Transformación digital

Cinco claves para garantizar la seguridad digital en las empresas

Las Tecnologías de la Información y la Comunicación (TIC) nos proporcionan una ventajas que nos ayudan a aumentar la productividad y ser más competitivos, pero también comportan unos riesgos a tener en cuenta

REDACCIÓN

En plena sociedad de las Tecnologías de la Información y la Comunicación (TIC) éstas nos proporcionan unas ventajas que nos ayudan a aumentar la productividad y la competitividad. No obstante, las TIC también comportan una serie de riesgos de seguridad. En el caso de las empresas, según explica Jordi Castellà, director del Departamento de Ingeniería Informática y Matemáticas de la URV y miembro del grupo de investigación CRISES Security and Privacy, recuerda que «estos riesgos van desde el acceso no autorizado a información confidencial, la destrucción o bloqueo de sus datos, o parar su actividad».

Para este experto en seguridad informática, «la incorporación de la ciberseguridad va más allá de instalar un producto u otro de seguridad. La seguridad es un proceso, tiene un ciclo de vida». Además «como las tecnologías y empresas evolucionan hay que volver a empezar con la primera parte del ciclo de vida».

Estos serían, según Jordi Castellà, los pasos a seguir para cubrir el ciclo de ciberseguridad en una empresa:

1.- Estudio de los requisitos de seguridad. Identificar las amenazas y vulnerabilidades de la empresa y para cada una de ellas evaluar su riesgo y nivel de exposición (posibles pérdidas).

2.- Diseño de seguridad. A partir del punto anterior, diseñar un plan de seguridad que incluirá unas políticas de seguridad. Este plan incluiría, entre otros puntos, la formación del personal en seguridad. Todo el personal de la empresa tiene que ser consciente de que son una parte importante para garantizar la seguridad. Por ejemplo, no tienen que apuntar sus contraseñas en un papel y dejarlo a la vista de terceros. También tienen que cerrar la sesión del ordenador si o están trabajando y que desconecten la sesión del servidor cuando hayan acabado la actividad que estaban haciendo.

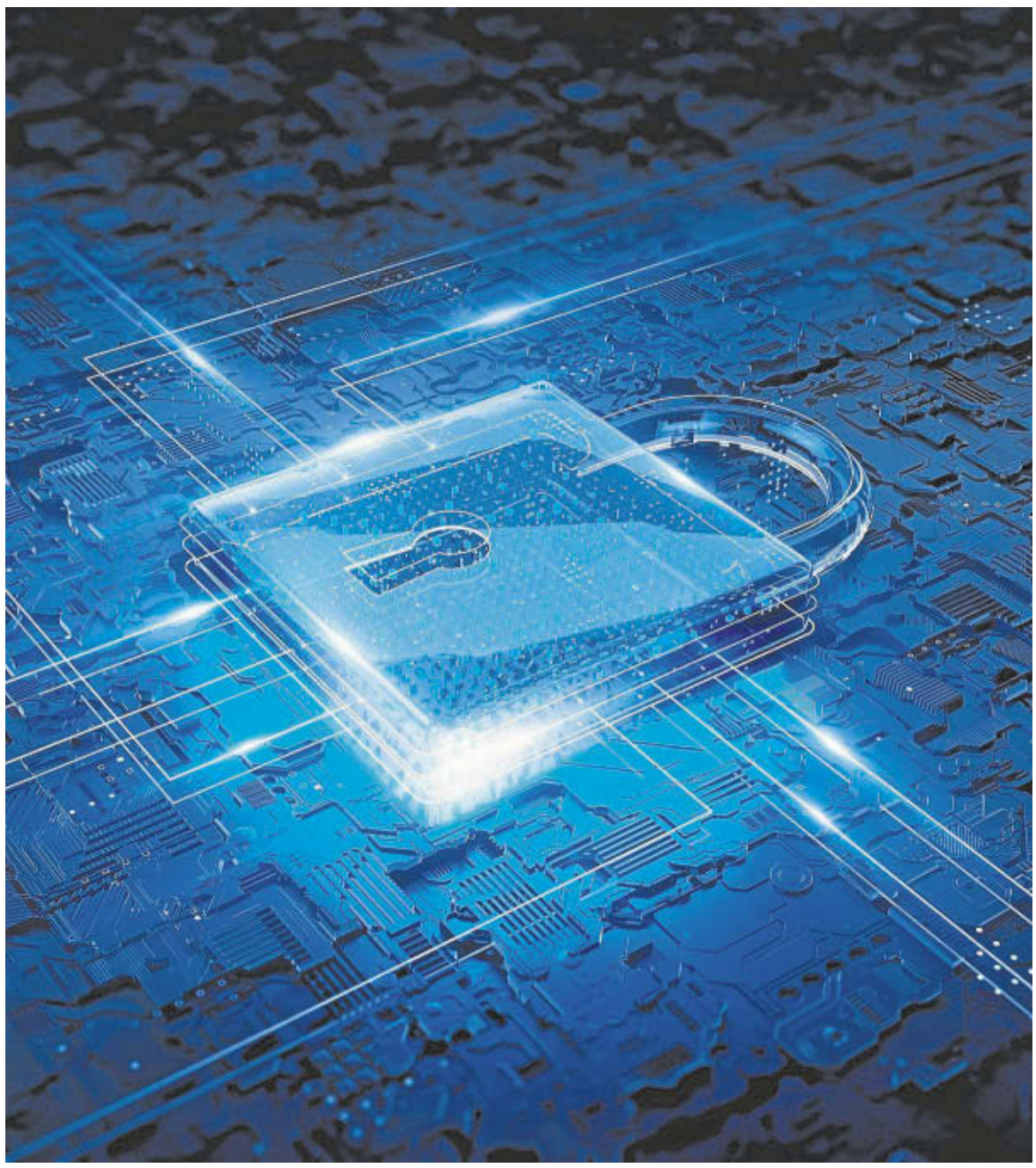
El control de acceso también es importante. En este sentido, para acceder a la información y servicios de la empresa el personal y los usuarios se tienen que identificar y autentificar. El método más habitual es la utilización de un identificador de usuario y una contraseña. Cada sistema o servicio debería tener una contraseña diferente, porque si una contraseña se ve comprometida quedarán comprometidos todos los servicios que tengan aquella contraseña.

Necesitamos unas comunicaciones seguras. Para acceder a los servicios, información, etc. se tiene que establecer una conexión segura. En esta conexión se tiene que garantizar la confidencialidad, integridad y autenticidad de los datos. Para hacerlo hay que utilizar protocolos de comunicación como el TLS o redes privadas virtuales (Virtual Private Network-VPN).

Debemos protegernos contra accesos no autorizados. Cualquier máquina o dispositivo accesible remotamente es susceptible de ser atacado. El objetivo del atacante puede ser tomar el control de la máquina, robar información, utilizar la máquina para hacer ataques, interrumpir el servicio, etc.

La información también debe protegerse. La empresa tiene que establecer qué usuarios o personal puede acceder a qué información y cuando lo pueden hacer. Una forma de conseguirlo es mediante los roles de usuario.

Cada ordenador tiene que incluir un programa para detectar y eliminar virus y otros programas maliciosos (Malware); o la dotación por parte de la empresa de la capacidad de responder ante cualquier imprevisto que pueda surgir para mantener su actividad de forma aceptable.



La ciberseguridad es vital para un buen desarrollo de nuestro proyecto empresarial. FOTO: GETTY IMAGES

3.- Implementación de la seguridad. A partir del diseño de la seguridad se tiene que hacer la implementación o despliegue de las medidas.

4.- Evaluación de la seguridad. Además de hacer la instalación, hay que verificar que las medidas funcionan correctamente. Por ejemplo, con test de seguridad. El responsable de la seguridad tiene que realizar evaluaciones periódicas de seguridad para comprobar que las medidas de seguridad funcionan correctamente. Estas evaluaciones van desde comprobar que los sistemas responden correctamente, revisar los ficheros de logs, asegurarse que los usuarios siguen las directivas de seguridad, o realizar pruebas de penetración (pen-testing).

5.- Vigilancia, mantenimiento y respuesta. Identificación de las situaciones anómalas, porque aunque se implementen medidas de seguridad no se puede garantizar que se esté completamente protegido. La empresa tiene que considerar la instalación en su red de un sistema de detección de intrusiones o de un Sistema de Prevención de Intrusiones. El primero es un sistema pasivo que analiza el tránsito y avisa al administrador cuando detecta una actividad anómala. El segundo también analiza el tránsito pero además de avisar toma decisiones según cada caso.

También es importante la actualización de los sistemas operativos y responder cuando se detecta un ataque o una situación anómala. La empresa tiene que instalar las actualizaciones de seguridad que proporcionan los desarrolladores de sistemas operativos, servicios y aplicaciones. Por último, cuando se detecta un ataque debe estudiarse cómo se ha producido y darle una respuesta lo más rápido.

Para Jordi Castellà (URV) «la ciberseguridad es un proceso que tiene un ciclo de vida»