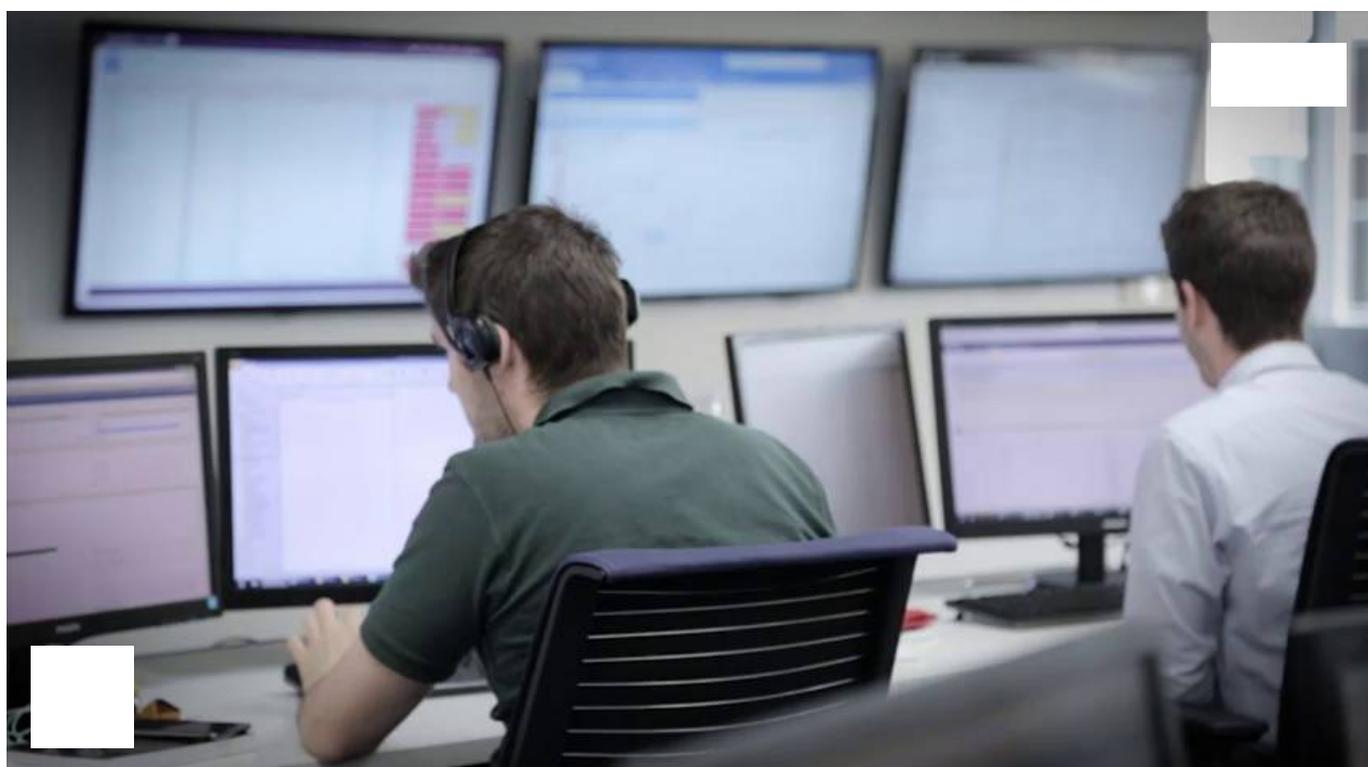


# El gran negocio de la ciberseguridad: 1.000 millones para proteger tus datos

El gasto de las empresas españolas en barreras informáticas contra los fraudes no para de aumentar y aumentará un 36% hasta 2019

LAURA DELLE FEMMINE

Madrid - 6 JUN 2016 - 20:54 CEST



CyberSOC de Deloitte, en Madrid. / VIDEO: CARLOS MARTÍNEZ

## MÁS INFORMACIÓN

Un 'hacker' roba y pone en venta 360 millones de cuentas de MySpace

“En 2020 ya no podremos proteger nuestras redes frente

Adolfo Pedriza no es un directivo cualquiera. Unas pequeñas calaveras piratas, entramadas en una corbata de fondo oscuro, quitan solemnidad a su traje y delatan su pasado. El actual director de operaciones del [CyberSOC de la consultora Deloitte](#) —centro especializado en la gestión de ciberataques— procede del *hacking ético*, el arte de destripar los sistemas

a los ataques”

---

Desarticulada una red que ‘hackeaba’ cuentas de altos directivos de empresa

---

informáticos para descubrir sus vulnerabilidades y arreglarlas. “Detectamos unos 30.000 ataques al mes dirigidos a nuestros clientes”, comenta, y asegura que esta cifra no ha parado de crecer. Por ello, las empresas están apostando fuerte por la [ciberseguridad](#), un negocio que en 2015 movió más de 60.000 millones de euros en el mundo y que se estima alcance los 150.000 millones en 2020, según las previsiones de la firma de análisis Gartner.

También en España, ante un aumento de los incidentes de ciberseguridad del 200% el año pasado, las empresas se están dando cuenta de que es vital apostar por la protección informática. En 2014, este capítulo de gasto rebasó los 700 millones de euros, y se estima que en 2019 supere los 1.000 millones, según el último informe del [Observatorio Nacional de las Telecomunicaciones y de la Sociedad de la Información](#) y el [Instituto Nacional de Ciberseguridad \(Incibe\)](#).

Miguel Rego, director general de Incibe, apunta sin embargo a que la inversión en ciberseguridad en España podría, ya en 2015, haber alcanzado los 1.000 millones de euros. “Este negocio no está clasificado como actividad económica y es difícil recopilar los datos”. Por otro lado, lamenta que faltan profesionales para satisfacer las necesidades del mercado y que las empresas todavía no asignan a la seguridad informática el peso que se merece.

## FALTA DE CONCIENCIACIÓN

El principal objetivo de los ciberataques es el dinero, y los ciudadanos son las presas más indefensas. Sin embargo, no parece haber cundido en el imaginario colectivo la necesidad de proteger nuestros datos. “La tecnología no nace segura y las empresas no se lo toman en serio”, lamenta Raúl Siles, fundador y analista de seguridad de DinoSec.

Adolfo Hernández, subdirector de THIBER, the cybersecurity think tank, explica que solo en algunas grandes compañías existe un responsable de ciberseguridad que reporta directamente a la dirección general, síntoma de que falta mucho por

hacer. Además, los escasos recursos con los que suelen contar las pymes, que en España copan más del 90% del tejido empresarial, hacen el sistema aún más endeble.

Lo que sí está claro es que es necesario pisar el acelerador porque el futuro ya ha llegado. El [ataque que devastó al gigante tecnológico Sony Pictures](#) en 2014 o los recientes [asaltos a la plataforma bancaria SWIFT](#) son solo la punta del iceberg: en tan solo cinco años, el número de [dispositivos conectados a la Red](#) cuadruplicará la población mundial y alcanzará los 28.000 millones de aparatos, según el *Ericsson Mobility Report*. “La nevera se encargará de hacerte la compra y la televisión grabará automáticamente los programas que más te gustan”, ejemplifica Gianluca D'Antonio, CISO (Chief Information Security Officer, en inglés) de FCC y presidente de [ISMS Forum Spain](#), Asociación Española para el Fomento de la Seguridad de la Información.

El problema es que todas las monedas tienen doble cara: lo que nace para facilitarnos la vida puede a la vez destruirla. “A través de las redes, cualquiera se te puede meter en casa y generar un incendio”, presagia D'Antonio. En este mundo conectado, la responsabilidad de las empresas es cada vez más delicada, y los legisladores ya están trabajando para evitar escenarios apocalípticos.

El pasado mayo, la UE publicó un reglamento —que se espera entre en vigor en 2018— relativo al tratamiento y circulación de los datos de las personas físicas, que obliga a poner la ciberseguridad en pole position entre las prioridades empresariales. En particular, impone que todas las compañías que operen en el Viejo Continente cumplan con la ley europea y notifiquen eventuales incidencias y fugas de datos —lo que se conoce como data breach notification, ya obligatorio en otros países— a los usuarios afectados y a la autoridad competente. “El problema es que las empresas no están acostumbradas ni quieren hacerlo, porque saben que notificar un ataque tiene un coste reputacional brutal”, dice Carlos Saiz, [socio de Ecix](#) y vicepresidente de ISMS Forum Spain.

## El tabú de la seguridad

Todos los expertos coinciden en que las empresas evitan presumir de sus medidas de ciberseguridad. “Y no es solo un fenómeno español”, señala Eden Shochat, experto de la [Fundación Innovación Bankinter](#). “Estamos mucho más orgullosos del coche que compramos que del seguro que hemos contratado para protegerlo”, ejemplifica.

Según D’Antonio, la razón está en el miedo que tienen las compañías a recibir más ataques tras desvelar sus esfuerzos en seguridad. La contrapartida, sin embargo, es que se postergue aún más la concienciación acerca de un asunto que nos afecta a todos. “Estamos en la cultura de ‘a mí esto no me va a pasar’”, lamenta Rosa Díaz, directora general de [Panda Security](#) para España. “Pero este mundo es digital”.

---

### ARCHIVADO EN:

Incibe · Ontsi · Ministerio del Interior · Usuarios internet · Ataques informáticos  
· Seguridad internet · Ministerios · Empresas públicas · Sector público · Internet

### CONTENIDO PATROCINADO



**Una estufa de combustión limpia para luchar contra**

(CHIVAS, THE VENTURE: WIN THE RIGHT WAY)



**Proyecto la Chira en Lima para recuperar una zona**

(ACCIONA)



**Trabajo después de los 50: ¡Reinvéntate y disfruta!**

(VICTORIA 50)



**Así tributa un plan de pensiones**

(EN NARANJA)

---

### Y ADEMÁS...



**Errejón rescata y hace viral este tuit borrado por el PP**

(HUFFINGTON POST)



**Google prepara un protocolo de emergencia contra**

(MERISTATION GADGETS)



**“Supe que estaba embarazada y mi marido, delante de**

(CADENA DIAL)



**Intenta suicidarse lanzándose a los leones de un zoo en**

(AS.COM)

recomendado por

© EDICIONES EL PAÍS S.L.

[Contacto](#) | [Venta](#) | [Publicidad](#) | [Aviso legal](#) | [Política cookies](#) | [Mapa](#) | [EL PAÍS en KIOSKOyMÁS](#) | [Índice](#) | [RSS](#) |