PROTECCIÓN DE OFICINAS CONECTADAS

La rápida expansión del Internet de las cosas (IoT, por sus siglas en inglés) plantea complejos desafíos de seguridad para las empresas.

La tecnología ha simplificado más que nunca el uso compartido de la información gracias a la creciente importancia de la informática en la nube, las redes móviles y los servicios de impresión gestionados.

Más de la mitad de los responsables de tomar decisiones en EMEA **comparten documentos** fuera de los sistemas empresariales.

A pesar del incesante crecimiento de la innovación, **la seguridad de los datos sigue siendo importante...**

El 32 % de las empresas sufrieron actos de **cibercrimen** en 2016[1]

El coste total medio de una **vulneración de datos** fue de **3,07 millones de €** en 2017[2]

Especialmente debido a la frecuente **omisión** de las medidas **básicas**

Puntos ciegos de seguridad

Los dispositivos empresariales tradicionales pueden ser puntos débiles también:

El 42 %

de los documentos contiene información confidencial, pero solo al **50 % de los directores** les preocupa que **los empleados dejen documentos confidenciales** en una impresora o fotocopiadora

El 47 %

de los directores son conscientes de que los empleados **pierden documentos en el interior** de sus empresas, frente a un **46 %** que sabe que esto ocurre **fuera de su empresa**

además, **el Reglamento General de Protección de Datos** ha aumentado todavía más **la presión sobre las empresas...**

El 80 %

de **los directores sénior** quiere **actualizar** la **seguridad de los documentos** en los próximos **1 o 2 años**

La gestión de la seguridad de la información no tiene por qué ser compleja...

Pero implica tener en cuenta todo el ciclo de la información y todos los dispositivos conectados de la oficina...

El 77 %

mencionó que los **sistemas** que **convierten los documentos en papel a formato digital** editable son **vitales** o **importantes**

Aunque las **impresoras multifunción** (MFP) reducen la distancia entre la información física y la digital:

Impresión · Copia · Envío · Escaneo

Cada acción supone un aspecto de seguridad que debe ser considerado.

Cuatro pasos para proteger las oficinas conectadas

Hay pasos que las empresas pueden dar para **disfrutar de las ventajas del IoT** sin que la seguridad suponga un quebradero de cabeza.

Primer paso

Auditar y evaluar
Identifica tus carencias físicas y digitales, y establece prioridades.

Segundo paso

Proteger el entorno
Lleva a cabo comprobaciones del estado de la red para identificar cualquier fallo de seguridad adicional.

Tercer paso

Ser inteligente con los dispositivos y sistemas de impresión
Selecciona dispositivos que se ajusten a tus procesos y políticas de seguridad.

Cuarto paso

Adoptar una política de protección
Revisa y actualiza continuamente las políticas de seguridad, y forma a tus empleados sobre la importancia de la seguridad de los datos.

Descarga aquí el informe «IoT Security: 4 steps to a safer connected office» (Seguridad del IoT: 4 pasos para lograr una oficina conectada más segura)

1. http://www.pwc.com/gx/en/services/advisory/forensics/economic-crime-survey.html
2. https://www.ibm.com/security/data-breach