NOTAS OBSERVATORIO DE LA DIGITALIZACIÓN FINANCIERA

FUNCAS- 5 de diciembre de 2017 **ODF-Funcas 19/2017**

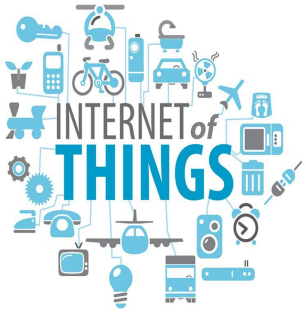
Ciberseguridad en las empresas

El término "Ciberseguridad" hace referencia a la protección de todo lo relacionado con la información e infraestructura computacional de una determinada empresa, grupo de empresas o sector. Es necesaria, básicamente, para preservar la privacidad de la compañía y no compartir información privilegiada o sensible.

Sin embargo, los ataques cibernéticos -que suponen la violación de esta privacidad- han resultado ser uno de los problemas más relevantes y significativos a los que se enfrentan, a menudo, empresas de cualquier tamaño en todo el mundo.

Robo de datos, daños en activos físicos, deterioro en la calidad de los productos, suspensión de operaciones... Éstos son algunos de los tipos de ataques más comunes que sufren globalmente las empresas, y para los cuales se arbitran ciertos controles que limitan su expansión pero todavía no se ha encontrado una solución tajante.

Un elemento que influye de manera significativa en el crecimiento de la preocupación por la ciberseguridad es lo que se conoce como "Internet de las cosas", que hace referencia al número de aparatos conectados por red. Son numerosas las empresas que, sin embargo, no cuentan con un plan estratégico definido para hacer frente a esta creciente amenaza.



Resulta curioso pensar en qué perfil de individuo realiza el ciberataque. Sorprendentemente, casi la mitad son realizados por trabajadores de la empresa (actuales o antiguos), y el resto por organizaciones criminales, activistas o competidores del mismo sector.

¿Qué se puede hacer para aumentar la ciberseguridad y

hacer más difícil la labor de los "hackers"? Trabajar en una mejor gestión de las identidades, monitorizar activamente las redes y sistemas de la empresa, aumentar la conciencia de los empleados con programas de formación e incrementar la seguridad de los smartphones, pueden ser prácticas bastante útiles.

Pero el objetivo debe seguir siendo una mayor coordinación internacional y una estrategia completa de ciberseguridad que haga mínima la incidencia de este tipo de ataques.

En este campo, uno de los grandes éxitos sería la garantía de seguridad de información almacenada en la "nube", ya que su uso es cada vez más extendido tanto corporativamente como para usuarios individuales. El desarrollo de herramientas que faciliten la monitorización y detección de códigos maliciosos e intrusiones debe llegar a todos los ámbitos para que no se genere una "brecha" en ciberseguridad entre aquellos que puedan permitirse sistemas más complejos y los que no.

El campo de las finanzas es particularmente sensible y en él se están realizando esfuerzos ímprobos en materias de seguridad en las comunicaciones y transacciones. En España, existe una estrategia de ciberseguridad nacional –en el marco de la coordinación europea- que presta especial atención a los temas financieros, por su incidencia social. El Consejo Nacional de Ciberseguridad centra sus esfuerzos en mejorar las capacidades de los equipos de respuesta ante incidentes de este tipo en la industria (iniciativa CERTSI), en coordinación con el Mando Conjunto de Ciberdefensa y el Centro Criptológico Nacional.