Soluciones de seguridad de Ricoh

¿Está protegido tu negocio?

Realidades, riesgos y soluciones empresariales: lectura esencial para empresas ***smart***

La ciberseguridad es fundamental para la protección de activos de información, a través del tratamiento de amenazas que ponen en riesgo la supervivencia y el éxito de los negocios modernos.

Empresas de todos los tamaños están en riesgo de ser víctimas de ataques con interrupción de las actividades, tales como la suplantación de identidad (***phishing***), el DDoS o el ***ransomware***, con un coste económico muy elevado. Las normativas gubernamentales, tales como el GDPR (Reglamento General de Protección de Datos), pretenden castigar los negocios con severas sanciones por no poder proteger sus sistemas y datos adecuadamente. Mientras tanto, la expansión y la digitalización del lugar de trabajo moderno agravan los retos cibernéticos. A medida que los flujos de trabajo se expanden entre dispositivos, redes y regiones, la información necesita más protección.

Al mismo tiempo, en los últimos años se han multiplicado por diez las capacidades de las impresoras y los dispositivos multifuncionales de las oficinas. Ahora, estos dispositivos se encargan de una gran parte de las entradas, salidas, transferencias y almacenamientos de datos de la empresa. Esto los convierte en una de las mayores amenazas potenciales para los entornos de trabajo actuales; una amenaza que a menudo las empresas pasan por alto.

Ante estos desafíos, es más importante que nunca que las empresas tengan sistemas de gestión de datos y documentos fundamentalmente seguros y que sean capaces de demostrarlo.

60 %

Empresas de Europa y de Estados Unidos que informaron de una filtración de información por culpa de una impresión no segura el año pasado*

*Estudio de Quocira Enterprise MPS, 2017. Datos: 240 organizaciones de más de 500 empleados de Reino Unido, Francia, Alemania y Estados Unidos en varios sectores.

20m €

Es la sanción máxima posible para empresas que no cumplan el GDPR*

*Portal de la UE sobre el GDPR, 'Frequently Asked Questions about the incoming GDPR' en www.eugdpr.org/gdpr-faqs.html.

RICOH
imagine. change.

Aspectos que hay que tener en cuenta para proteger tu negocio

¿Están los datos protegidos?

- Almacenamiento de datos
- Riesgo de pérdida/hurto
- Riesgo de ataque cibernético
- Riesgo de alteración/corrupción
- Acontecimientos imprevistos

La realidad

Los datos son el bien más valioso de tu empresa. Aunque pueda ser fácil esconder la cabeza frente a amenazas como el hurto de datos, los ataques cibernéticos o los desastres naturales, el impacto de la falta de protección frente a estos acontecimientos puede ser devastador.

Los riesgos

- Ataques cibernéticos: En Ricoh evitamos unos ocho mil millones de ataques de cortafuegos al mes
- Pérdida de continuidad empresarial por desastres naturales
- Hurto de datos desde dentro o desde fuera de la empresa

¿Es la gestión de documentos segura?

- Uso compartido de documentos
- Destrucción de documentos
- Gestión de los dispositivos
- Impresión segura

La realidad

El uso compartido de documentos, su almacenamiento e impresión también pueden suponer riesgos para la seguridad. La típica impresora de oficina suele ser una vulnerabilidad que se pasa por alto a la hora de gestionar la documentación de forma segura.

Los riesgos

- Información confidencial que cae en malas manos por culpa de una impresión no segura
- Divulgación de información confidencial por no destruir completamente los dispositivos o los documentos
- Ataques de piratas a dispositivos

¿Es el lugar de trabajo digital seguro?

- Gestión del flujo de trabajo
- Entorno de trabajo móvil
- Protección de datos en movimiento
- Infraestructura de TI

La realidad

Las grandes ventajas del entorno de trabajo flexible y móvil también suponen grandes riesgos. ¿Cómo gestionas el enfoque "traiga su propio dispositivo"? ¿Wifi público inseguro? ¿Dispositivos en malas manos?

Los riesgos

- Pérdida de información confidencial de la empresa por los puntos débiles de un entorno de trabajo flexible
- Filtración de datos por la falta de visibilidad y de control de la utilización de los dispositivos

¿Cumple tu empresa la normativa?

- Cumplimiento normativo
- Cumplimiento del Reglamento General de Protección de Datos (GDPR)

La realidad

Además de las obligaciones normativas existentes, el GDPR entrará en vigor en mayo de 2018. ¿Cómo puedes saber si estás preparado? ¿Cómo puedes demostrar el cumplimiento normativo?

Los riesgos

- Un gran coste en multas para las empresas que no cumplan la normativa
- Daños en la reputación

La combinación de amenazas de seguridad y requisitos legislativos implica que el potencial de riesgo cibernético de daño fiscal y a la reputación nunca había sido tan grande. Ha llegado el momento de invertir en la seguridad de tu entorno de trabajo digital con un socio en el que puedes confiar.

RICOH
imagine. change.

La buena noticia es que Ricoh ya ha pensado en la seguridad por ti. Somos expertos a la hora de comprender estos riesgos, puesto que hemos pasado varias décadas desarrollando formas de mitigarlos a través de medidas de seguridad de última generación incorporadas en todos nuestros productos y soluciones. Por ejemplo, nuestras impresoras integran funcionalidades de sobrescritura protegida del disco duro desde hace más de 20 años. La seguridad está en el ADN de toda nuestra cartera de servicios para entornos de trabajo digitales.

Ricoh ofrece una estructura sólida de servicio y soporte en todo el mundo a sus clientes que garantiza que se comparta la información y se actúe ante las amenazas. Y no solo implementamos la certificación IEEE 2600 como estándar en nuestros equipos de impresión sino que, además, Ricoh es miembro destacado y autor fundamental en la Asociación de estándares IEEE. Ricoh también cuenta con la certificación ISO 27001 y está comprometido con seguir respetando este sistema de gestión de seguridad de la información.

Para cumplir los exigentes requisitos de buenas prácticas en ciberseguridad demostrables y efectivas, la seguridad se incluye desde la fase de diseño de cada producto y servicio de la cartera de Ricoh, no a posteriori. Creemos que esta visión global de las vulnerabilidades es esencial para la supervivencia de los negocios modernos.

Todos los aspectos de nuestro enfoque de seguridad están respaldados por estos principios de privacidad y seguridad: confidencialidad, integridad y disponibilidad.

RICOH
imagine. change.

Cómo protege Ricoh el entorno de trabajo digital

Entendemos la importancia que tiene proteger tu entorno de trabajo digital en el complejo ciclo de vida de los datos empresariales. Esto se consigue mediante la implementación de medidas de seguridad en cuatro etapas cruciales: control, preservación, destrucción y soporte.

CUATRO ETAPAS CRUCIALES

1 CONTROL

Protege la integridad de los datos con el fin de evitar su manipulación. Protege los dispositivos de entrada y captura de datos, así como el modo de almacenamiento y transporte de los datos por la red.

- Protección de copia
- Autenticación y autorización del usuario
- Acceso restringido/impresión bloqueada
- Protección contra *malware* en los dispositivos

2 PRESERVACIÓN

Acceso seguro a los datos. Nos aseguramos de que los protocolos de seguridad no dificultan la productividad, la funcionalidad ni la innovación empresarial.

- Cifrado de datos
- Infraestructura de autorización
- Módulo de plataforma segura (TPM)
- Acceso seguro y rápido, independientemente de la ubicación del usuario o el dispositivo

3 DESTRUCCIÓN

Reduce el riesgo de pérdida o robo de datos a través de una eliminación eficaz de los datos según la normativa.

- Sistema de seguridad de sobrescritura de datos (DOSS)
- Borrado de datos de dispositivos al final del ciclo de vida
- Eliminación de discos duros
- Vaciado de memoria

4 SOPORTE

Ofrecemos soporte en materia de seguridad integral a las empresas.

- Evaluación de seguridad de la infraestructura
- Optimización de la seguridad de impresión
- Equipo de respuesta ante incidencias de seguridad (SIRT)
- Soporte de documentación con cumplimiento normativo

El entorno de trabajo digital moderno debe ser tan dinámico como las amenazas cibernéticas a las que se enfrentan las organizaciones y tan flexible como las prácticas laborales que desarrollen. Por eso pensamos que la ciberseguridad debe funcionar a la perfección con cualquier tecnología que nuestros clientes elijan para su entorno de trabajo. Con nuestro compromiso con la norma ISO 27001 en todas nuestras oficinas y la certificación IEEE 2600 en todos nuestros productos, sabrás que, con Ricoh, los mejores controles de seguridad estarán implementados, sea cual sea la solución que elijas para estructurar y hacer crecer tu empresa.

¿Quieres algo más técnico? Para conocer los detalles sobre las funcionalidades de protección de Ricoh, descárgate el informe completo: **Soluciones de seguridad de Ricoh**

Para descubrir cómo puede ayudarte Ricoh a proteger y potenciar tu negocio, visítanos en **ricoh.es** o ponte en contacto con un representante local de Ricoh.

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

+34 900 81 83 02

ricoh.es

RICOH
imagine. change.

Los datos y cifras expresados en este folleto se refieren a casos comerciales específicos. Los resultados pueden variar en función de circunstancias concretas. 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 su diseño no pueden ser modificados, adaptados, copiados en parte o en su totalidad ni utilizados en otros trabajos sin la aprobación previa por escrito de Ricoh Europe PLC.