RICOH
imagine. change.

Soluciones de seguridad de Ricoh

Te ayudamos a proteger tu negocio

La ciberseguridad es fundamental para proteger los activos de información, a través del tratamiento de las amenazas que ponen en riesgo la supervivencia y el éxito de los negocios modernos. Empresas de todos los tamaños están en riesgo constante de ser víctimas de ataques disruptivos, tales como la suplantación de identidad (*phishing*), DDoS o *ransomware*. El coste económico real de estos ataques es muy elevado. En 2017, el Ponemon Institute desveló que el coste medio global de una filtración de información era de 3,62 millones de dólares. Este coste no hará más que crecer en los próximos años, ya que las normativas gubernamentales, tales como el GDPR (Reglamento General de Protección de Datos), pretenden castigar a los negocios con severas sanciones por no proteger sus sistemas y datos adecuadamente. Para evitar estas sanciones debilitantes, los negocios deben demostrar su capacidad para proteger los datos. Esto requiere una visión global de todas las vulnerabilidades de la empresa.

Otro factor que se añade al reto de la ciberseguridad para las empresas es la expansión y la digitalización de los entornos de trabajo modernos, así como la explosión en el volumen de datos. Los flujos de trabajo se expanden a menudo entre dispositivos, redes y regiones. La información está más expuesta al riesgo durante las relaciones comerciales. Debe permanecer protegida en todas las etapas de su recorrido. Dado el riesgo de seguridad que esto plantea, los negocios modernos ya no pueden funcionar sin sistemas de protección de datos y documentos. 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 están a cargo 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 para los entornos de trabajo actuales; una amenaza que a menudo las empresas pasan por alto.

Aunque muchas empresas afirman ofrecer funcionalidades de protección, Ricoh lleva décadas desarrollando soluciones y servicios para un entorno de trabajo seguro. 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. Actualmente tenemos más de cuatro millones de productos de oficina en el mercado. Cada uno de estos productos y cada servicio que implementamos con ellos integran funcionalidades de protección. También utilizamos un sistema operativo exclusivo de Ricoh en muchos de nuestros productos. Es un componente esencial para nuestras defensas de seguridad, que proporciona control y aislamiento de amenazas específicas de SO que afectan a los sistemas operativos más comunes.

Ricoh ofrece a sus clientes en todo el mundo una estructura sólida de servicio y soporte 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. Nuestro desarrollo de productos se centra en las necesidades empresariales y las inquietudes de seguridad de los clientes mediante una serie de programas de innovación globales orientados al cliente.

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.

RETO DE SEGURIDAD PARA EL CLIENTE

TENDENCIAS: Cuando aumenta el volumen de datos, también lo hacen las vulnerabilidades, los ataques y las sanciones.

Protección y empoderamiento de entornos de trabajo digitales

Ricoh desea promover y proteger el trabajo digitalizado seguro, en cualquier lugar donde se trabaje. En una economía digital moderna, esto implica añadir valor más allá de los límites de la oficina tradicional, en los entornos de trabajo de primera línea. Las oficinas remotas y los empleados a distancia permiten a las empresas gozar de una gran flexibilidad y productividad en las operaciones cotidianas, ya que les ayudan a cumplir mejor las expectativas y los requisitos de servicio de los clientes.

Sin embargo, esta nueva forma de trabajar plantea algunos de los mayores riesgos para la seguridad de las empresas. Los datos que estos empleados generan y los dispositivos remotos que utilizan para capturarlos se tienen que proteger adecuadamente. A menudo, los empleados operan entre redes y regiones, complicando aún más esta tarea. Existen normativas gubernamentales, tales como el GDPR, que requieren que las empresas protejan los datos de forma demostrable durante su ciclo de vida para no enfrentarse a graves sanciones. A medida que los entornos de trabajo evolucionan y adoptan los flujos de trabajo digitales, el ciclo de vida de los datos se hace cada vez más complicado. Ahora lo examinaremos, etapa por etapa.

El primer paso se centra en los dispositivos de entrada y captura de datos, un componente esencial de la defensa de seguridad de Ricoh. Desde ahí, los datos se deben transportar por las redes y almacenar de forma segura. En esta etapa, preservar la integridad de los datos es esencial. Los sistemas de Ricoh restringen el acceso del usuario al dispositivo y la funcionalidad de red para garantizar que los datos no se puedan manipular durante el transporte o cuando no estén activos. Estos servicios incluyen control de acceso, cifrado y protección de copia. A esta etapa la llamamos Control.

Sin embargo, una vez almacenados, los documentos estarán accesibles directamente para aquellos usuarios de la empresa que los necesiten. La capacidad de utilizar la información cuando sea necesario y visualizarla de forma efectiva depende de su disponibilidad. El análisis de datos es un componente esencial del entorno de trabajo digital empoderado. Permite examinar de forma efectiva cada elemento de la empresa, desde ventas a recursos humanos. Las herramientas de infraestructura de autorización proporcionan un acceso seguro rápido, independientemente de la ubicación del usuario o el dispositivo que elija. Es esencial que los protocolos de seguridad no obstaculicen la innovación o la funcionalidad ni provoquen el rechazo de los empleados. A esta etapa la llamamos Preservación.

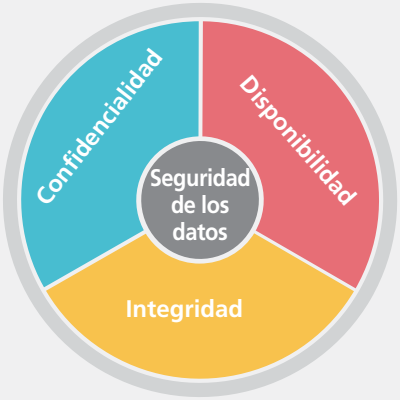
Por último, estos datos se pueden borrar de forma segura y auditable. Este paso es esencial para cumplir con los requisitos normativos y minimiza la posibilidad de pérdida o robo posterior. Este proceso normalmente ocurre a lo largo del ciclo de vida de un documento hasta su eliminación definitiva. Imprimir cualquier archivo deja una imagen latente en el disco duro de las impresoras multifuncionales que se deberá sobrescribir para evitar un acceso no autorizado. Los servicios de borrado de datos de Ricoh incluyen la limpieza de discos duros, el vaciado de memoria, la eliminación de archivos no impresos y la función de borrado al cerrar sesión para impedir que los piratas informáticos reúnan información confidencial a partir de las huellas que deja un documento. A esta etapa la llamamos Destrucción.

Para proteger de forma segura los datos de un entorno de trabajo a lo largo de su ciclo de vida, Ricoh utiliza estos principios para la privacidad y la seguridad: confidencialidad, disponibilidad e integridad. Estas son nuestras directrices para diseñar nuestros productos y soluciones de forma que cumplan las normativas y los estándares necesarios. Este enfoque permite la innovación y el crecimiento en el entorno de trabajo, mientras mantiene los procesos efectivos y seguros.

ENFOQUE DE RICOH ANTE LA SEGURIDAD

El acceso a la información y los documentos se debe restringir según las directrices y los requisitos definidos por el cliente.

Acceso a la información y los documentos donde y cuando se necesite.



Impedir la edición no autorizada de un documento en tránsito y en almacenamiento.

Seguimos estos principios de privacidad y seguridad: confidencialidad, integridad y disponibilidad

Llevamos la seguridad en el ADN. Cada producto fabricado y servicio implementado por Ricoh contiene funciones y funcionalidades de seguridad integradas

Ricoh ofrece un paquete completo de productos y servicios de seguridad para proteger la creación de documentos de principio a fin. Ahora examinaremos cada etapa crucial: control, preservación, destrucción y soporte.

LAS CUATRO ETAPAS DE LA SEGURIDAD EN EL ENTORNO DE TRABAJO DIGITAL

1 CONTROL

Los controles efectivos de datos son esenciales para mantener la confidencialidad y la integridad de los datos. La información comercial es un activo fundamental y se debe proteger. Los dispositivos de hardware actuales son terminales de información que pueden actuar como puertas de enlace vulnerables a la información de la empresa. Como tal, Ricoh emplea diversas herramientas de gestión de dispositivos y autenticación de usuarios para controlar y proteger los datos de la empresa. Estas herramientas se encuentran en la configuración de los dispositivos físicos que permiten y restringen el acceso a determinados datos y funcionalidades. Limitar el acceso de los empleados a la transferencia de información desde cualquier impresora multifuncional es una práctica recomendada esencial para mantener la seguridad de los documentos. La etapa de control también incluye la protección contra *malware* mediante el enfoque de tres niveles de Ricoh respecto del firmware del dispositivo.

Control de copia no autorizada

Para protegerse de los intentos de realización de copias no autorizadas, Ricoh ofrece una solución inteligente que garantiza la seguridad de los documentos en papel. La función de protección de copia imprime o copia los documentos con patrones invisibles especiales incrustados en el fondo. Si el documento impreso o copiado se fotocopia y/o escanea, los patrones incrustados serán visibles en las copias. El módulo de protección contra las copias no autorizadas permite a la impresora multifuncional detectar los patrones incrustrados y reemplazar la imagen fotocopiada con una imagen en gris para evitar filtraciones de información. Esta función es útil cuando se imprime información confidencial. Restringir la copia de información confidencial evita este tipo de filtraciones de información.

Impresión bloqueada

Un documento recibido desde un ordenador se puede almacenar en el disco duro de la impresora multifuncional. Con la función de impresión bloqueada de Ricoh, se especifica una contraseña cuando un usuario envía el documento y se debe introducir esa contraseña en la impresora multifuncional para poder imprimirlo. Dado que el documento no se imprimirá hasta que el propietario alcance el dispositivo, la impresión bloqueada garantiza que el documento permanezca bajo el control de su propietario.

Seguridad de captura avanzada

La cartera de soluciones de captura avanzada de Ricoh ofrece diversas capas de cifrado y descifrado a través de las capas de procesamiento, en todas las etapas del proceso de captura. Los administradores pueden autorizar el acceso para procesar colas por inicio de sesión de usuarios individuales o por credenciales de grupo. Entre las capas adicionales de seguridad se incluyen el marco SALM (Lenguaje de marcado de aserción de seguridad) para SSO (inicio de sesión único), la verificación de identidad personal (PIV) y el cifrado PKI (infraestructura de clave pública).

Controles de autenticación incrustados

Los protocolos de acceso e identificación de dispositivo en los productos Ricoh se pueden gestionar de forma centralizada. Entre los métodos disponibles están la tarjeta de identificación, el número PIN, el inicio de sesión de red o una combinación multifactor de los anteriores. La autenticación multifactor mejora la seguridad, pero puede ralentizar a los usuarios ocupados. El inicio de sesión único (SSO) ayuda a ello ya que permite a los usuarios acceder a diversos dispositivos sin problemas. Además, la Autenticación rápida de Ricoh, un software de autenticación basado en tarjetas que se pasan por un lector, viene preinstalado en todos nuestros dispositivos, proporcionando a los usuarios un método fácil para acceder a sus documentos. El uso de un lector/escritor NFC simplifica mucho el proceso de inicio de sesión del usuario, a la vez que garantiza y controla de forma efectiva el acceso a la impresora multifuncional. Este método de acceso también funciona en conjunción con la configuración de los permisos de impresoras multifuncionales existentes para restringir el acceso de los usuarios a funciones del dispositivo según las necesidades del cliente.

Streamline NX (SLNX)

El módulo Device Manager dentro de la plataforma Streamline NX de Ricoh permite gestionar y supervisar dispositivos en una red. Este software permite a los administradores ver o configurar parámetros de seguridad para dispositivos mediante plantillas precargadas y parámetros personalizados. Entre los parámetros de seguridad básicos se incluyen la habilitación/deshabilitación de protocolos, la configuración de la dirección IP, las contraseñas del usuario administrador, las direcciones de correo electrónico para alertas o la configuración de cifrado. SLNX también puede avisar de cualquier impresora que no cumpla las directrices del cliente.

Protección contra *malware* en los dispositivos

Ricoh adopta un enfoque de triple capa ante la protección contra el *malware* en sus dispositivos. En primer lugar, los dispositivos de Ricoh solo se pueden poner en funcionamiento con un sistema operativo o lenguaje de máquina exclusivo de Ricoh. En segundo lugar, para impedir que el software malicioso manipule el software del dispositivo, cualquier actualización de software debe estar escrita y aprobada únicamente en este lenguaje de máquina exclusivo de Ricoh. Por último, todas las actualizaciones de firmware las debe firmar Ricoh digitalmente. Con este método de tres pasos, el firmware no autorizado no se puede cargar en los dispositivos de Ricoh, y así eliminamos de forma efectiva el *malware*, el *spyware* y los virus.

Seguridad de documentos físicos

Las prácticas recomendadas de seguridad no tienen por qué ser complicadas. Las oficinas son espacios con mucho tráfico de datos, y la documentación en formato físico presenta un riesgo significativo para la empresa, tanto de robo como de negligencia por parte de los empleados. Ricoh proporciona diversas opciones de seguridad física adicional para evitar el acceso no autorizado a los documentos en papel. Por ejemplo, cerrar bajo llave los archivadores de papel evita el robo de papeles confidenciales almacenados, tales como recetas médicas en los entornos sanitarios. Instalar placas ciegas para todos los cables también impide la manipulación por parte de amenazas internas. Una solución de liberación segura de documentos (Print-to-me) garantiza que los documentos solo se impriman cuando el propietario esté presente para eliminar el riesgo de que el material quede sin recoger.

2 PRESERVACIÓN

Según los requisitos normativos nuevos y existentes, las empresas deben garantizar tanto la confidencialidad de la información, para que no la roben ni se filtre, como su integridad continua, para que no se pueda alterar. Para lograrlo, las empresas deben restringir el acceso a los documentos confidenciales. Esto evita la modificación y la falsificación no autorizadas. También actúa como protección ante amenazas selectivas u oportunistas dentro de la empresa.

Un entorno de trabajo móvil añade complejidad a cualquier escenario de ciberseguridad. Debe haber medidas de seguridad adicionales implementadas para permitir el uso compartido de archivos desde cualquier ubicación. Esos archivos deben estar tan protegidos en tránsito por redes y entre dispositivos como lo están cuando se encuentran almacenados. Una tecnología de cifrado fuerte puede realizar un seguimiento y proteger los datos de forma efectiva en todo su ciclo de vida. Esto se aplica naturalmente a los documentos, pero se extiende a elementos de seguridad esenciales como las contraseñas almacenadas, la configuración de macros y las libretas de direcciones. Con el cifrado implementado, aunque los piratas informáticos puedan acceder a su red, tendrán que esforzarse por extraer datos útiles, con lo que se preserva su integridad incluso en caso de filtración.

Muchos sectores no pueden permitirse un parón de la actividad. Por lo tanto, acontecimientos imprevistos como los desastres naturales pueden presentar un riesgo directo para el negocio. Los documentos en papel son especialmente vulnerables en este caso. Al utilizar un repositorio seguro basado en la nube para los documentos digitalizados, se añade una resiliencia crucial ante los desastres naturales y causados por el hombre. Sin embargo, se deben seguir los pasos de seguridad adecuados para preservar estos datos digitales.

Cifrado de datos esenciales

Para proteger la información mientras se transfiere entre dispositivos, se debe habilitar el cifrado para cualquier dato que viaje a o resida en un disco duro de una impresora multifuncional Ricoh. Las opciones de software integradas proporcionan cifrado íntegro para los archivos escaneados e impresos mediante la clave de infraestructura de clave pública (PKI). Esto protege contra ataques de intermediarios dentro del entorno de TI del cliente.

Para una seguridad añadida, el Data Overwrite Security System (DOSS) de Ricoh sobrescribe los datos impresos continuamente (hablaremos de ello con más detalle más adelante, en la etapa de Destrucción del ciclo de vida de los datos.

Protección de la bios y del sistema operativo

Las impresoras multifuncionales de Ricoh incluyen un Módulo de plataforma seguro (TPM), un módulo de seguridad de hardware a prueba de manipulaciones. El módulo TPM desempeña funciones criptográficas y almacena de forma segura los datos cifrados. Ricoh utiliza el módulo TPM para almacenar la clave de cifrado raíz que protege la clave de cifrado de los datos del disco duro y el certificado digital de las impresoras multifuncionales. También permite a los administradores realizar una operación de arranque seguro gracias a la validación de la autenticidad del firmware de las impresoras multifuncionales antes de permitirles operar.

Validación del firmware

Las funciones criptográficas y de clave raíz siempre están integradas en la impresora multifuncional y no se puede alterar desde fuera del cortafuegos, lo cual evita el uso indebido o la manipulación maliciosa de nuestros productos. Este proceso proporciona una validación de alto nivel del firmware de la impresora multifuncional, la identidad del dispositivo y la seguridad del disco duro. Este es otro buen ejemplo de cómo los productos para impresoras multifuncionales de Ricoh están diseñados teniendo en cuenta los intereses de seguridad de los clientes de Ricoh.

Gestión de contraseñas

Los dispositivos de Ricoh se pueden configurar con varios usuarios administradores, cada uno con distintos roles en los dispositivos y contraseñas propias. Las contraseñas para estos usuarios se pueden configurar de forma remota con herramientas de administración basadas en web y verificar frecuentemente. Esto permite la segregación de tareas, que es un requisito presente en diversas normativas empresariales.

Restricción del acceso para usuarios

La herramienta de gestión de usuarios de Ricoh permite a los administradores del sistema restringir los privilegios de acceso de los usuarios. Por ejemplo, el administrador puede configurar privilegios para proporcionar acceso a los usuarios seleccionados a una libreta de direcciones registrada de la impresora multifuncional. Esto bloquea el acceso no autorizado a la información personal y los registros almacenados en los dispositivos de la oficina.

Función de bloqueo del usuario

Cuando se introducen contraseñas erróneas consecutivamente durante el proceso de inicio de sesión, una impresora multifuncional de Ricoh puede evaluar si alguien está intentando descifrar la contraseña. Esto activa la función de bloqueo de este nombre de usuario en cuestión. El nombre de usuario bloqueado no se podrá autenticar aunque se combine con la contraseña correcta. El bloqueo solo se puede liberar una vez transcurrido un determinado lapso de tiempo o si lo hace un administrador. De esta manera, se frena de forma efectiva a los posibles *hackers*.

3 DESTRUCCIÓN

El borrado seguro de datos es una parte esencial de cualquier defensa de ciberseguridad integral. Es fácil caer en la trampa de asumir que las responsabilidades de la empresa terminan cuando los datos salen de una organización. Sin embargo, numerosas normativas regulan que la destrucción de datos debe ser un proceso integral, que elimine cualquier riesgo de posterior robo o uso indebido. Hasta que no se demuestre que no existe tal riesgo, las obligaciones de una empresa con respecto a los datos no han terminado.

Los dispositivos de oficina que han finalizado su ciclo de vida o se han devuelto plantean a menudo un riesgo no reconocido para la información de la empresa. Ricoh ofrece un servicio certificado auditable para borrar los datos de estas impresoras que han llegado al fin de su vida útil. Esto incluye material olvidado como la configuración de red guardada, los datos de los usuarios, los datos de los discos duros o incluso los adhesivos que se han dejado en el dispositivo. Si no se realiza, las empresas corren un importante riesgo de exponer información confidencial personal y de la empresa. Pero, para poder cumplir con la normativa, este proceso también debe desarrollarse constantemente a lo largo de la vida útil de un dispositivo. Esto garantiza que los negocios tengan el máximo control posible sobre los datos de los que son responsables.

Sobrescritura de imagen: Sistema de seguridad de sobrescritura de datos (DOSS)

Los discos duros de las impresoras multifuncionales funcionan de forma efectiva almacenando imágenes latentes de datos de documentos en su memoria para el procesamiento de trabajos. La Solución Data Overwrite Security de Ricoh garantiza que se sobrescriban constantemente antes de que comience el siguiente trabajo. De esta forma, si alguien quiere acceder al disco duro maliciosamente, no podrá acceder a la huella de datos de trabajos anteriores. En Ricoh nos sentimos orgullosos de ofrecer esta medida de seguridad, que es una práctica recomendada desde hace más de 20 años.

Servicio Borrado certificado de datos tras el fin de la vida útil

Ricoh ofrece el Borrado certificado de datos, un servicio tras el fin de la vida útil de las impresoras multifuncionales que borra todos los módulos de memoria y almacenamiento de disco del dispositivo sin posibilidad de recuperación mediante soluciones de seguridad certificadas por la industria. Los Servicios de TI de Ricoh ofrecen soluciones de eliminación integral de los equipos, incluidos servicios de borrado certificados de varios niveles de datos.

Reemplazo de discos duros y almacenamiento extraíble

Ricoh también ofrece un servicio de eliminación de discos duros que deja que los clientes se queden con su disco duro, reemplazándolo por un disco duro nuevo vacío cuando devuelven el equipo al final de su vida útil. Esto garantiza un control total y demostrable de la empresa con respecto a su entorno de datos.

4 SOPORTE

A medida que el negocio crece, el número de conexiones entre dispositivos y redes crece también inevitablemente. Las empresas necesitan estrategias para garantizar que este crecimiento de infraestructura no plantee un riesgo de seguridad. Deben ser conscientes de los puntos débiles de su sistema, y adoptar medidas para atajar ataques selectivos y oportunistas antes de que ocurran.

A menudo, se requiere experiencia previa en seguridad de TI para analizar la infraestructura de un negocio e identificar estas vulnerabilidades. Muchas empresas no se pueden permitir disponer del personal de TI en plantilla con los conocimientos necesarios para gestionar su entorno de ciberseguridad. Los costes y las ineficiencias de este enfoque a menudo conducen a estas empresas a una situación peligrosa por no tomar medidas.

El servicio de soporte de TI de Ricoh ofrece servicios de adquisición y configuración de TI, así como supervisión remota, asistencia técnica y funcionalidades de gestión de transiciones para respaldar adicionalmente el proceso de ciberseguridad. La ciberseguridad depende de comprender globalmente los riesgos para el negocio. El equipo de respuesta ante incidencias de seguridad (SIRT) de Ricoh garantiza que los conocimientos esenciales sobre amenazas se comparten con los clientes de todo el mundo, y que se pueden coordinar respuestas efectivas de inmediato.

Evaluación de la seguridad de la infraestructura

La funcionalidad de Device Manager de Streamline NX (SLNX) de Ricoh está diseñada para realizar una valiosa función de auditoría de las directrices de seguridad. SLNX proporciona una funcionalidad que permite a los gestores de TI configurar dispositivos basándose en las directrices de la empresa, distribuir esa configuración y analizarla en un informe. SLNX también puede avisar a la dirección cuando un dispositivo incumple las directrices de la empresa.

Optimización de la seguridad de impresión

Ricoh ofrece un servicio integral de Optimización de la seguridad de impresión (PSO) junto con servicios de asesoramiento gestionados y profesionales para identificar brechas de seguridad relacionadas con el dispositivo. Se trata de una herramienta web con un asistente gráfico que proporciona una visión del estado actual y permite a Ricoh ofrecer recomendaciones sobre el producto para lograr una reducción del riesgo.

Equipo de respuesta ante incidentes de seguridad de productos (PSIRT)

La respuesta activa de Ricoh con respecto a las nuevas amenazas y el desarrollo de contramedidas efectivas lo gestiona el Product Security Incident Response Team (PSIRT, Equipo de respuesta ante incidentes de seguridad de productos). Se trata de un programa que Ricoh utiliza para garantizar que todo nuestro paquete de productos (hardware y software) se actualice continuamente y quede protegido contra las nuevas amenazas y vulnerabilidades identificadas. Esto nos ayuda a mantener un alto nivel de servicio constante a escala global y minimizar el impacto de los problemas de vulnerabilidad de los productos de Ricoh.

Documentación de soporte

La preparación y la formación son elementos cruciales de cualquier configuración de ciberseguridad. Al cliente se le debería proporcionar formación, documentación sobre copias de seguridad, guías de usuario y nociones sobre seguridad. Al igual que sucede con muchos elementos del entorno de ciberseguridad, el cumplimiento demostrable de la normativa es crucial y esta documentación desempeña un papel clave para garantizar la seguridad básica de una empresa.

¿CÓMO PUEDE AYUDAR RICOH?

La posición exclusiva de Ricoh para proporcionar soluciones de seguridad líderes en la industria para cualquier entorno de TI e impresión se basa, en parte, en una sólida comprensión de los cambios en el mercado y en la adopción de nuevas estrategias adaptadas a estos cambios. Nuestras soluciones están diseñadas para proteger toda la información a lo largo de todo su ciclo de vida y responder de forma estricta a las cuatro áreas de seguridad de datos expuestas en este informe.

Disponemos de expertos en la materia responsables de analizar las necesidades del mercado, incluidos los requisitos específicos de la industria para los que pueden crearse nuevas soluciones o adaptar otras existentes.

Nos comprometemos también a desarrollar nuestra capacidad interna para diseñar e implementar soluciones centradas en la seguridad.
A tal fin, hemos creado equipos dedicados dentro de nuestro departamento de desarrollo de servicios que se centran en desarrollar nuevos servicios de gestión del riesgo en cumplimiento de las normativas gubernamentales, así como servicios de ciberseguridad.

Autenticación y autorización de usuario

- Impresión bloqueada
- SW con estándar incrustado para autenticación
- Autenticación / restricción de acceso al usuario
- Inicio de sesión único
- Roles múltiples de administrador
- Protección de PDF con contraseña (contraseña para documentos escaneados)
- Protección de copia no autorizada
- Control de acceso basado en intervalo de IP
- Gestión segura de impresión y del dispositivo
- Compatibilidad con PKI (infraestructura de clave pública) / SmartCard
- Impresión segura (print2me / impresión bloqueada)

Protección contra *malware* en los dispositivos

- Servidores
- No/menos susceptible al *malware*
- SOP: versión reforzada de Android
- SO de máquina exclusivo de Ricoh (lenguaje de control de máquina) para impresoras multifuncionales
- Enfoque de 3 capas: firma digital, descarga mediante herramienta de Ricoh, necesidad de escritura en un lenguaje de control específico

Eliminación del disco duro

- Eliminación del disco duro, sobrescritura de imagen
- Servicio de Borrado certificado de datos
- Servicio de fin de vida útil: destrucción de datos de los módulos de la memoria, almacenamiento

Gestión del dispositivo

- Asignación de cuotas / límite de cuenta
- DMNX: panel único de auditoría de seguridad, gestión de contraseñas, monitorización, alertas

Protección de la bios y del sistema operativo

- Arranque seguro mediante el Módulo de plataforma segura (TPM)

Sobrescritura de imagen y soporte de almacenamiento extraíble

- Sistema de seguridad de sobrescritura de disco (DOSS)
- Disco duro extraíble

Cifrado de datos

- Cifrado de disco duro mediante TPM
- Claves de cifrado mediante TPM
- Cifrado integral de archivos impresos y escaneados con clave PKI
- Disco duro con certificado FIPS (Estándar federal de procesamiento de información)
- Cifrado de impresión integral
- Cifrado de escaneo integral

Actualizaciones de firmware y gestión de contraseñas

- Auditoría de contraseña remota
- Función de bloqueo de usuario
- Validación del firmware mediante TPM

Cumplimiento de los estándares industriales

- Certificación ISO 27001
- Certificación IEEE 2600.2 para productos seleccionados
- Certificación ISO 15408 para productos seleccionados
- Documentación de seguridad y formación

ENFOQUE DE SEGURIDAD DEL DISPOSITIVO POR CAPAS DE RICOH

No hay duda de que el papel del proveedor de impresoras multifuncionales ha evolucionado más allá de la simple provisión de hardware transaccional y monodimensional hasta la actual gestión de datos. Las capacidades de las impresoras multifuncionales ahora abarcan la captura de información, desde las entradas multicanal hasta la clasificación de los datos capturados y la integración del flujo de trabajo hasta su análisis y almacenamiento seguro. En esta compleja red de estrictas normas y regulaciones y requisitos de conservación (junto con las amenazas internas y externas que ponen los datos en peligro de pérdida, destrucción o falsificación), hemos adoptado un enfoque de seguridad del dispositivo por capas para garantizar que su impresora multifuncional y el sistema al que se conecta le proporcionen la mejor protección posible.

1. El dispositivo

En el centro de cualquier modelo de Ricoh se encuentra el dispositivo. Estos están diseñados, fabricados e implementados teniendo en cuenta la seguridad como un requisito fundamental. El sistema operativo exclusivo de Ricoh no tiene las vulnerabilidades que presentan otros muchos sistemas operativos comerciales, y nuestros dispositivos cumplen con el estándar IEEE2600.2. La seguridad del cifrado del disco duro y la sobrescritura del disco garantizan que la información procesada sea confidencial.

2. El Smart Operation Panel (SOP) proporciona la interfaz de usuario

Al igual que las impresoras multifuncionales, el SOP utiliza el sistema operativo exclusivo de Ricoh. No se instalan componentes innecesarios y el acceso a raíz no está disponible. Ricoh ha trabajado muy duro para garantizar que la seguridad del dispositivo no se vea comprometida por la introducción del SOP.

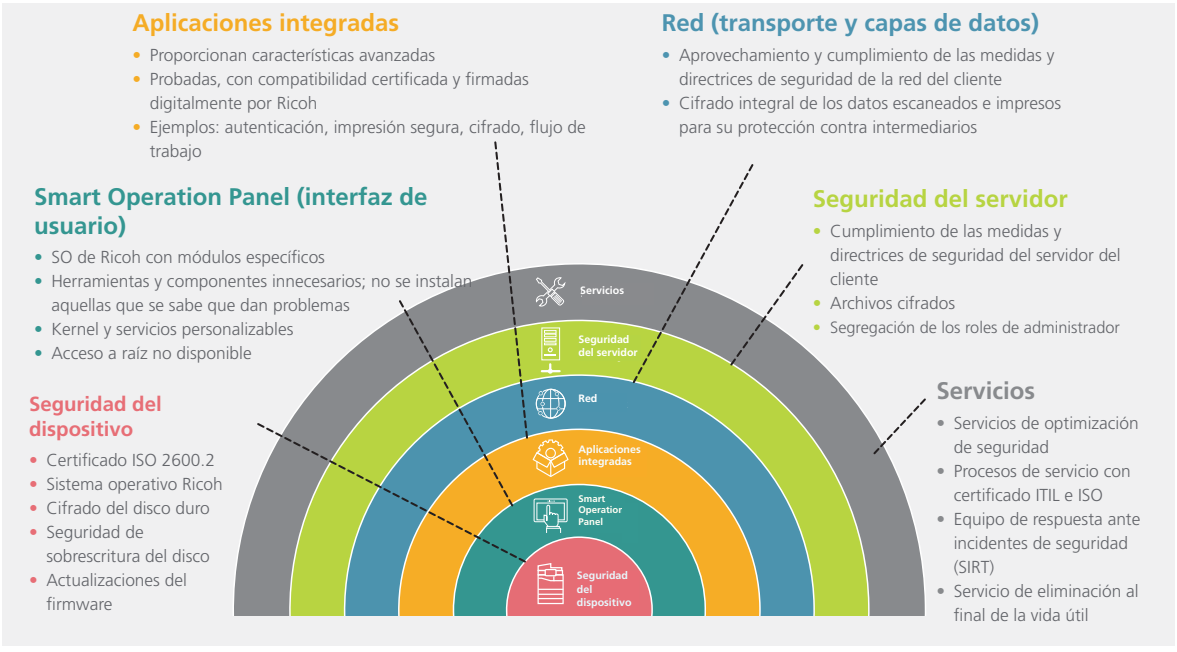
3. Aplicaciones inteligentes

Pueden integrarse en el SOP proporcionando una funcionalidad adicional al usuario, incluyendo flujo de trabajo y captura de datos. Algunas aplicaciones proporcionan características de seguridad esenciales. Entre ellas se incluyen las funcionalidades de impresión segura, tarjeta de acceso y cifrado. Las aplicaciones las desarrolla Ricoh u otros miembros de su programa de desarrollo, y todas las aplicaciones deben superar las pruebas de compatibilidad de Ricoh y firmarse digitalmente para poder ejecutarse en el SOP.

4. Red y servidores

Independientemente de quién gestione la infraestructura de TI, en Ricoh nos aseguramos de que nuestros productos y servicios cumplan con sus directrices de seguridad de red y TI. El cifrado integral de los archivos impresos y escaneados, el cifrado de datos en los servidores y la segregación de los derechos de administrador son técnicas utilizadas para proteger contra intermediarios o «trabajos internos».

Nuestra oferta incluye una amplia gama de servicios integrales de seguridad. Esto incluye servicios de gestión y asesoría para ayudar a los clientes a supervisar, optimizar y gestionar la seguridad de sus documentos e información. También disponemos de una gama de servicios de fin de vida útil para garantizar que las memorias RAM y los HDD de antiguos dispositivos de clientes se borren por completo antes de su eliminación.



CÓMO PROTEGE RICOH EL ENTORNO DE TRABAJO DIGITAL

Nuestros clientes presentan diversas preocupaciones con respecto a la seguridad, ya que en el mundo empresarial, cuando aumenta el volumen de datos, también lo hacen las vulnerabilidades, los ataques y las sanciones. Mantener la información confidencial, protegida e imposible de falsificar es una lucha constante. Por ejemplo, en Ricoh evitamos unos ocho mil millones de ataques de cortafuegos al mes. Hay decenas de miles de normativas sobre información confidencial a nivel industrial nacional y mundial, y las empresas deben ser capaces de demostrar el cumplimiento de cada una de ellas. Como es de esperar, las empresas de todos los tamaños buscan socios en los que poder confiar, que les ayuden a mantener la seguridad en un entorno digital.

Ricoh ha desarrollado una amplia gama de soluciones para mitigar los diversos riesgos a los que se enfrentan las empresas. Mientras el panorama de amenazas a la seguridad evoluciona rápidamente, en Ricoh trabajamos en nuestros programas basados en la "opinión del cliente" para continuar desarrollando y ofreciendo nuestros servicios.

Nuestros Consejos de clientes asesores funcionan como grupos de sondeo estratégicos clave. Los utilizamos para comprender mejor las tendencias, los impulsores y las prioridades que conforman las empresas de nuestros clientes. Nuestras Conferencias de asesoramiento tecnológico proporcionan información esencial de responsables clave en la toma de decisiones. Los equipos de ingeniería e I+D utilizan estas conferencias para escuchar valiosas opiniones de los clientes sobre ideas, conceptos y prototipos. Por último, Ricoh colabora con clientes individuales ayudándoles a desarrollar nuevas funciones de seguridad más avanzadas para clientes de mercados verticales y generales. Este enfoque orientado al cliente nos ayuda a validar nuestro plan de productos y ayuda a nuestros clientes a beneficiarse de una red global de servicios y asistencia.

El entorno de trabajo digital moderno debe ser tan dinámico como las amenazas cibernéticas a las que se enfrenta y tan flexible como las prácticas laborales que desarrolle. Por ello pensamos que la ciberseguridad debe funcionar a la perfección en cualquier tecnología que nuestro cliente elija para su entorno de trabajo. Nuestro compromiso con la norma ISO 27001 en toda nuestra empresa y la certificación IEEE 2600 en todos nuestros productos, junto con el sistema operativo exclusivo de Ricoh que les instalamos, hacen que los controles de seguridad y las prácticas recomendadas estén implementados, sea cual sea la solución que elija para estructurar y hacer crecer su empresa.

La combinación de amenazas de seguridad, requisitos legislativos y estándares industriales complejos implica que el potencial de daño reputacional y fiscal por riesgo cibernético nunca había sido tan grande. Ahora es el momento de trabajar con un socio de confianza que te ayude a mantener la seguridad de los activos más vulnerables de tu empresa y proteja sus aspiraciones futuras.

RICOH
imagine. change.

www.ricoh.es