



Ciberseguridad en las empresas: en el punto de mira

Las empresas de España y Reino Unido, a la cabeza en el ránking de ciberataques recibidos en los últimos dos años

Debemos concebir la ciberseguridad como algo global: tanto a nivel de gran empresa, pasando por las pequeñas y medianas, como a nivel usuario. En la última encuesta de [Kaspersky Lab](#), más de la mitad de las compañías europeas se enfrentaron a varios ciberataques y a sus consecuencias: vulnerabilidad en los datos de sus clientes, pérdida de dichos datos e interrupciones en sus servicios.

Por esto, y por la gran cantidad de información confidencial existente en el entorno empresarial, se hace necesario y vital la prevención en estos ciberataques. Empresas como [Dolbuck](#), con su lema "[La ciberseguridad comienza con la prevención](#)", son especialistas en la previsión de estos ataques informáticos con sus servicios de auditorías internas y externas de sistemas, [análisis de amenazas](#) y [peritajes informáticos \(análisis forenses\)](#)



Sólo en el mes de marzo de 2019, encontramos numerosos ciberataques a

grandes empresas. ASUS se vio afectada por un malware firmado digitalmente que funcionó durante al menos cinco meses, y vio como varios servidores eran interrumpidos y, por tanto, miles de usuarios habían quedado afectados. Hydro, el gigante noruego de aluminio, cuyos sistemas se han visto afectados a nivel global. Nadie está a salvo de los cibercriminales: en [Forbes](#) apuntan hacia la ciberseguridad como “un riesgo del negocio, no solo un problema IT”. Otro ejemplo importante, si bien es menos reciente, es el catastrófico ataque WannaCry que afectó globalmente a Telefónica. ¿Están los profesionales de TI correctamente [formados en ciberseguridad](#)?

A nivel de usuario existen aún más vulnerabilidades: nadie queda exento de los ciberataques. De entre las preocupaciones de los españoles en aspectos de seguridad informática, destacan la usurpación de identidad (pishing), la obtención de información personal, el acceso a los datos bancarios, o el acceso a la biblioteca de imágenes del teléfono móvil. Todo el mundo utiliza un smartphone, o varios; pero prácticamente nadie usa un antivirus para sus teléfonos inteligentes. Por estos motivos, desde [Hardening de Usuarios](#) se busca la [concienciación de los usuarios de Internet](#) en materias de ciberseguridad, como por ejemplo en aspectos del Reglamento General de Protección de Datos (RGPD) o del Esquema Nacional de Seguridad (ENS).

¿Cómo podemos evitar o suavizar las consecuencias de un ciberataque?

Es la pregunta que tanto usuarios de Internet como empresas, independientemente de su tamaño, deben hacerse. La respuesta es sencilla: contratando a profesionales que sepan. Por ello, desde [Dolbuck SL](#) proponemos, primero que todo, el análisis de riesgo y las auditorías pertinentes de sus sitios web y de sus sistemas; y secundariamente, la formación de su personal IT.



Asimismo, esta consultora experta en seguridad tiene entre sus servicios la [certificación de normas ISO 27001](#), la norma internacional para la Gestión de

Seguridad de la Información; esencial como ventaja competitiva para las empresas.

Es un asunto serio: el sector de las finanzas, si bien es el más preparado con diferencia, están en el punto de mira en cuanto a ataques informáticos. Le siguen, de cerca, las pequeñas empresas industriales: sería un auténtico desastre parar la producción durante dos o tres semanas.