INFORME

proofpoint®

# CIBERSEGURIDAD CENTRADA EN LAS PERSONAS:

# UN ESTUDIO ENTRE LÍDERES DE TI DE ESPAÑA

# RESUMEN EJECUTIVO

El panorama de ciberamenazas sigue evolucionando en todo el mundo, y España no es una excepción. Y, cada vez más, los ciberdelincuentes dirigen sus ataques a las personas en lugar de a la infraestructura.

Ya sea mediante amenazas a través del correo electrónico, como las estafas BEC (Business Email Compromise), del compromiso de cuentas en la nube o de ataques de ransomware, los atacantes son perfectamente conscientes de que los empleados son un objetivo fácil. Los ciberdelincuentes recurren a ataques de ingeniería social para robar credenciales, apropiarse de datos sensibles y transferir fondos de manera fraudulenta. Empleados de todos los niveles y cargos pueden poner en riesgo a su empresa de muchas maneras: utilizando contraseñas débiles y compartiendo credenciales, haciendo clic en enlaces maliciosos o descargando aplicaciones no autorizadas.

A esto se añade la adopción global del teletrabajo, que ha introducido nuevos desafíos de ciberseguridad para organizaciones de todo el mundo. Los empleados han estado trabajando al margen de los procedimientos de seguridad habituales a los que están sometidos en la oficina, y los ciberdelincuentes lo saben bien.

Para hacer frente a esta situación, las empresas necesitan tener una visión clara sobre cómo están siendo atacadas, los riesgos que suponen estos ataques y cuál es su nivel de preparación (y más importante aún, el de sus empleados) para protegerse frente a ellos. Esto es de particular importancia en el clima actual, en el que la imposición del teletrabajo aumenta la presión sobre los equipos de ciberseguridad en todo el mundo.

La formación y concienciación en materia de seguridad de los empleados es el eje de cualquier estrategia eficaz, y a menudo marca la diferencia entre que un ataque tenga éxito o se quede en un intento.

Para comprender mejor el impacto que tienen en las organizaciones los ciberataques centrados en las personas, Proofpoint encargó una encuesta entre 150 CISOs y CSOs de toda España. Para el trabajo de investigación, realizado por la empresa de estudios Censuswide, se realizaron entrevistas a empresas españolas de una amplia variedad de sectores en octubre de 2020.

**La encuesta analizó las siguientes áreas clave:**

- Frecuencia de los ciberataques
- Preparación de los empleados y de la organización
- Impacto de la adopción global del teletrabajo
- Preparación de las organizaciones para el panorama de amenazas futuro

El estudio puso de manifiesto que la necesidad de proteger a las personas de ataques inminentes nunca ha sido mayor, ya que la mayoría de las organizaciones españolas habían experimentado más de un ciberataque en el último año.

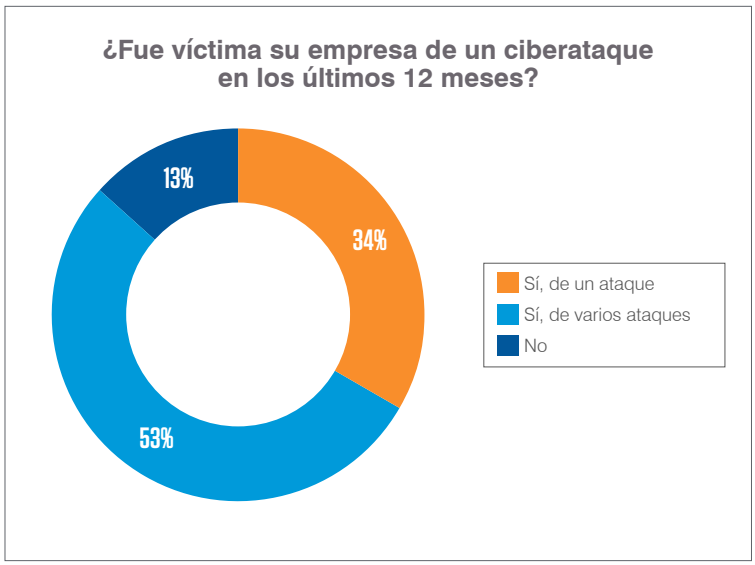
Desde la implicación de los equipos directivos al incremento de la concienciación en materia de ciberseguridad, las empresas españolas están tomando medidas para reforzar sus ciberdefensas.

Este informe pone de relieve estos y otros datos importantes extraídos del estudio.

# RESULTADO 1: EN ESPAÑA, LAS EMPRESAS SE ENFRENTAN A UN PANORAMA DE AMENAZAS DIVERSO

Al igual que sus equivalentes en todo el mundo, las empresas españolas se encuentran bajo la amenaza prácticamente constante de los ciberdelincuentes.

Nuestra encuesta reveló que el 87% de las empresas españolas sufrió al menos un ciberataque en los últimos 12 meses. Más de la mitad (53%) denunció varios incidentes y un tercio (34%) sufrió uno.



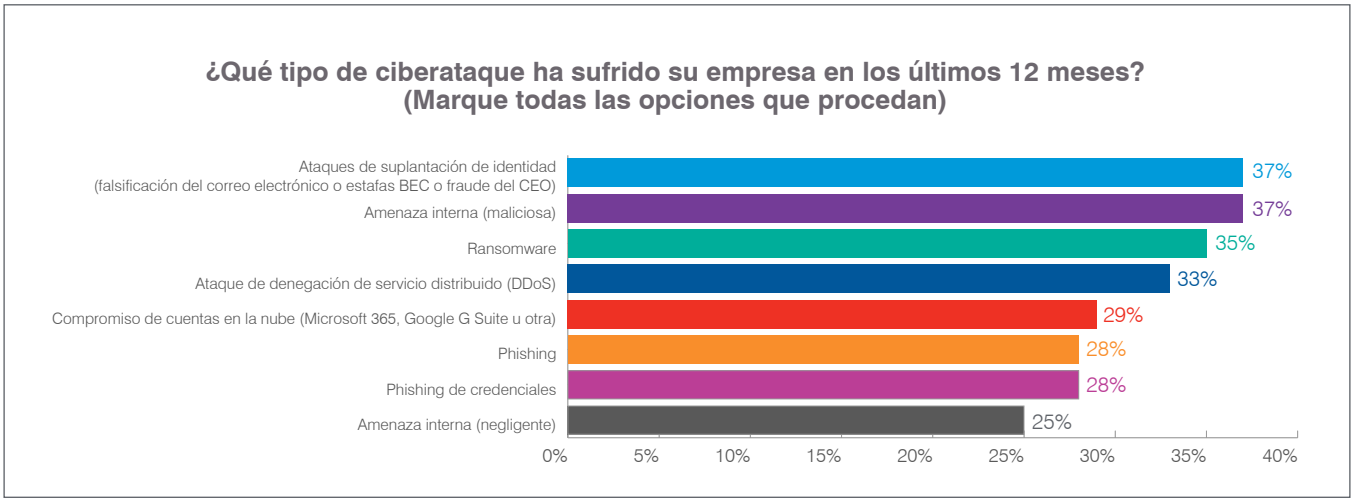

## Los ataques de suplantación de identidad son los más habituales

Los ataques de suplantación de identidad (como las estafas BEC o fraude del CEO) se están convirtiendo rápidamente en uno de los problemas de ciberseguridad que mayor daño económico genera. De hecho, el FBI situó recientemente las pérdidas por dichos ataques en 26.500 millones de dólares en los tres últimos años.

Nuestro estudio descubrió que, en los últimos 12 meses, los ataques de suplantación de identidad fueron uno de los principales métodos utilizados por los ciberdelincuentes en España, llegando a afectar al 37% de las empresas encuestadas. Igual de importantes fueron las amenazas internas maliciosas (37%), seguidas por el ransomware (35%) y los ataques DDoS (33%).

Los ciberdelincuentes utilizan cada vez más credenciales comprometidas para acceder a cuentas de correo electrónico, información sensible y sistemas corporativos. Para conseguirlas, a menudo recurren a ataques de phishing por correo electrónico, un método que sigue siendo alarmantemente eficaz.

El estudio de Proofpoint ha revelado que casi la cuarta parte de las personas que recibe un mensaje de phishing lo termina abriendo, y más del 10% admitió haber hecho clic en los enlaces maliciosos que incluían.

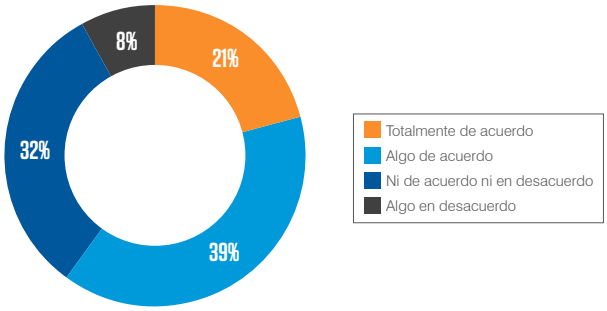


# RESULTADO 2: LA IMPOSICIÓN DEL TELETRABAJO INTRODUCE NUEVOS DESAFÍOS PARA LOS EQUIPOS DE CIBERSEGURIDAD

La migración masiva al teletrabajo como reacción a la pandemia mundial de COVID-19 ha aumentado la presión sobre los equipos de ciberseguridad. Encargados de defender una superficie de ataque más grande y compleja, muchos admiten que tienen dificultades para hacer posible la transición.

Poco más de un quinto (21%) de los CSO/CISOs en España está totalmente de acuerdo en que los empleados están bien equipados para el teletrabajo, y más de un tercio (39%) afirma estar algo de acuerdo.

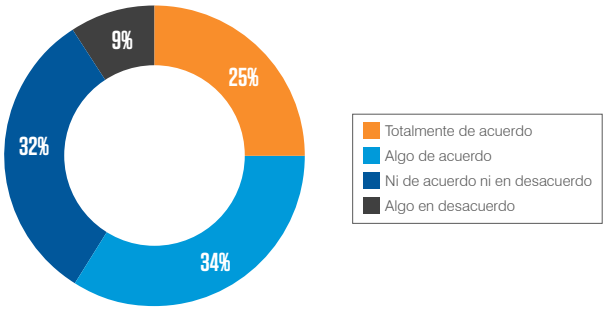
**En qué medida está de acuerdo o en desacuerdo con la siguiente afirmación: Nuestros empleados están adecuadamente equipados para el teletrabajo**




Y no son solo los usuarios los que están poco preparados. La nueva plantilla distribuida también ha puesto en evidencia sistemas y aplicaciones mal protegidos.

Más de la mitad de los CSOs y CISOs de España (59%) coinciden en afirmar que el cambio al teletrabajo ha vuelto obsoletos los sistemas y aplicaciones a la hora de defenderse de las ciberamenazas actuales.

**El cambio al teletrabajo ha vuelto obsoletos nuestros sistemas y aplicaciones de defensa contra las ciberamenazas actuales**

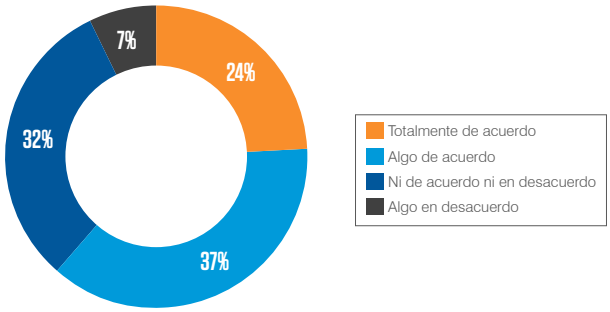


## Los ciberdelincuentes están aprovechándose de plantillas de trabajadores vulnerables

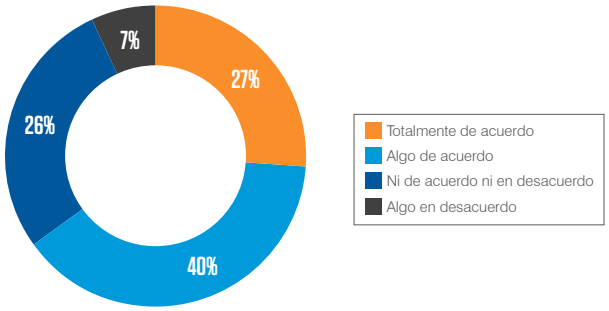
El desafío que supone garantizar unas ciberdefensas adecuadas con plantillas de teletrabajadores más amplias no ha pasado desapercibido para los ciberdelincuentes. Muchos también utilizan intensamente los timos relacionados con el coronavirus para apoderarse de credenciales y otra información confidencial de víctimas desprevenidas.

A la pregunta de si habían observado un aumento en las tentativas de ataques de phishing desde la implementación de una política de teletrabajo, casi dos tercios de los CSO/CISOs (61%) afirmaron que sí. Solo el 7% no estaba de acuerdo.

**Hemos observado más intentos de ataques de phishing desde la implementación de una política de teletrabajo generalizado debido a la pandemia de COVID-19**




**La adopción del teletrabajo ha vuelto más vulnerable a nuestra empresa frente a ciberataques**




Una mayor superficie de ataque, un número creciente de ataques y una plantilla mal equipada ha generado entre las empresas españolas una sensación de mayor vulnerabilidad.

Más de dos tercios (67%) de los CSOs y CISOs de España están de acuerdo en que la implementación de una política de teletrabajo los ha vuelto más vulnerables a ciberataques, y solo un 7% piensa de manera diferente.

En esta línea, el 60% admite que el aumento del teletrabajo ha debilitado sus defensas. Solo el 6% cree que esta afirmación no se ajusta a la realidad.

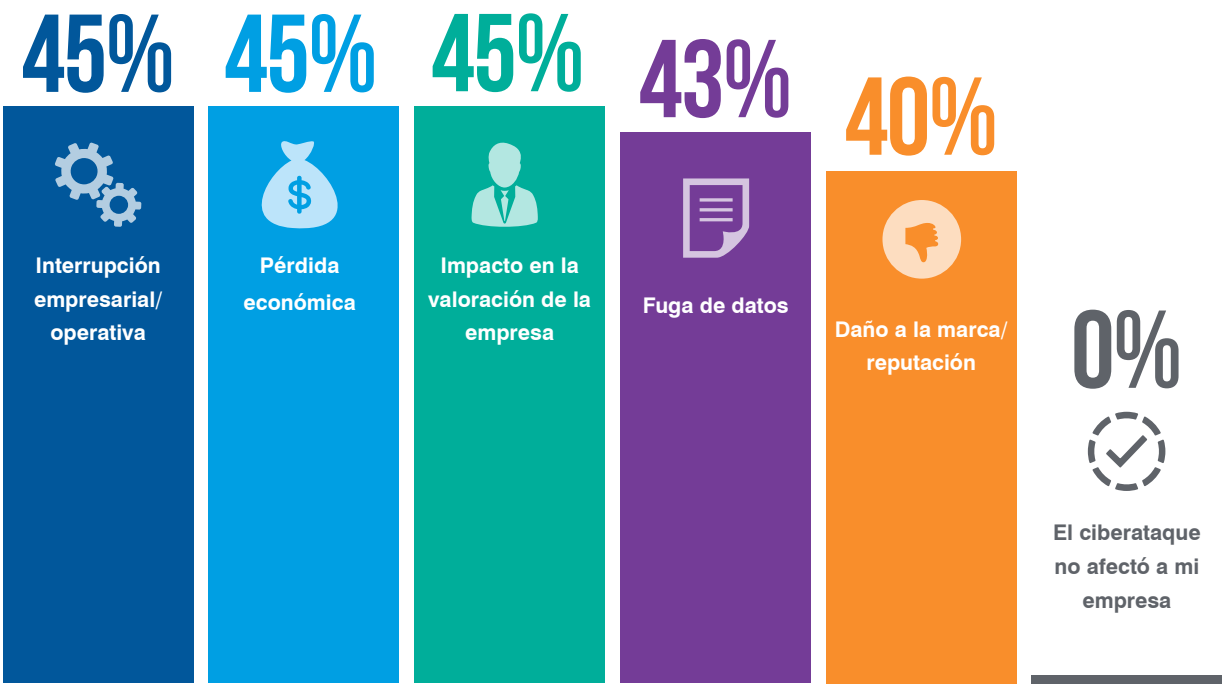
# RESULTADO 3: LA INTERRUPCIÓN DE LAS OPERACIONES Y LAS PÉRDIDAS ECONÓMICAS SON LAS PRINCIPALES CONSECUENCIAS DE LOS CIBERATAQUES

Los ciberataques pueden tener consecuencias devastadoras para las empresas que los sufren. El Foro Económico Mundial calcula que, entre 2019 y 2023, estarán en riesgo 5,2 billones de dólares de valor mundial por la actividad de los ciberdelincuentes.

Esas pérdidas se deben a varias razones: pérdida de ingresos, tiempo de inactividad, costes jurídicos, indemnizaciones y reparaciones, daño en el valor de la marca, etc.

Nuestra encuesta reveló que casi la mitad (45%) de los CSOs y CISOs españoles menciona la interrupción de la actividad, las pérdidas económicas y el impacto en la valoración de la empresa como la principal consecuencia de un ciberataque (un 45% en todos los casos), seguidas de las fugas de datos (43%) y el daño reputacional (40%).

**Si las hubo, ¿cuáles fueron las consecuencias para su empresa tras sufrir un ciberataque? (Marque todas las opciones que procedan)**



# RESULTADO 4: LAS EMPRESAS ESPAÑOLAS SON CONSCIENTES DE LOS RIESGOS A LOS QUE SE ENFRENTAN, PERO AUN ASÍ TIENEN LA SENSACIÓN DE ESTAR POCO PREPARADAS

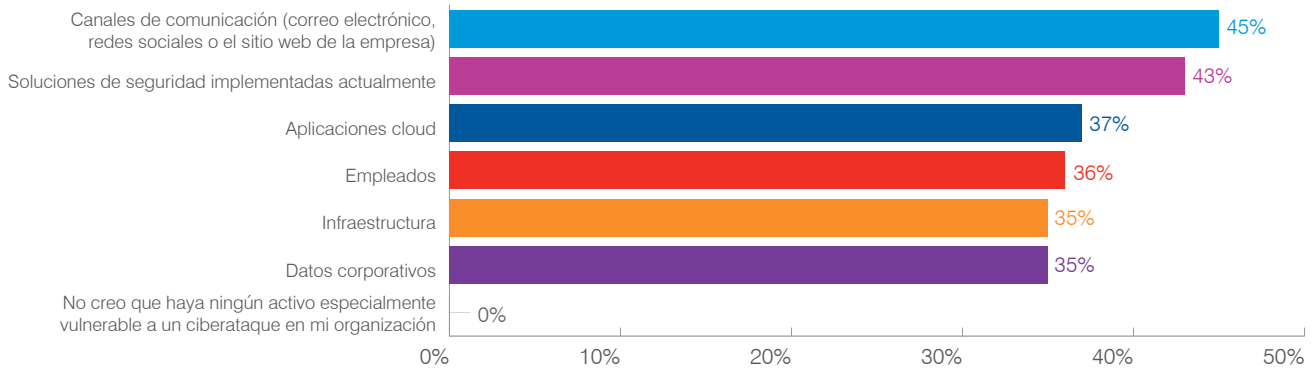
Las empresas españolas son plenamente conscientes de los riesgos a los que se enfrentan en el amplio panorama de ciberseguridad moderno y saben que los cibercriminales están atacando sus negocios.

Casi la mitad (45%) identifica correctamente que los canales de comunicación, como el correo electrónico o las redes sociales, son sus vectores de ataque potencialmente más vulnerables. Las soluciones de seguridad (43%), las aplicaciones en la nube (37%) y los empleados (36%) se encuentran entre los otros recursos considerados más vulnerables por los CSOs y CISOs españoles.

Los CSOs y CISOs manifiestan cada vez más sufrir estos ataques, y un 64% reconoce haber observado un aumento respecto al año anterior.

*Solo el 23% de las organizaciones cree firmemente que están preparadas para un ciberataque*

**¿Qué activos considera que serían los más vulnerables frente a un ciberataque dentro de su organización? (Marque un máximo de 3)**




Si bien resulta alentador que en España los líderes de TI muestren ese nivel de conocimiento de los riesgos y desafíos a los que se enfrentan, sorprende la falta de preocupación entre los directivos sobre el nivel de seguridad de sus organizaciones. Solo un 20% de los CSOs y CISOs coincide plenamente en que la ciberseguridad ha sido una preocupación de nivel directivo para la empresa en 2020, a pesar de que solo el 23% cree firmemente que su organización está preparada para un ciberataque.

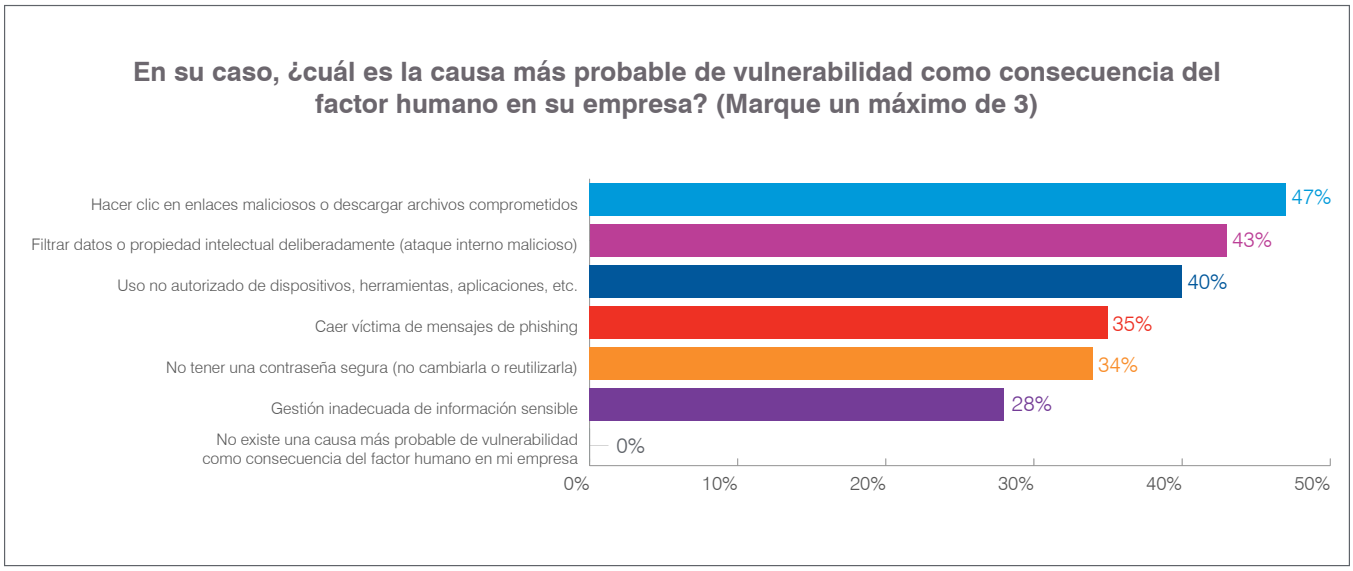
**¿En qué medida está de acuerdo o en desacuerdo con las siguientes afirmaciones?**

| | Totalmente de acuerdo | Algo de acuerdo | Ni de acuerdo ni en desacuerdo | Algo en desacuerdo | Totalmente en desacuerdo |
|---|---|---|---|---|---|
| Nuestra empresa está preparada para un ciberataque | 23% | 34% | 35% | 8% | 0% |
| La ciberseguridad es una preocupación de nivel directivo para nuestra empresa en 2020 | 20% | 41% | 32% | 7% | 0% |
| Hemos observado más ciberataques contra nuestra empresa este año | 22% | 42% | 27% | 8% | 1% |
| El aumento del teletrabajo ha debilitado nuestras defensas | 17% | 43% | 35% | 4% | 1% |

# RESULTADO 5: LOS EMPLEADOS NO ESTÁN EQUIPADOS PARA COMBATIR LOS CIBERATAQUES

A pesar de que los usuarios forman la última línea de defensa frente a los ciberataques, entre las plantillas españolas existe falta de conocimiento y concienciación sobre seguridad.

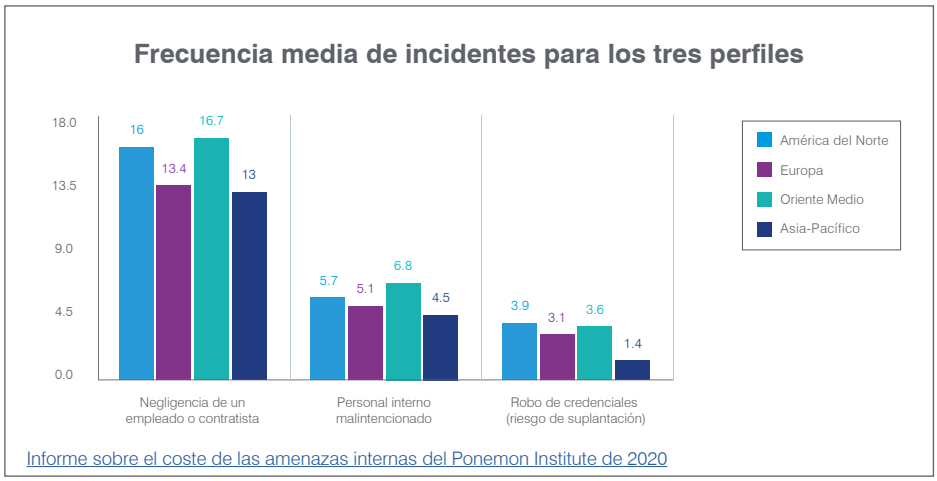
Los comportamientos habituales de los empleados que aumentan el riesgo de ataque de las organizaciones incluyen hacer clic en enlaces maliciosos (47%), algo que el 10% de los usuarios admite hacer, seguido de los ataques internos maliciosos (43%), el uso no autorizado de dispositivos y aplicaciones (40%), caer víctima del phishing (35%) y una deficiente higiene de contraseñas (34%).




## Las amenazas internas van en aumento

Resulta sorprendente que casi la mitad de las empresas españolas afirme que la filtración de datos o propiedad intelectual de forma deliberada (también conocida como amenaza interna maliciosa) pone en riesgo a su empresa.

Esto es un problema global. Las amenazas internas son una preocupación creciente para las empresas, con un número de incidentes que ha aumentado un sorprendente 47% en tan solo dos años.

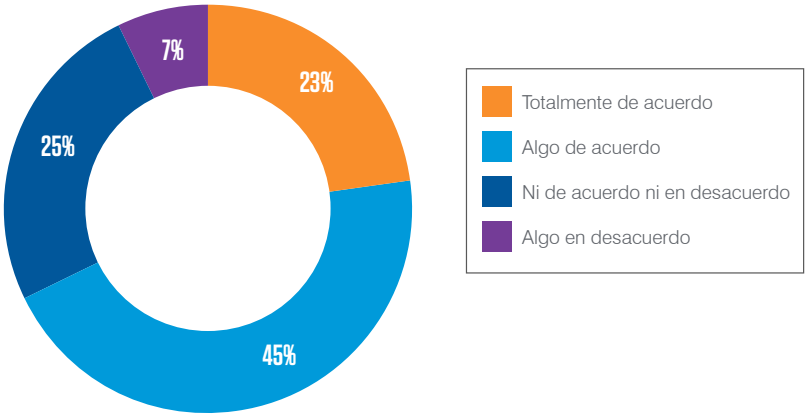



El informe sobre el coste de las amenazas internas del Ponemon Institute de 2020 pone de relieve que las empresas europeas sufren un nivel elevado de negligencia de contratistas, amenazas internas maliciosas y robo de credenciales.

## La concienciación de los empleados sobre ciberseguridad, en el punto de mira

Las personas son a menudo la última línea de ciberdefensa de una organización y los CSOs y CISOs españoles son absolutamente conscientes de esta realidad. Más de dos tercios (68%) creen que, a pesar del resto de protecciones de seguridad, son el error humano o la falta de concienciación en materia de ciberseguridad las que presentan el riesgo más importante para las organizaciones.

**No importa cuáles sean las soluciones de ciberseguridad implementadas, el error humano o la falta de concienciación sobre ciberseguridad (por empleados o terceros dentro de mi ecosistema) son el mayor riesgo para mi empresa**



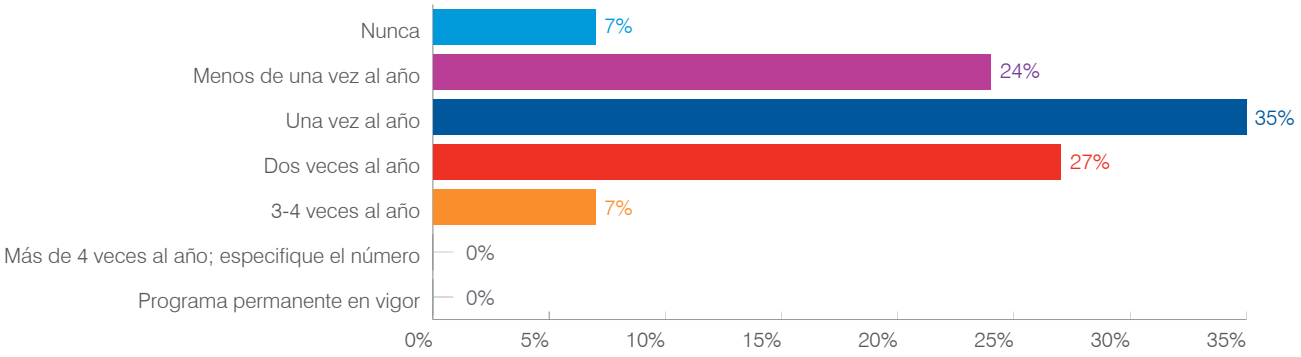

Aunque los líderes de TI españoles son conscientes de los riesgos que pueden suponer los empleados para sus empresas, no son conscientes de quiénes son las personas más atacadas en el seno de la organización. A la pregunta de si sabían quiénes eran los empleados de riesgo en su organización, más de la mitad (55%) afirmaba desconocer ese dato.

Sin embargo, este nivel de conocimiento no se refleja en los programas de formación de las organizaciones (o en su ausencia) para concienciar en materia de ciberseguridad. A pesar de enfrentarse a un panorama de amenazas muy dinámico, casi todos (93%) admitieron ofrecer formación a sus empleados sobre las mejores prácticas de ciberseguridad solo dos veces al año o menos, y solo el 7% ponía en práctica un programa completo tres veces al año o más.

Sin embargo, resulta esperanzador que un buen número de empresas esté adaptando su formación para concienciar en materia de ciberseguridad en línea con las presiones asociadas a la pandemia actual, y un 22% afirma que ha ofrecido a los empleados formación adicional sobre cómo protegerse mientras teletrabajan.

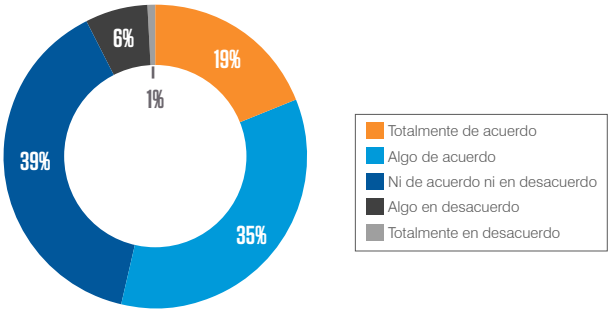
Una formación regular y completa es fundamental para estar ciberprotegido. Todos los programas deben revisarse de manera continua para garantizar que siguen siendo relevantes y van al ritmo que marca un panorama de amenazas dinámico. La formación y concienciación de los empleados a menudo marca la diferencia entre una tentativa de ataque y un ataque con éxito. La incapacidad para implementar y revisar dichos programas expone peligrosamente a las empresas.

**De media, ¿con qué frecuencia ofrece formación a sus empleados sobre concienciación en materia de ciberseguridad/mejores prácticas?**

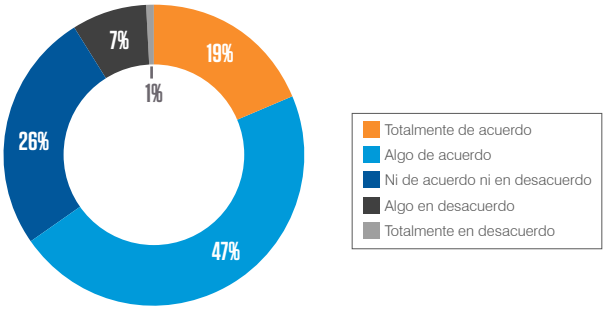



Este es un motivo de preocupación para muchos líderes de TI españoles. Más de la mitad (54%) afirma que el programa de formación en ciberseguridad de su empresa debe mejorarse para ser eficaz. Desafortunadamente, una mayoría todavía más amplia (66%) cree que la falta de tiempo y recursos es el mayor obstáculo para conseguir el objetivo de mejorar la concienciación sobre ciberseguridad de los empleados.

**Nuestro programa de formación para concienciar en materia de ciberseguridad debe mejorarse para ser más eficaz**




**La falta de tiempo/recursos es el mayor obstáculo para disponer de un programa de concienciación en materia de ciberseguridad dentro de mi empresa**



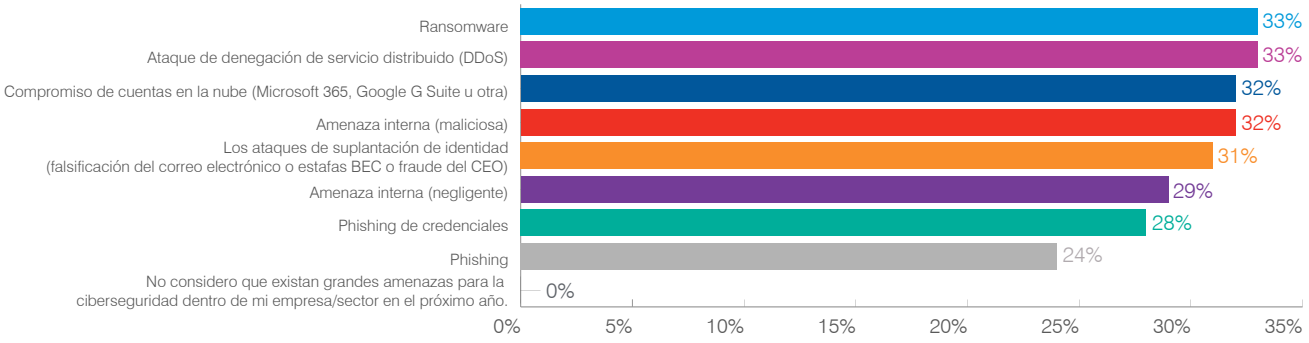
# RESULTADO 6: EL FUTURO DE LOS RIESGOS DE CIBERSEGURIDAD EN ESPAÑA ESTÁ CAMBIANDO

## Vectores de ataque dinámicos y ciberestrategias adaptadas

Con vistas a los próximos dos años, un tercio (33%) de los encuestados piensa que los ataques de ransomware y DDoS se encontrarán entre las mayores ciberamenazas a las que se enfrentarán las empresas españolas.

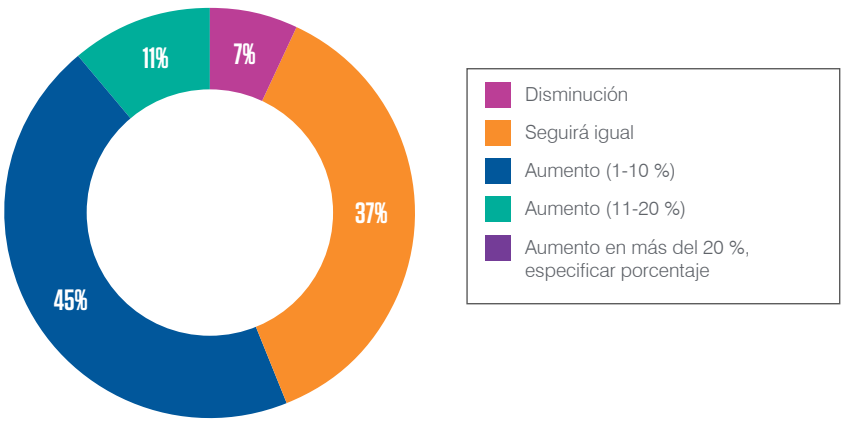
El compromiso de cuentas en la nube (32%), las amenazas internas maliciosas (32%), y los ataques de suplantación de identidad (31%) también se prevé que constituyan una amenaza permanente en los próximos años.

**En su caso, ¿cuáles considera que son las mayores amenazas para la ciberseguridad dentro de su organización en los próximos 2 años? (Marque un máximo de 3)**



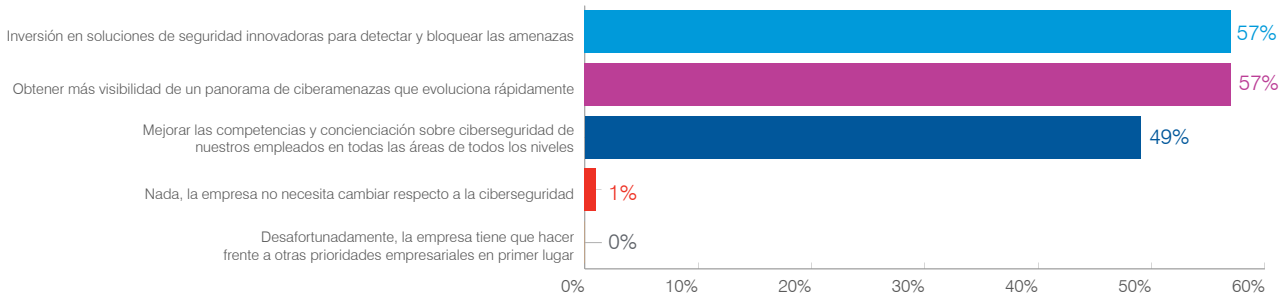

Este cambiante panorama de amenazas aboca a un cambio en las ciberdefensas y a la reevaluación permanente de las prioridades estratégicas de una organización. En esta línea, más de la mitad (56%) de los CSOs y CISOs españoles espera que se produzca un aumento de la inversión en ciberseguridad para apoyar esta estrategia de seguridad.

**¿Cómo espera que evolucione su presupuesto de ciberseguridad en los próximos dos años?**




Se espera que la inversión se centre en varias áreas. Soluciones de seguridad innovadoras para detectar y bloquear amenazas encabezan la lista de prioridades (57%), seguidas en igual medida por una mayor visibilidad del panorama de ciberseguridad dinámico (57%), y mejoras en las competencias y concienciación en materia de ciberseguridad de los empleados (49%).

**En términos de ciberseguridad, ¿qué cambios espera que se produzcan en el seno de sus empresas en los próximos dos años? (Marque un máximo de 3)**




# CONCLUSIONES

Independientemente de los métodos de ataque (correo electrónico, aplicaciones cloud, la web, las redes sociales, etc.), los ciberdelincuentes siguen aprovechando el factor humano.

Ya se trate de impostores que se hacen pasar por compañeros de confianza o de mensajes de correo electrónico de phishing convincentes y enlaces maliciosos, son los usuarios los que se encuentran en la primera línea de batalla contra los ciberdelincuentes.

Esa es la razón por la que resulta imprescindible que las empresas adopten una estrategia centrada en las personas. Esto empieza por identificar a los usuarios más vulnerables y garantizar que cuentan con los conocimientos y las herramientas necesarias para defender su empresa.

Junto con las soluciones técnicas y los controles, la estrategia de ciberseguridad debe tener en el centro un programa de formación completo. La formación debe ser regular, completa, adaptable y cubrir una amplia variedad de temas, desde las motivaciones y las mecánicas de las ciberamenazas a cómo comportamientos tan simples como reutilizar contraseñas y no proteger adecuadamente los datos pueden aumentar la probabilidad de que un ataque consiga su objetivo.

Los ciberdelincuentes tienen un objetivo claro, y perfeccionan sin descanso sus habilidades y técnicas. Si no haces lo mismo, solo puede haber un ganador.

> *"Los ciberdelincuentes tiene un objetivo claro y mejoran constantemente sus habilidades y técnicas. Si no haces lo mismo, solo puede haber un ganador".*
>
> **Fernando Anaya, director regional de Proofpoint para España**

Todos los datos, excepto que se indique lo contrario, hacen referencia a la investigación llevada a cabo por Censuswide entre 150 CISOs/CSOs en España, en octubre de 2020. Censuswide acata y emplea miembros de la Market Research Society, que se basa en los principios ESOMAR.

proofpoint®

## Para obtener más información sobre cómo puede ayudar Proofpoint a su empresa, visite www.proofpoint.com/es.

**ACERCA DE PROOFPOINT**

Proofpoint, Inc. (NASDAQ:PFPT) es una compañía líder en ciberseguridad y cumplimiento normativo que protege los activos más importantes y de mayor riesgo para organizaciones y empresas: las personas. Gracias a una suite integrada de soluciones basadas en cloud, Proofpoint ayuda a empresas de todo el mundo a detener las amenazas dirigidas a salvaguardar sus datos y a hacer a los usuarios más resilientes frente a ciberataques. Compañías líderes de todos los tamaños, entre las que se encuentran más de la mitad de las incluidas en el Fortune 1000, confían en las soluciones de Proofpoint de seguridad centradas en las personas y de cumplimiento de normativas para mitigar los riesgos críticos en sus sistemas de correo electrónico, cloud, redes sociales y web. Más información en https://www.proofpoint.com/es.