten a los delincuentes obtener una gran rentabilidad económica y facilidad para ocultarse gracias al uso de sistemas de pago internacionales

Evolución de filtraciones de datos por ransomware

Total acumulado de filtraciones de datos por ransomware
noviembre 2019 - septiembre 2020



Iniciativas en la gestión de riesgos de terceros



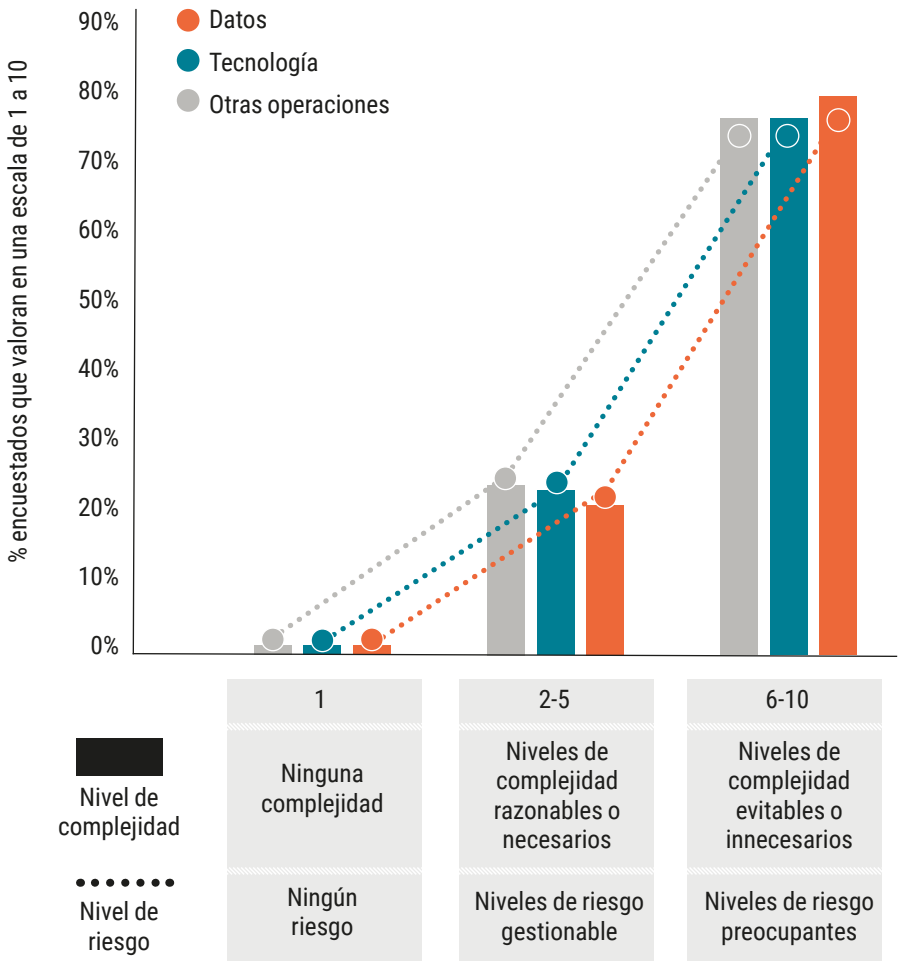
que permiten el anonimato, como las criptodivisas.

Pero, ¿cómo pueden entonces protegerse las empresas de estos ataques? Para reducir el riesgo de un ataque de ransomware de origen humano, las organizaciones, aparte de concienciar a los empleados sobre los correos electrónicos de phishing, deben implementar controles técnicos de seguridad para evitar que este tipo de correos maliciosos comprometan los puestos de trabajo, como, por ejemplo, con una buena configuración de sus herramientas de filtrado web y de correo o restringiendo y/o deshabilitando la ejecución de scripts o macros que comprometan los puestos de trabajo.

En este sentido, no solo es determinante que las organizaciones tengan implementados estos controles, sino que deben validar que estos estén funcionando de manera efectiva previniendo y detectando las técnicas utilizadas en cada uno de ellos. En muchos casos analizados, se muestra una 'desconexión' entre dónde creen las organizaciones que están y el nivel de reducción del riesgo real en el que se encuentran (por ejemplo, desplegando herramientas sin haberlas configurado correctamente, falta de controles por incompatibilidad en sistemas 'legacy', etc.).

Tal y como refleja el informe Digital Trust 2022, las vías de penetración que más van a utilizar los ciberdelincuentes

Complejidad percibida en las empresas



serán fundamentalmente los móviles, el Internet de las Cosas, los proveedores de servicios en la nube, la ingeniería social y las terceras partes.

Ciberseguridad en terceras partes

El conjunto de proveedores y terceras partes preocupa especialmente a las organizaciones, dado que se considera como una de las principales amenazas que continuará incrementándose en los próximos años, pudiendo convertirse en un punto ciego de entrada de los ciberataques. El 60% de los entrevistados reconoce no tener un conocimiento profundo de las brechas de seguridad asociadas con estas terceras partes y un 20% asegura tener poco o ninguno.

Como primer paso para poder mejorar el nivel de madurez en seguridad en la gestión de terceros de una empresa es fundamental simplificar el volumen de proveedores, aumentando y mejorando sus indicadores de control. Como medida proactiva, las empresas podrían utilizar sus datos como input para mejorar la gestión de sus riesgos de ciberseguridad, pero actualmente solo el 26% -24% en el caso de los encuestados españoles- cuantifica los riesgos IT y de ciberseguridad.

Hay que tener en cuenta que una organización puede ser vulnerable a un ataque a su cadena de suministro, incluso aunque disponga de ciberdefensas robustas, ya que los atacantes de ahora se adaptan a cada cambio tecnológico con facilidad, encontrando nuevas vías de penetración a través de sus proveedores, por lo que la implicación debe darse a todos los niveles dentro de la empresa como parte de su modelo operativo y estrategia futura.

57%

El 57% de los responsables de seguridad afirman que su principal preocupación para los próximos años son los ataques a servicios cloud y los ransomware.

Complejidad del modelo operativo

Por otro lado, con el impulso de la transformación digital y la conectividad, la lucha contra las ciberamenazas se hace mucho más complicada. Es por ello que el 75% de los encuestados afirman que en sus empresas existe un exceso de complejidad en su modelo operativo y procesos, así como que esta complejidad conlleva un incremento notable de los riesgos de ciberseguridad y de privacidad.

La complejidad en sí misma no es mala, de hecho, suele ser inherente al crecimiento del negocio, al necesitar más personas y más tecnología. Para los encuestados, estas son las principales consecuencias de la complejidad operativa:

1. Pérdidas financieras debidas a robo de datos o ciberataques.
2. Incapacidad de innovar al ritmo que el mercado lo posibilita.
3. La falta de resiliencia operativa, o la capacidad de recuperación ante un ciberataque o un fallo tecnológico.

Conclusiones

Como conclusión, resaltar que las organizaciones que aumentaron sus presupuestos de ciberseguridad en el pasado afirman haber logrado sus objetivos eficazmente, apalancándose en diferentes iniciativas:

- Evitando graves pérdidas económicas gracias a las medidas de seguridad tomadas (30% a nivel global y 33% en España).

- Impulsando la formación y concienciación en ciberseguridad de sus empleados (29% a nivel global y 21% en España).

- Activando las relaciones entre el sector público y el privado para dar respuestas más eficaces a un ciberataque (28% a nivel global y 21% en España).

- Fomentando el intercambio de información sobre nuevas amenazas y soluciones, permitiendo mejorar el conocimiento colectivo para aprender a combatirlas (31% a nivel global y 28% en España). ■