

Seguridad BYOD

Autelsi aborda un fenómeno nuevo, no planificado, sin metodologías claras

Autelsi ha querido dar claridad a uno de los temas que más inquietud despierta en el seno de las organizaciones, como es BYOD. Para ello, ha elaborado a través de su Comisión de Calidad y Seguridad una Guía que trata sobre “las buenas prácticas para el uso de los dispositivos móviles en la empresa”; se centra en una serie de recomendaciones tanto para los usuarios finales como para los responsables de seguridad de las empresas.

El primer argumento que presenta Autelsi es la necesidad de saber enfocar BYOD, una laguna que presenta un alto número de entidades y que, lógicamente, está provocando que apenas tenga lugar la puesta en marcha de estrategias adecuadas. Una de las razones de ello es que BYOD ha llegado de repente sin que los departamentos de Tecnología hayan tenido tiempo para desarrollar proyectos específicos para su adopción. Juan José Martínez Pagán, presidente de la Comisión de Calidad y Seguridad de Autelsi, lo compara con el PC, “toda vez que la última vez que surgió un fenómeno como BYOD fue el Personal Computer, y su llegada tampoco estaba prevista por los departamentos de tecnología”. Se entiende que es un fenómeno nuevo, no planificado, sin prácticas al uso, ni metodologías establecidas por las organizaciones. Este es el principal inconveniente que entraña BYOD, con el añadido, como asegura Pagán, “de que hay que innovar y no quedarse atrás y muchas empresas no montan un proyecto así porque no se atreven, al abordar sólo proyectos limitados”.

Es evidente que en los últimos años estamos siendo testigos de la preferencia creciente de los usuarios hacia un tipo de dispositivos móviles inteligentes, principalmente tabletas y smartphones, una tendencia que se ha extendido al ámbito de la empresa. Se puede hablar de ventajas para los usuarios relacionadas con su experiencia de uso, acces-

ibilidad a la información y productividad y motivación. Sin embargo, introduce una serie de complejidades en cuanto a la gestión y soporte de estos dispositivos por parte de los departamentos TIC; entre ellos, los riesgos de seguridad y la propia práctica de utilización de los usuarios.

Los expertos de la Comisión de Autelsi han querido hacer frente a estas problemáticas y dar respuestas y recomendaciones. La más importante, dirigida a los usuarios, en los que conviven datos personales y corporativos, es que “éstos deben tomar conciencia de la vulnerabilidad del dispositivo que utilizan, principalmente en cuanto a la seguridad -activar el código PIN, tener en cuenta actualizaciones automáticas relacionadas con la seguridad,...”. A su vez, desde el punto de vista de los departamentos TIC, el uso de dispositivos móviles en la organización introduce una serie de complejidades en su administración y gestión, y unas amenazas en lo que se refiere a la seguridad de los datos corporativos. José Martínez Pagán cree necesario contar con nuevos procedimientos, políticas, herramientas y soluciones, tanto desde el punto de vista de la Gobernanza y aspectos legales y de recursos humanos, como desde el tecnológico de las arquitecturas, herramientas, aplicaciones y políticas a implantar.

La sensación es que estamos ante un mundo que comienza a abrir sus puertas para dar paso a una nueva interacción entre el usuario y la empresa, que acrecentará la productividad y podrá llevar a una reducción de costes pero que necesitará dar pasos seguros. “Hay que definir el alcance de lo que se quiere hacer, qué se deja que se use y qué no; establecer acuerdos de uso, considerar herramientas de gestión y de monitorización, y dar mayor control y gestión de los dispositivos al departamento TIC”, subraya el representante de Autelsi. ■

