

Los retos de seguridad de las empresas modernas y cómo afrontarlos

La flexibilidad en el lugar de trabajo



Las empresas modernas necesitan acceder a la información, así como moverla y compartirla, a una velocidad y a una escala nunca vistas hasta ahora. Los empleados esperan formas de trabajar más flexibles, eficientes y colaborativas. A medida que el lugar de trabajo se expande más allá de las paredes de la oficina tradicional, necesitas que la información sea tan móvil como tus empleados.

Existen una serie de situaciones a las que casi todas las empresas se enfrentan hoy en día, y a pesar de que estas ofrecen grandes oportunidades de fomentar la innovación y la productividad empresarial, también pueden conllevar amenazas muy graves para la seguridad de los datos de tu empresa.

¿Cómo puedes obtener un equilibrio entre las expectativas de los empleados y la necesidad de proteger la información? Esta guía explora el reto que supone crear un lugar de trabajo digital flexible a la vez que seguro, describe los riesgos de seguridad que deben tenerse en cuenta y ofrece algunas soluciones tangibles para hacer frente a ellos.

RICOH
imagine. change.



La situación

Tus empleados esperan un lugar de trabajo flexible y una mayor movilidad.

La tecnología permite que hoy en día los trabajadores puedan trabajar desde cualquier lugar.

Aunque tu empresa no cuente con personal remoto, la proliferación de tecnologías móviles y en la nube permite trabajar desde otros lugares diferentes a la mesa de trabajo tradicional. El ideal de movilidad para los profesionales va mucho más allá de intercambiar correos electrónicos desde el teléfono, significa acceder de forma sencilla a documentos, datos, compañeros y clientes desde el lugar y en el momento necesarios. Esta libertad se ha convertido en una expectativa básica, por lo que deberás cumplirla si deseas atraer y retener el talento.

Sin embargo, la implementación de un lugar de trabajo realmente flexible y móvil podría exponer tu empresa a una nueva dimensión de posibles amenazas de seguridad. ¿Qué ocurre cuando se sufre la pérdida o el robo de un portátil o un teléfono? ¿Cómo gestionas la seguridad de la información cuando los empleados pueden acceder a ella desde sus dispositivos personales? ¿Cómo se defienden los trabajadores de las miradas digitales indiscretas cuando se conectan a redes WiFi públicas?



Los retos

El hecho de contar con un sistema inadecuado para almacenar y compartir información con los empleados tanto dentro como fuera de la oficina puede afectar enormemente tanto a la productividad como a la seguridad.

Al creer que no tienen a su disposición las herramientas necesarias, tus empleados acudirán a lo que ya conocen para salir del paso. Los archivos se envían por correo electrónico a cuentas personales y se accede a ellos desde ordenadores personales. Los documentos se almacenan y se comparten a través de las soluciones en la nube de los consumidores. La adopción no autorizada de diferentes servicios en la nube puede convertir rápidamente un sistema de información bien diseñado en un desorden fragmentado.

Estas soluciones pueden conducir al inquietante fenómeno conocido como "fuga de datos", que representa una pérdida constante del control sobre la información.

Las soluciones bien intencionadas exponen su información más valiosa

El 84 % de los empleados utiliza correos electrónicos personales para enviar archivos confidenciales¹.

El método de uso de dispositivos propios se está expandiendo

Más de la mitad de las empresas de Norteamérica y Europa están desarrollando programas de uso de dispositivos propios (BYOD) como respuesta a la demanda de los empleados².

Muchas filtraciones de datos son accidentales

Más de 28 millones de registros de datos se vieron afectados en el Reino Unido en el año 2017. De estos, el 38 % se atribuyeron a pérdidas accidentales³.

Las redes WiFi públicas son un campo de minas

Se calcula que tan solo el 5 % de los puntos de acceso WiFi públicos está cifrado, pero el 95 % de las personas los utiliza para trabajar al menos una vez a la semana⁴.

Es posible que no seas consciente del riesgo que esto conlleva

Más de la mitad de los administradores de TI no pueden ver las transferencias de datos y archivos que se producen dentro de sus organizaciones⁵.

1. Ipswitch File Transfer, "Are Employees Putting Your Company's Data at Risk? Survey Results Exposing Risky Person-to-Person File Sharing Practices: An eBook report" www.ipswitchft.com. 2. [www.forrester.com/Bring-Your-Own-Device-\(BYOD\)](http://www.forrester.com/Bring-Your-Own-Device-(BYOD)). 3. www.theregister.co.uk/2017/09/20/gemalto_breach_index/. 4. gfi.com/blog/survey-95-6-of-commuters-in-the-us-put-company-data-at-risk-over-free-public-wi-fi/. 5. Informe de eBook de Ipswitch File Transfer www.ipswitchft.com



Las soluciones

La creación de un sistema de movilidad seguro empieza por saber cómo fluye la información a través de tu organización, dónde se almacena y cómo se utiliza. A medida que los datos se mueven por la empresa de un dispositivo a otro, esta debe protegerse con medidas de seguridad sofisticadas.

Integra tu información en el sistema

El mejor sistema de sincronización y uso compartido de archivos no servirá de nada si la información que necesitas se encuentra en un archivador. Una solución de escaneo a la nube podrá enviar los documentos de forma inteligente directamente al servicio que desees y almacenarlos de forma segura. **Escanea a la nube de forma fácil y segura con la solución de software Streamline NX de Ricoh.**

Imprime cuando lo necesites

A pesar de la comodidad y la flexibilidad que ofrecen los archivos digitales, siempre hay tiempo y lugar para las copias impresas. Asegúrate de que la información correcta caiga siempre en las manos adecuadas con la ayuda de **soluciones de impresión segura, como la funcionalidad Streamline NX Print2Me de Ricoh.**

Impresión móvil y para visitas

La necesidad de imprimir de los invitados y del personal visitante suele solucionarse enviando los archivos a un empleado dentro de la oficina. Esta práctica podría aumentar el riesgo de transmisión de virus y *malware*. La comunicación de igual a igual entre el dispositivo y el teléfono móvil y la impresión Pull basada en la nube mitiga ese riesgo. **Infórmate sobre la solución de impresión móvil MyPrint de Ricoh.**

Gestiona tu información

La implementación de una solución de gestión de documentos puede garantizar que cada empleado tenga el nivel de acceso a la información correspondiente. Asimismo, puede proporcionar datos útiles sobre cómo y cuándo se visualizan o editan los documentos, y sobre quién realiza estos procesos. **Descubre cómo Ricoh y DocuWare trabajan de forma conjunta para ofrecer una solución de gestión de documentos segura y eficiente.**

Pregunta
a un
experto

Visítanos en ricoh.es o contacta con tu representante local de Ricoh para obtener información sobre cómo podemos ayudarte a implementar un lugar de trabajo seguro y flexible.



Ricoh España SL
Av. Vía Augusta 71-73
08174 Barcelona



+34 900 81 83 02



ricoh.es

RICOH
imagine. change.

Los datos y las cifras mostrados en este folleto corresponden a casos empresariales específicos. Las distintas circunstancias pueden generar resultados distintos. Todos los nombres de empresas, marcas, productos y servicios son propiedad y marcas comerciales registradas de sus respectivos propietarios. Copyright © 2017 Ricoh Europe PLC. Todos los derechos reservados. Este folleto, su contenido y diseño no podrán modificarse ni adaptarse, copiarse de forma total o parcial ni integrarse en otros materiales sin el permiso previo por escrito de Ricoh Europe PLC.