

# La mitad de las empresas carece de un plan integral de ciberseguridad

**ENCUESTA GLOBAL DE PwC/** La mayor parte de organizaciones españolas asume que sufrirá ataques cibernéticos pero no cuenta aún con procedimientos establecidos para responder a los 'hackers'.

Expansión. Madrid

La seguridad plena no existe, pero es responsabilidad de las organizaciones tratar de minimizar los riesgos o el impacto de un eventual ataque cibernético. A este respecto, la consultora PwC ha llevado a cabo una macroencuesta global a más de 9.500 directivos (más de 300 en España) en la que evalúa el nivel de protección de las empresas ante incidentes de seguridad.

Las conclusiones de la encuesta evidencian que mejora la sensibilización hacia los riesgos que entraña la digitalización de las organizaciones, pero que aún queda mucho por hacer en la práctica. En España, por ejemplo, el 67,7% de los directivos encuestados considera "probable" o "muy probable" que sus empresas vayan a ser objeto del algún tipo de ciberataque en los próximos meses.

Y, sin embargo, el 49% de los directivos españoles entrevistados (el 44% en el mundo) reconoce que sus compañías carecen de una estrategia integral de seguridad, el 53% no cuenta con programas de formación para los empleados y el 55% no dispone de procedimientos previamente establecidos para responder a los incidentes de seguridad.

El documento de PwC revela que las empresas de todo el mundo sufren, de media, 3,4 incidentes de seguridad al año, que generan unas pérdidas de 4,8 millones de dólares. La pérdida de datos sensibles, los daños en activos físicos de la compañía, el deterioro en la

**Las empresas sufren, de media, 3,4 incidentes de seguridad al año, según PwC**

**Estos ataques obligan a parar las operaciones un promedio de 17 horas al año**

**Casi la mitad de los ciberataques son realizados por trabajadores o ex empleados**

**La protección de las organizaciones se complica con la proliferación del Internet de las Cosas**

calidad de sus productos y la suspensión de sus operaciones son, por este orden, las principales consecuencias de los ciberataques para las empresas (ver gráfico adjunto).

Según la encuesta, las empresas españolas se ven obligadas a parar sus operaciones, de media, 17 horas al año como consecuencia de los ataques informáticos.

**Internet de las Cosas**

El desafío se complica a medida que las organizaciones integran un número cada vez mayor de aparatos conectados, ya sean dispositivos personales con acceso a las apli-

## OBJETIVO: REDUCIR EL RIESGO

> ¿Qué impacto tiene un ciberataque para las empresas?



> ¿Cuáles son las prioridades de las empresas españolas en materia de ciberseguridad para los próximos doce meses?



Fuente: Encuesta Mundial de Seguridad de la Información 2018. PwC

Expansión

caciones empresariales, u objetos a los que se les añaden sensores o chips de conectividad. Es lo que se conoce como el Internet de las Cosas (IoT, por sus siglas en inglés).

Los resultados de la citada encuesta de PwC confirman que el IoT y la consiguiente proliferación de dispositivos

interconectados se va a convertir en una de las principales vulnerabilidades de seguridad para las empresas de todo el mundo en el futuro inmediato. En España, por ejemplo, sólo el 34% de los directivos encuestados dice tener una estrategia de seguridad para el Internet de las Cosas.

El estudio concluye asimismo que, en España, aproximadamente el 47% de los ciberataques que tienen su origen dentro de la compañía son realizados por empleados o ex empleados. Y una proporción algo menor (del 40,7%), por proveedores. En cuanto a aquellos de origen externo, el 28,2% son realizados por competidores, el 25,4% por organizaciones criminales y un 17,5% por activistas y ciberactivistas.

**Prioridades**

En este contexto, ¿cuáles son las principales prioridades en materia de ciberseguridad de las empresas españolas en el corto y en el medio plazo? En los próximos doce meses, según el informe, estas prioridades pasan por combatir los ataques que se producen desde dentro de la organización; garantizar la seguridad de los dispositivos móviles; monitorizar los sistemas y redes de la compañía; mejorar la gestión de identidades; y aumentar la conciencia y la formación de los empleados sobre los riesgos informáticos a los que se enfrentan las empresas.

En el medio plazo –a cinco años vista–, la principal preocupación se centra en la capacidad de las compañías para garantizar la seguridad de los servicios y funciones que, cada vez en mayor medida, tienen previsto almacenar en la nube. El 50% de las empresas encuestadas en España prevé llevar a la nube información sensible para su organización en los próximos doce a die-

## Ideas clave

- El mejor modo de prevenir ataques informáticos es contar con un plan integral de ciberseguridad, apoyado en una auditoría interna de los activos y su nivel de criticidad, y supeditado a objetivos de negocio.

- Ese plan se hace más necesario aún a medida que el perímetro de la seguridad de las organizaciones se amplía por 'culpa' de la movilidad, el 'cloud' o el Internet de las Cosas.

- El eslabón más débil son los propios empleados de las empresas. La sensibilización es fundamental, si bien menos de la mitad de las empresas cuentan con programas de formación.

- La seguridad debe estar presente desde el mismo diseño de nuevas soluciones digitales.

ciocho meses.

Si hablamos de tecnología, las inversiones de las compañías españolas entrevistadas se van a centrar en soluciones de identificación biométrica, en herramientas de monitorización y de detección de códigos maliciosos y en aquellas destinadas a la detección de intrusiones.

Finalmente, el estudio insiste en que el factor impulsor de la inversión en ciberseguridad sigue siendo el profundo proceso de digitalización al que se ha sometido el mundo de los negocios. Así lo asegura el 59% de los directivos y responsables de IT de todo el mundo entrevistados en el informe y el 61% de los pertenecientes a empresas españolas.

## “Integrar la seguridad en el diseño de las soluciones es lo más económico y efectivo”

Elena Arrieta. Madrid

PwC apuesta por una visión integral de la seguridad, que ha de estar apoyada en una estrategia corporativa que marque los objetivos, las prioridades y el nivel de "riesgo aceptable" de cada organización.

Para esta consultora, que actúa como socio en la auditoría y concepción de ese necesario plan integral de seguridad de las empresas, la ciberseguridad debe estar su-

peditada a objetivos de negocio. Además, aunque incide en la necesidad de incrementar el presupuesto destinado a seguridad informática, PwC recalca el concepto de "inversión razonable". "No siempre es cuestión de tener la tecnología más cool o más cara. Resulta más útil realizar un análisis que permita saber dónde mitiga más el riesgo una determinada herramienta", expone Jesús Romero, responsable de Soluciones de Segu-

ridad de Negocio de PwC.

Para Romero, es indispensable que en el desarrollo de nuevas soluciones digitales, ya sea una app, un portal de comercio electrónico o un proyecto de Internet de las Cosas, se tenga en cuenta la ciberseguridad "desde la fase de diseño. Sale mucho más económico y, además, es infinitamente más efectivo que actuar a posteriori".

Las nuevas tendencias tecnológicas como el cloud, el big

data y el Internet de las Cosas "aportan numerosos beneficios en términos de negocio, agilidad y eficiencia, pero amplían el mapa de riesgos operativos de las compañías", advierte este experto.

Por suerte, "las empresas son cada vez más conscientes de la necesidad de proteger su información", en parte a causa de la trascendencia que han tenido sucesos recientes como el macroataque de ransomware Wannacry.



Jesús Romero, socio responsable de Soluciones de Seguridad de Negocio de la consultora PwC.