Ricoh Seguridad Descripción General

RICOH
imagine. change.

¿Se está preguntando si sus dispositivos son vulnerables?

Las amenazas de seguridad ya no se limitan a computadoras personales, servidores o redes. Los dispositivos de impresión, incluso las impresoras láser básicas, necesitan contramedidas contra una amplia gama de amenazas. A medida que las impresoras multifunción se han convertido en verdaderos terminales de información, se han convertido en activos de TI básicos por derecho propio. La capacidad de computación de lo que tradicionalmente se ha categorizado como "Impresoras/Copiadoras" ha crecido, pero también tiene amenazas potenciales, que pueden incluir:

- Acceso malicioso a través de las redes
- El manejo y la alteración de la información a través de la red
- La información se filtra desde los medios de almacenamiento HDD
- Acceso no autorizado a través del panel de operación de un dispositivo
- Acceso inapropiado a través de líneas telefónicas de fax
- Fugas de información a través de una copia impresa
- Violaciones de la política de seguridad debido a descuidos

Simplemente esperar que no te ataquen no es la respuesta. La tecnología superior, el compromiso y el know-how son esenciales. Ricoh puede ayudarlo a abordar problemas potenciales causados por vulnerabilidades en sus dispositivos, los datos que procesan y las redes a las que se conectan.

Enfoque en capas de Ricoh

En el corazón de nuestro modelo de seguridad está el dispositivo en sí. El sistema operativo (SO) en el núcleo de nuestros dispositivos actuales diseñados por Ricoh ha sido diseñado y endurecido específicamente por Ricoh para nuestros equipos, y muchos de nuestros modelos de dispositivos MFP están certificados según el Perfil de protección estándar IEEE 2600.2 para dispositivos de copia impresa. El cifrado del disco duro y la seguridad de sobrescritura del disco vienen de serie en algunos de nuestros dispositivos y ayudan a garantizar que los datos procesados permanezcan confidenciales. Ricoh ha trabajado arduamente para garantizar que la seguridad del dispositivo no se vea debilitada por la introducción del Smart Operations Panel, que también utiliza un sistema operativo exclusivo de Ricoh. Ricoh no instala componentes innecesarios, y el acceso a la raíz no está disponible. Las aplicaciones integradas deben pasar las pruebas de compatibilidad de Ricoh y firmarse digitalmente antes de que puedan ejecutarse en el Panel de operación inteligente. Ricoh se compromete a trabajar con nuestros clientes para entregar productos y servicios que estén sincronizados con sus políticas de seguridad de TI y de red. Utilizamos una serie de técnicas para ayudar a proteger contra amenazas de "hombre en el medio" o "trabajo interno", incluido el cifrado de extremo a extremo de archivos de impresión y escaneo, el cifrado de datos en servidores y la segregación de tareas de administrador. Una gama de servicios de seguridad líder en la industria, que incluye consultoría y servicios administrados, envuelve a las otras capas para monitorear, optimizar y administrar de manera efectiva la seguridad de los documentos y la información.

Aplicaciones Incrustadas

- Proporcionar funciones extendidas
- Probadas, certificadas en cuanto a compatibilidad e firmadas digitalmente por Ricoh
- Ejemplos: autenticación, impresión segura, encriptado, flujo de trabajo

Red (capa de enlace de datos y transporte)

- Aproveche y cumpla con los requisitos del cliente de políticas y medidas de seguridad de red
- Encriptado de extremo a extremo de archivos de escaneo e impresión para protegerse del "hombre en el medio"

Interfaz de usuario (Panel de operación inteligente)

- Ricoh reforzó el sistema operativo basado en módulos específicos
- Herramientas y componentes innecesarios, herramientas con problemas conocidos no instalados
- Kernel y los servicios son personalizados
- El acceso raíz no está disponible

Seguridad del servidor

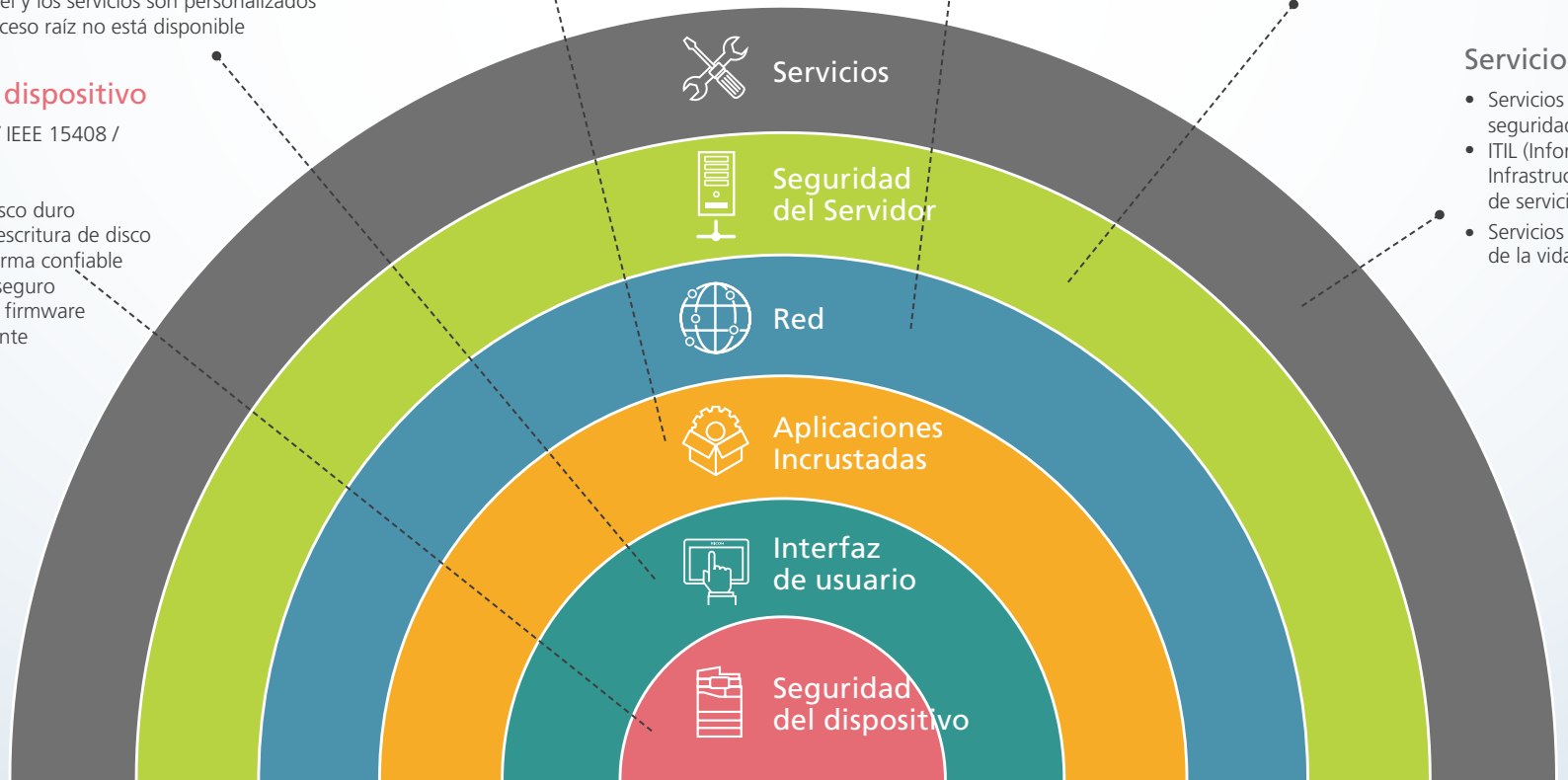
- Aproveche y cumpla con las políticas y medidas de seguridad del servidor del cliente
- Archivos encriptados
- Segregación de roles del administrador

Seguridad del dispositivo

- Certificación ISO / IEEE 15408 / IEEE 2600.2
- OS solo de Ricoh
- Encriptación del disco duro
- Seguridad de sobrescritura de disco
- Módulo de plataforma confiable para un arranque seguro
- Actualizaciones de firmware firmadas digitalmente

Servicios

- Servicios de optimización de seguridad
- ITIL (Information Technology Infrastructure Library) y procesos de servicio certificados ISO
- Servicios de eliminación al final de la vida útil



La seguridad es nuestro ADN

Los dispositivos Ricoh están diseñados, fabricados e implementados con la seguridad como requisito básico. El pensamiento centrado en la seguridad está presente desde el principio en todo, desde el diseño del producto hasta las ventas. Está en nuestro ADN, informando tanto nuestra filosofía de diseño como nuestro compromiso de trabajar continuamente para apoyar a nuestros clientes con soluciones a medida que las amenazas evolucionan.

Gobernanza de la información y seguridad cibernética

La experiencia, capacidades y servicios de seguridad de Ricoh también se extienden más allá del dispositivo (consulte la página 33).

Seguridad del dispositivo

Las capacidades de seguridad de nuestros dispositivos pueden ayudar a proteger los dispositivos multifunción y las impresoras láser contra posibles amenazas, como el compromiso del firmware, la unidad de disco duro de un dispositivo, la memoria no volátil, los puertos de red abiertos y el sistema de autenticación. Ricoh obtuvo la certificación para una amplia gama de productos basados en Common Criteria (ISO / IEC 15408). En dispositivos que se someten a la certificación Common Criteria, las funciones de seguridad son probadas por laboratorios externos independientes con licencia del gobierno para garantizar que las características de seguridad funcionen correctamente y se ajusten a las normas establecidas tanto por el gobierno como por la industria.

Como parte de nuestro compromiso continuo para evitar que sus activos de información importantes estén expuestos a amenazas, desarrollamos y ofrecemos características de seguridad y productos para ayudar a proteger sus documentos electrónicos y en papel, sin obstaculizar los procesos fáciles de usar y la productividad

El firmware inseguro Puede verse comprometido

Actualizaciones de firmware firmadas digitalmente

Si un MFP o software integrado de la impresora, también conocido como firmware, es alterado o comprometido, ese dispositivo puede ser utilizado como un método de intrusión en la red corporativa, como un medio para dañar el dispositivo o como una plataforma para otros fines maliciosos. Los dispositivos diseñados por Ricoh se crean usando un Trusted Platform Module (TPM) solo de Ricoh y están diseñados para que no arranque si el firmware se ha visto comprometido. El TPM de Ricoh es un módulo de seguridad de hardware que valida los programas centrales del controlador, el Sistema operativo, BIOS, cargador de arranque y firmware de aplicación

El MFP de Ricoh y las impresoras usan una firma digital para juzgar la validez del firmware: la clave pública usada para esta verificación se almacena en una región protegida por sobre escritura y no volátil del Trusted Platform Module (TPM) de Ricoh. Una clave de encriptado raíz y las funciones criptográficas también se encuentran dentro del TPM ay no pueden ser alteradas desde el exterior. Ricoh usa un procedimiento de Trusted Boot que emplea dos métodos para verificar La validez de los programas/firmware:

1. Detección de alteraciones
2. Validación de firmas digitales

Un dispositivo de Ricoh no arrancará a menos que se haya verificado que sus programas/firmware son auténticos y seguros para los usuarios.

Los datos temporales son Datos vulnerables

Sistema DataOverwriteSecurity (DOSS)

Cuando un documento es escaneado o cuando se reciben datos desde una PC, Algunos datos pueden almacenarse temporalmente en el disco duro o en la memoria hecho a medida. Esto puede incluir datos de escaneo/impresión/copiado, datos ingresados por el usuario y configuración del dispositivo. Estos datos temporales (o “latentes”) representan una vulnerabilidad potencial de seguridad.

El Sistema DataOverwriteSecurity (DOSS) de RICOH cierra esta vulnerabilidad, destruyendo los datos temporales almacenados en el disco duro de MFP sobrescribiéndolos con secuencias al azar de “1” y “0.” Los datos temporales se sobrescriben de forma activa y se borran cada vez que se ejecuta un trabajo.

- Cumple con las recomendaciones de la Agencia de Seguridad Nacional (NSA) y del Departamento de Defensa (DoD) para el manejo de información clasificada
- Hace que sea virtualmente imposible acceder a datos latentes de trabajos de copia / impresión / escaneo / fax una vez que el proceso de sobrescritura se completa (el proceso de sobrescritura se puede seleccionar de 1 a 9 veces)
- Funciona con el sistema de seguridad RICOH de Disco duro extraíble (RHD), que proporciona un enfoque de varias capas
- Ayuda a los clientes a cumplir con los requisitos de HIPAA, GLBA y FERPA
- Proporciona información visual sobre el proceso de sobrescritura (es decir, completado o en proceso) con un simple icono de panel de visualización

El encriptado protege Contra el robo de datos

Encriptación del disco duro

Incluso si el disco duro se elimina físicamente de una máquina Ricoh, los datos encriptados pueden leerse. La función de encriptado del disco duro puede ayudar a proteger el disco duro de una impresora multifunción contra el robo de datos mientras que ayuda a las organizaciones a cumplir con las políticas de seguridad empresariales. El encriptado incluye datos almacenados en un libro de direcciones del sistema, reduciendo el riesgo de que los empleados, clientes o proveedores de una organización vean amenazada su información de forma Inadecuada potencialmente. Los siguientes tipos de datos, que se almacenan en la memoria no volátil o disco duro de las impresoras multifunción, pueden encriptarse:

- Libro de direcciones
- Datos de autenticación del usuario
- Documentos almacenados
- Documentos almacenados temporalmente
- Registros
- Configuraciones de interfaz de red
- Información de configuración

Ricoh ofrece un encriptado del disco duro usando la metodología Advanced Encryption Standard (AES) a 256 bits.

¿Su línea de fax le proporciona una entrada?

Seguridad de la línea de fax

La habilitación de la función de fax de un dispositivo puede significar conectarla al exterior a través de una línea telefónica, lo que significa que es crítico bloquear el acceso no autorizado a través de la línea de fax. El software Ricoh incrustado está diseñado para procesar solo los tipos de datos apropiados (es decir, datos de fax) y enviar esos datos directamente a las funciones adecuadas dentro del dispositivo. Debido a que solo se pueden recibir datos de fax de la línea de fax, se elimina la posibilidad de acceso no autorizado desde la línea de fax a la red o a programas dentro del dispositivo.

Ricoh utiliza una serie de métodos para ayudar a asegurar las operaciones de fax:

- El controlador de fax solo contiene un módem de fax y no un módem de datos, por lo que todas las comunicaciones se realizan a través del protocolo de fax G3.
- Los datos de la imagen no se guardan en la memoria de la página del controlador del motor ni en el área de almacenamiento temporal, lo que imposibilita el acceso a estos datos desde el controlador de fax.
- Los datos almacenados en la memoria de la página del controlador del motor o en el área de almacenamiento temporal se envían solo a la unidad de impresión.
- No hay conexión activa entre los buses de video de impresión / escaneo y el controlador del motor, por lo que es imposible acceder a los datos almacenados en la memoria de la página del controlador del motor o Área de almacenamiento temporal del controlador de fax.
- Los datos de ubicación de la página se borran al finalizar cada trabajo.

Certificación de seguridad independiente

IEEE 2600

El estándar de seguridad IEEE 2600 define los requisitos mínimos para las características de seguridad utilizadas por los dispositivos que requieren un alto nivel de seguridad del documento, estableciendo una línea de base común de expectativas de seguridad para impresoras multifunción e impresoras. Para garantizar que un dispositivo demuestre conformidad con el estándar establecido, un laboratorio externo independiente prueba y proporciona verificación de las características de seguridad del fabricante.

Estas áreas, que han sido identificadas como las más vulnerables por una posible violación de datos, han sido validadas en muchos dispositivos Ricoh según el estándar IEEE 2600 y se pueden habilitar:

- Identificación de usuarios y sistemas de autenticación
- Tecnología de encriptación de datos disponible para impresoras multifunción
- Validación del firmware del sistema
- Separación de la línea de fax analógica y el controlador de copia / impresión / escaneo
- Validación de algoritmos de cifrado de datos
- Operación de seguridad de sobrescritura de datos

Ricoh ofrece una amplia línea de impresoras multifunción e impresoras que han sido certificadas conforme al estándar de seguridad IEEE 2600— y nuestra línea de productos se mejora constantemente para cumplir con los requisitos cambiantes de nuestros clientes.

Controlar el acceso y reducir riesgos

Autenticación del usuario del dispositivo

Las funciones de autenticación permiten que los usuarios autorizados accedan a una impresora multifunción Ricoh, mientras que se impide el acceso a las que no tienen las credenciales adecuadas. Ricoh también le brinda la capacidad de controlar el nivel de capacidades otorgadas a cada usuario o grupo de usuarios. Esto puede incluir la restricción de la capacidad de cambiar la configuración de la máquina y ver las entradas de la libreta de direcciones o la concesión de acceso a flujos de trabajo de escaneo particulares, servidores de documentos y otras funciones. Además, la función de Bloqueo de usuario, que se activa si detecta una alta frecuencia de intentos de inicio de sesión exitosos o fallidos, ayuda a protegerse contra un ataque de denegación de servicio o una contraseña de fuerza bruta..

Los métodos de autenticación incluyen:

- Autenticación básica: los usuarios ingresan un nombre de usuario y una contraseña, que están registrados localmente en la libreta de direcciones de la impresora multifunción.
- Autenticación del código de usuario: los usuarios ingresan un código de hasta 8 dígitos, que se compara con los datos registrados en la libreta de direcciones.
- Autenticación de Windows / LDAP: el acceso a las impresoras multifunción Ricoh se puede vincular con los controladores de dominio de Windows® y los servidores LDAP.
- Autenticación de tarjeta: en lugar de ingresar un nombre de usuario y contraseña, un usuario tiene una tarjeta debidamente registrada sobre un lector de tarjeta opcional para la autenticación.
- Autenticación de tarjeta de acceso común (Common Access Card, CAC): Common Access Card es un sistema de autenticación basado en una tarjeta de identificación especializada del Departamento de Defensa de EE. UU., Diseñado para usuarios gubernamentales que deben cumplir con la Directiva Presidencial de Seguridad Nacional 12 (HSPD-12).
- Verificación de identidad personal (PIV): la verificación de identidad personal es la versión civil de la tarjeta CAC.
- Solución de autenticación de tokens SIPRNet: el token SIPRNet es una variación de la ID de CAC, diseñada para redes controladas

Seguridad de datos

Es fácil perder información accidentalmente. Un documento dejado en la bandeja de una impresora multifunción puede convertirse en un riesgo de seguridad tan fácil como un archivo digital mal utilizado o el impacto de un error humano. Las impresoras multifunción Ricoh ayudan a proteger sus datos ya sea que imprima, copie, escanee o envíe faxes. El sistema de encriptación de datos de Ricoh, que utiliza un módulo de cifrado criptográfico RSSA BSAFE y está validado por FIPS 140-2, ayuda a proteger sus datos tanto cuando está en tránsito como cuando está en reposo.

174 millones

De registros digitales se vieron comprometidos por los intrusos de datos en 2011, un aumento de más de 4.000 % con respecto a 2010.*

*Verizon® 2012 Reporte de Investigaciones de Incumplimiento de Datos

Ricoh ayuda a proteger sus datos con tecnologías y funciones que están diseñadas para respaldar políticas de seguridad, proteger contra el uso indebido o descuido y fomentar el cumplimiento a través de la responsabilidad.

Protección para documentos digitalizados

Garantizar soluciones de escaneo

El proceso de digitalizar documentos en papel y enrutar los archivos electrónicos resultantes, ya sea para respaldar sistemas o por correo electrónico, puede ser un punto de compromiso de los datos si no se asegura adecuadamente. Los procesos de escaneo, aunque diseñados para que sean fáciles para los usuarios, también deberían ofrecer una protección sólida para la información digital enrutada. Esto comienza con la restricción de acceso. Limite las operaciones de escaneo a usuarios autorizados solo con varias opciones de autenticación, incluso a través de inicio de sesión de red, autenticación Kerberos opcional o inicio de sesión único a través de la tarjeta.

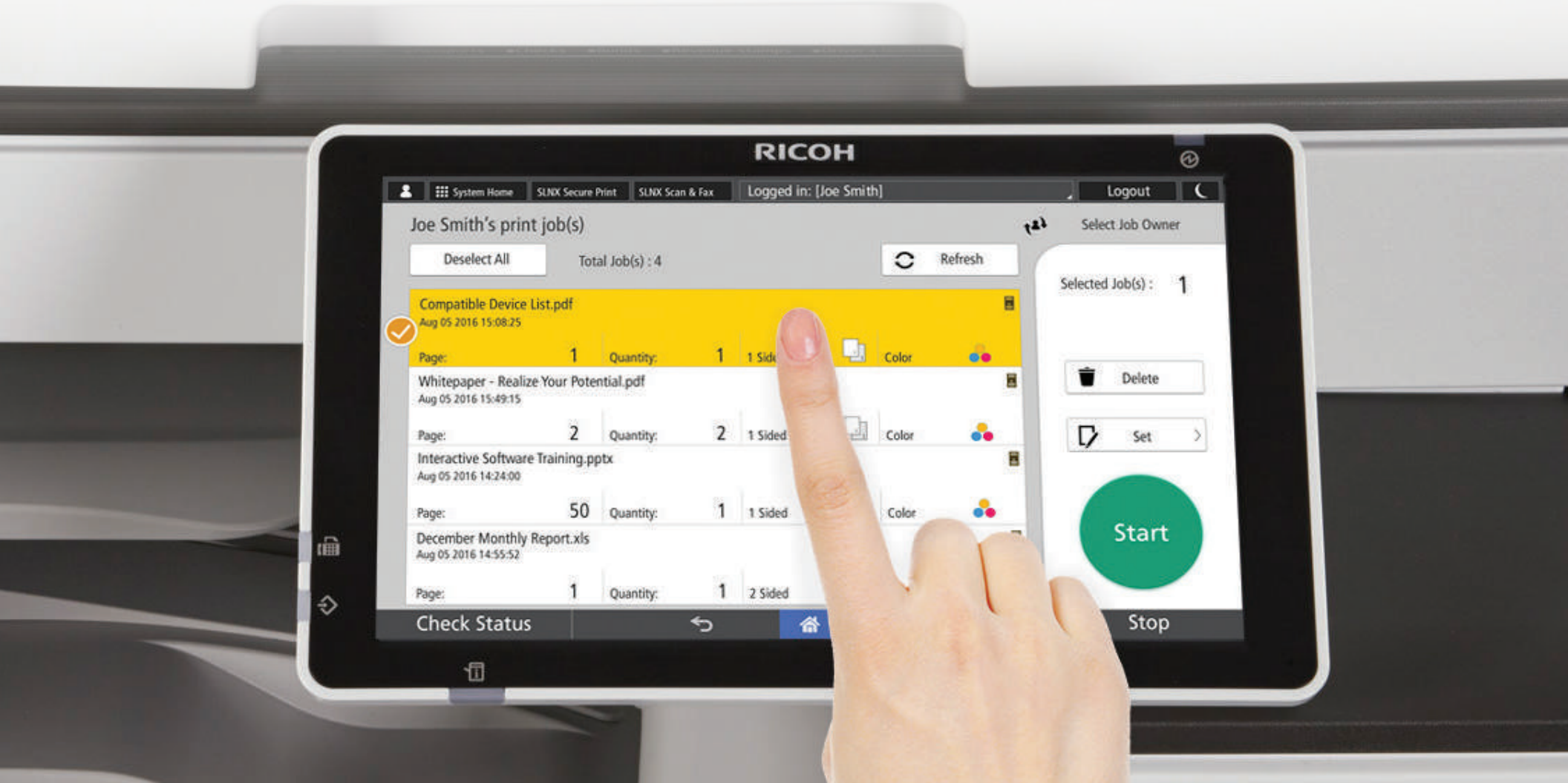
El cifrado de las comunicaciones de escaneo a correo electrónico ayuda a reducir el riesgo de compromiso de la información. Envíe mensajes de correo electrónico utilizando criptografía de clave pública y un certificado de verificación de usuario que se haya registrado en la libreta de direcciones del dispositivo de escaneo. También puede evitar la suplantación de correo electrónico y la alteración del mensaje adjuntando una firma electrónica que utiliza una clave secreta, basada en un certificado de dispositivo.

Las impresoras, copiadoras y escáneres multifunción diseñadas por Ricoh están equipadas con protocolos Secure Sockets Layer (SSL) y Transport Layer Security (TLS) y pueden utilizar algoritmos de cifrado potentes (AES y SHA-2 de 256 bits), así como proporcionar pistas de auditoría y control administrativo.

Las impresiones desatendidas pueden filtrar información

Locked Print

Los documentos impresos que se encuentran en la bandeja de papel o que se dejan al descubierto pueden ser recogidos por cualquier persona. Esto pone en riesgo la información del documento y el impacto potencial aumenta dramáticamente al imprimir documentos confidenciales. Las capacidades de impresión bloqueada de Ricoh pueden contener documentos cifrados en el disco duro del dispositivo hasta que llegue el propietario del documento e ingrese el código PIN correcto. Además de esta función de impresión bloqueada basada en el controlador, Ricoh también ofrece impresión bloqueada mejorada, que está vinculada a las cuentas de usuario y se puede combinar con la autenticación de la tarjeta. Para una capacidad aún mayor, un software como RICOH Streamline NX (en la imagen) puede proporcionar una liberación de documentos segura con todas las características, brindando a los usuarios opciones sobre su cola de impresión segura y permitiendo a los administradores mantener el control.

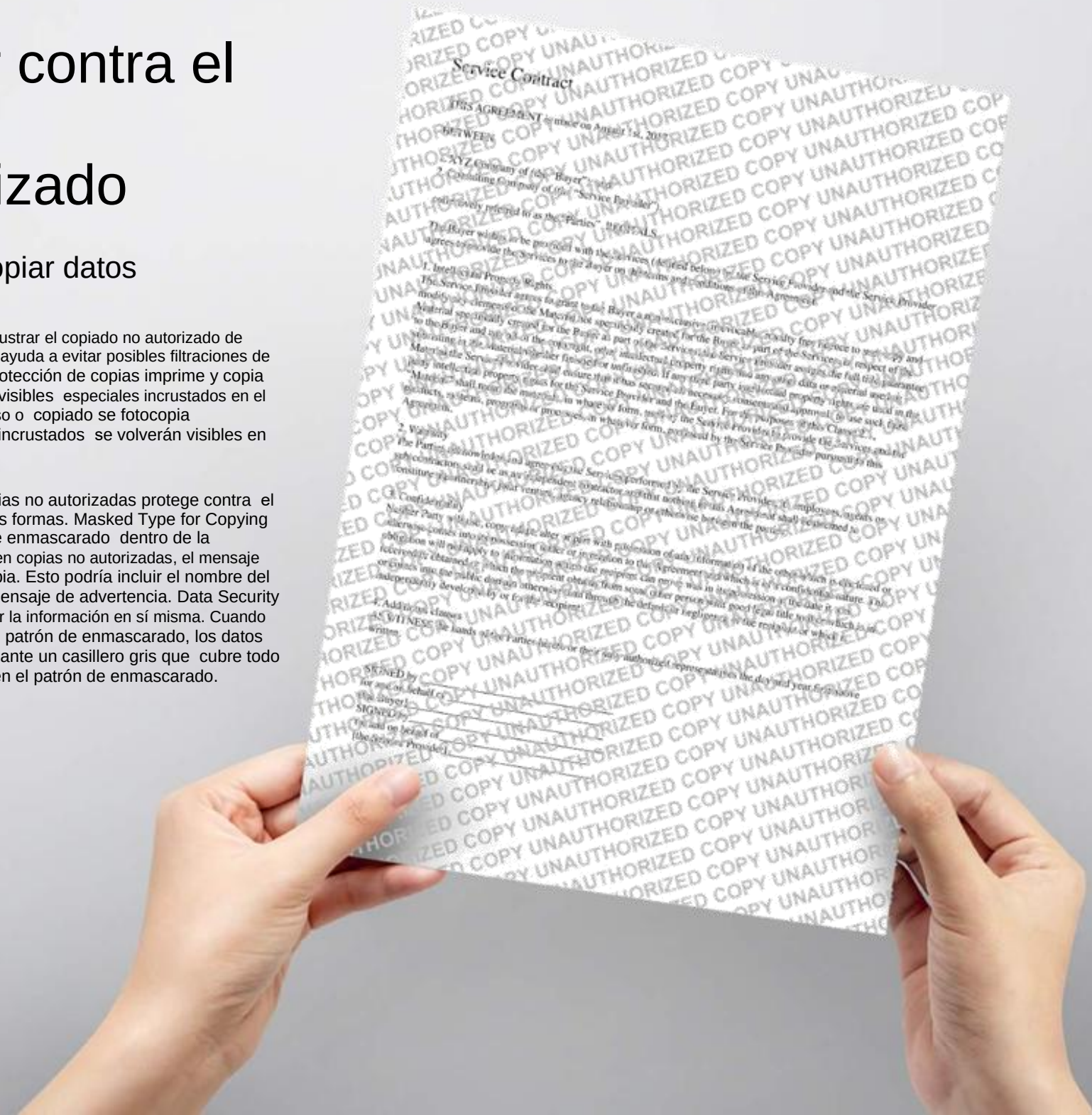


Proteger contra el copiado no autorizado

Seguridad de copiar datos

Ricoh ofrece funciones para frustrar el copiado no autorizado de documentos en papel, lo que ayuda a evitar posibles filtraciones de información. La función de protección de copias imprime y copia documentos con patrones invisibles especiales incrustados en el fondo. Si el documento impreso o copiado se fotocopia nuevamente, y los patrones incrustados se volverán visibles en las copias.

La función de control de copias no autorizadas protege contra el copiado no autorizado en dos formas. Masked Type for Copying incrusta un patrón y mensaje enmascarado dentro de la impresión original. Si se hacen copias no autorizadas, el mensaje incrustado aparece en la copia. Esto podría incluir el nombre del autor del documento o un mensaje de advertencia. Data Security for Copying ayuda a proteger la información en sí misma. Cuando el dispositivo Ricoh detecta el patrón de enmascarado, los datos impresos se oscurecen mediante un casillero gris que cubre todo menos un margen de 4mm en el patrón de enmascarado.



Los documentos anónimos son difíciles de controlar

Impresión obligatoria de informaciones de seguridad

Selle los documentos con la información clave de identificación para una mayor responsabilidad y control de gestión. La impresión de información de seguridad obligatoria es una función que obliga a imprimir información clave, como quién imprimió un documento, cuándo se imprimió y desde qué dispositivo, con un documento. Esta función se puede habilitar para las funciones de copia, impresión, fax y servidor de documentos. Los administradores pueden seleccionar la posición de impresión y qué tipo de información se imprimirá automáticamente en la salida, lo que puede incluir:

- Fecha y hora en que se imprimió el trabajo
- Nombre o ID de usuario de inicio de sesión que imprimió el trabajo
- Dirección IP y/o número de serie del dispositivo usado

Dispositivos seguros contra el uso indebido

Contabilidad y recuperación de costos

El uso incontrolado del equipo de imágenes puede ocasionar gastos imprevistos y posibles violaciones de las políticas de la compañía. El software de contabilidad y recuperación de costos Ricoh rastrea el uso hasta el individuo y automatiza el proceso de asignación de costos a los usuarios o departamentos. Crear una mayor responsabilidad estableciendo cuotas de usuarios y límites de cuentas presupuestarias. Establezca permisos de usuario para restringir el acceso a ciertas funciones según la necesidad, por ejemplo, la capacidad de imprimir en color. Controlar quién puede usar el equipo a través de la autenticación y designar lo que puede o no puede hacer, reduce las oportunidades de uso indebido y proporciona información de gestión útil.

Seguridad de red

Las impresoras multifunción intercambian información crítica con computadoras y servidores a través de redes. Si quedan desprotegidas, esta información está en riesgo de sufrir alteraciones a manos de aquellos con intenciones maliciosas que ingresan En las redes. Los productos y las tecnologías de Red Ricoh ofrecen características que pueden ayudar a proteger contra el acceso no autorizado. Las técnicas empleadas incluyen encriptado de comunicaciones de red y flujos de impresión, Autenticación de usuario de red y un puñado de contramedidas administrativas, como cerrar puertos de red y la gestión de dispositivos proactivos

Las funciones de seguridad de Ricoh pueden ayudar a reducir el riesgo de explotación de la red o de fuga de información derivada de una impresora o dispositivo multifuncional dañado.

Los usuarios no autorizados pueden ser una amenaza

Autenticación de usuario de red

Los dispositivos Ricoh admiten la autenticación de usuarios de red para limitar el acceso a usuarios autorizados. Por ejemplo, la autenticación de Windows® verifica la identidad de un usuario en la impresora multifunción comparando las credenciales de inicio de sesión (nombre de usuario y contraseña) con la base de datos de usuarios autorizados en el servidor de red de Windows. En el caso del acceso a la libreta de direcciones global, la autenticación LDAP valida al usuario contra el servidor LDAP (Protocolo ligero de acceso a directorios), por lo que solo aquellos con un nombre de usuario y contraseña válidos pueden buscar y seleccionar direcciones de correo electrónico almacenadas en el servidor LDAP.

Software como RICOH Streamline NX, un conjunto modular que abarca procesos de escaneo, fax, impresión, administración de dispositivos, seguridad y contabilidad, brinda opciones adicionales de autenticación de red. Estos incluyen autenticación contra LDAP, autenticación Kerberos y un SDK disponible para integraciones personalizadas.

Hacer dispositivos "invisibles" al exterior

Cerrar los puertos de red no utilizados

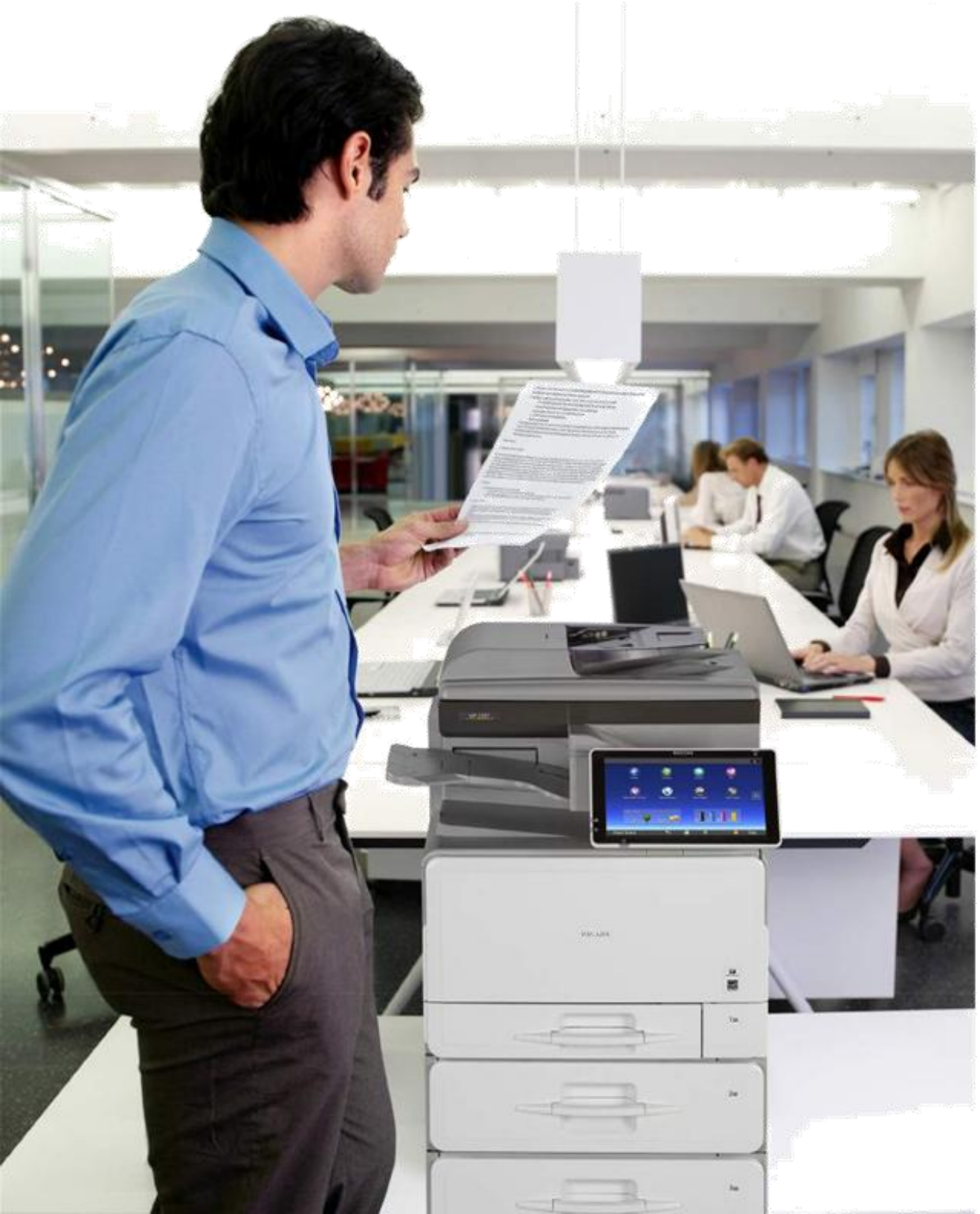
En un esfuerzo por facilitar la incorporación de dispositivos de red, muchos de los proveedores de red habilitados se envían rutinariamente al cliente con todos los puertos configurados como "abiertos", pero los puertos abiertos no utilizados en impresoras y equipos multifunción presentan un riesgo de seguridad. Los puertos comprometidos pueden conducir a diversas amenazas externas, incluida la destrucción o falsificación de datos almacenados, ataques de denegación de servicio (DoS) y virus o malware que ingresan a la red. Existe una solución simple pero a menudo olvidada para esta fuente de riesgo en particular: cerrar los puertos. Los administradores de dispositivos de Ricoh pueden bloquear fácilmente los puertos de red innecesarios, lo que ayuda a que los dispositivos sean prácticamente "invisibles" para la piratería. Además, los protocolos específicos, como SNMP o FTP, pueden desactivarse por completo para eliminar el riesgo de que sean explotados.

Los datos no encriptados en la red están en riesgo

Encriptado de red

A medida que los datos se mueven a través de la red, es posible que un pirata informático experto intercepte flujos de datos sin formato, archivos y contraseñas. Sin protección, la información inteligible se puede robar, modificar o falsificar y volver a insertar en la red con intención maliciosa. Ricoh utiliza protocolos robustos de seguridad de red que también se pueden configurar de acuerdo con las necesidades de los clientes. El protocolo Transport Layer Security (TLS) se utiliza para ayudar a mantener la integridad de los datos que se comunican entre dos puntos finales.

Los dispositivos Ricoh son compatibles con WPA2, WPA2-PSK mediante el cifrado AES (acceso protegido Wi-Fi), un sistema de encriptación para redes inalámbricas que proporciona una mayor seguridad que el sistema de cifrado convencional WEP (privacidad equivalente por cable). WPA2, WPA2-PSK cuenta con una función de autenticación de usuario y un protocolo de cifrado llamado CCMP (AES), que actualiza automáticamente la clave de cifrado en ciertos intervalos.



Los datos enviados a las impresoras podrían ser explotados

Cifrado de flujo de impresión

Los datos enviados en una secuencia de impresión pueden explotarse si no están encriptados y capturados en tránsito. Ricoh puede habilitar el cifrado de datos de impresión mediante Capa de sockets seguros / Seguridad de la capa de transporte (SSL / TLS) a través del Protocolo de impresión de Internet (IPP), encriptando datos de estaciones de trabajo a dispositivos de red o impresoras multifunción. Esto se puede lograr usando IPP sobre SSL / TLS. Debido a que este es un protocolo que ayuda a mantener la integridad de los datos, los intentos de interceptar flujos de datos de impresión cifrados en tránsito solo producirán datos indescifrables.

Manejar dispositivos puede consumir mucho tiempo

Device Manager NX

Debido a que la administración de dispositivos puede consumir mucho tiempo, las brechas de seguridad pueden surgir involuntariamente cuando los aspectos de la administración adecuada del dispositivo no se atienden. El software de administración de dispositivos Ricoh como Device Manager NX y Streamline NX brinda a los administradores de TI un punto de control central para monitorear y administrar un número virtualmente ilimitado de dispositivos de impresión conectados a la red, ya sea distribuido en múltiples servidores o regiones geográficas. Las comunicaciones cifradas SNMPv3 se utilizan para supervisar el estado operativo de los dispositivos y sus servicios, incorporando autenticación de usuario y funciones de cifrado de datos que ayudan a proteger los datos del usuario y la información del dispositivo de red.

Con el control central, los administradores pueden determinar quién puede acceder y usar un dispositivo o impresora multifunción, monitorear la configuración de DataOverwriteSecurity Solution (DOSS) y administrar los certificados del dispositivo. Las tareas automatizadas también pueden reducir la exposición del firmware desactualizado. El firmware del dispositivo Ricoh se compara con la versión de firmware aprobada por el cliente o con el último firmware disponible para el dispositivo del Centro de software global de Ricoh. Si el firmware es diferente, el firmware correcto se puede implementar en el dispositivo automáticamente.

Ayuda a los proveedores de servicios a responder rápidamente

@Remote

El @Remote Connector NX de Ricoh recopila alertas de servicios críticos que están por venir y puede comunicarlos directamente a su Proveedor de servicios usando

un método seguro. Su proveedor puede programar actualizaciones de firmware remotas, utilizando el conector para enviar actualizaciones críticas de inmediato. El @Remote Connector también recopila medidores de dispositivos y los pone a disposición en un cronograma predefinido, junto con notificaciones de niveles de consumibles, para mantener el tiempo de actividad y reducir la carga administrativa.

Programas y recursos

Las organizaciones que usan y almacenan información médica, información financiera, información de identificación personal (PII) u otros tipos de datos confidenciales pueden estar sujetas a varios requisitos reglamentarios, como HIPAA, Gramm-Leach-Bliley o la Ley de privacidad de derechos de educación familiar. Ya sea que su organización necesite adherirse al cumplimiento externo o demostrar soporte de sus propias políticas de seguridad, Ricoh puede ayudarlo.

Brindamos a nuestros clientes programas y recursos para ayudarlos a satisfacer sus requisitos específicos de cumplimiento normativo.

En Ricoh, brindamos soporte a nuestros clientes brindándoles la asistencia técnica necesaria, el conocimiento y la capacitación y la documentación de seguridad relacionada con nuestros equipos. Además, también ofrecemos la eliminación de datos del equipo de fin de vida útil como un servicio

Programas del final de vida útil del equipo

La información latente en los equipos retirados puede presentar un riesgo de seguridad hasta que se destruya por completo. En caso de verse comprometidos, terceros malintencionados podrían usar la información adquirida para una infracción de seguridad mayor. Los programas de Ricoh limpian la información de los equipos al final de su vida útil o cuando se devuelven al finalizar un contrato de arrendamiento o alquiler.

Servicios de sobreescritura del disco duro

Por lo general, se realiza cuando un dispositivo se retira del servicio o cuando concluye una concesión de equipo, el Servicio de sobrescritura de datos sobrescribe completamente los datos del cliente en el disco duro de la máquina. Se encuentran disponibles varios métodos de sobrescritura de datos, incluidos los métodos que cumplen con la Agencia Nacional de Seguridad (NSA) y el Departamento de Defensa (DoD). Además, NV-RAM se inicializa a los valores predeterminados para evitar que la información identificable, como direcciones IP, libretas de direcciones y otros datos administrativos, quede expuesta a terceros.

Servicios de eliminación del disco duro

El programa Hard Drive Surrender permite a los clientes retener su MFP o disco duro de la impresora al final de un arrendamiento o en la vida útil de la máquina. Un técnico certificado de Ricoh retira el disco duro antes de que salga del sitio del cliente y lo transfiere a la custodia de un representante del cliente. Los clientes mantienen el control de su información y pueden elegir destruirla a través del método que elijan.

Servicios de limpieza de MFP

El servicio de limpieza de MFP de Ricoh está diseñado para eliminar toda la información de identificación de un MFP o impresora antes de que ese dispositivo deje la ubicación del cliente. La información almacenada en la memoria del dispositivo, como las libretas de direcciones y la información de la dirección de red, se elimina. También se eliminan las marcas identificativas, como las etiquetas que mencionan los nombres de los departamentos, las direcciones IP y la información del servicio de atención al cliente, junto con cualquier papel o material de formulario específico del cliente. La eliminación de dicha información puede ayudar a evitar intentos maliciosos de recopilar información de TI de una organización.

Soporte técnico nacional/global

Ricoh ha establecido Centros de Tecnología en cada región para proporcionar soporte técnico a nuestros clientes en todo el mundo, respondiendo a sus necesidades de manera rápida y eficiente. El equipo de Ricoh Global Services brinda soluciones integrales, consistentes y de extremo a extremo. Con cobertura en aproximadamente 200 países y territorios en todo el mundo, Ricoh emplea a más de 30.000 profesionales de prestación de servicios. Nuestra red de soporte de ventas directas y distribuidores sin competencia tiene la capacidad de atender al 95 % de los empleados de la compañía Fortune Global 500, lo que significa que puede confiar en un socio para todas sus necesidades globales. Al contar con oficinas y profesionales de prestación de servicios en tantos países en todo el mundo, podemos responder rápidamente a las solicitudes de los clientes, independientemente de donde se encuentren.

Documentación de respaldo de seguridad

Ricoh proporciona documentación técnica para respaldar los requisitos de seguridad de la información de nuestros clientes, incluidos los documentos de certificación IEEE 2600 e ISO 15408 para determinadas ofertas de productos. Esta documentación proporciona la validación independiente de terceros de las afirmaciones de seguridad y puede proporcionarse previa solicitud. Además, los Documentos informativos de seguridad que cubren dispositivos y configuraciones de red y las Guías de Instalación de Seguridad de Dispositivos también están disponibles para los clientes. Estas guías proporcionan información detallada sobre cómo el equipo Ricoh comunica los datos dentro del dispositivo y cómo el dispositivo interactúa con la red.

Capacitación para usuarios finales y administradores

Mantener un alto grado de vigilancia y cumplir con las mejores prácticas de seguridad implica más que solo tecnología: involucra a las personas. Ricoh ofrece capacitación en nuestros dispositivos dirigidos tanto a los usuarios finales como a los administradores. Con el conocimiento correcto al alcance de la mano, su equipo puede comprender las capacidades de seguridad disponibles y aprender cómo su uso adecuado puede ayudar a su organización a proteger su información y cumplir con las políticas.

Seguridad más allá del dispositivo

Las mejores prácticas de seguridad exigen una "defensa en profundidad" que vaya más allá del dispositivo. Ricoh se está ocupando de las preocupaciones de seguridad en expansión de nuestros clientes a través de Gobernanza, Riesgo y Cumplimiento (Governance, Risk and Compliance, GRC) y Servicios de Seguridad Administrados. Estos servicios abarcan el ciclo de vida de los datos y la evaluación y gestión de riesgos, eDiscovery, seguridad del servidor y de punto final, acceso a la identidad, seguridad del correo electrónico y protecciones contra amenazas de red avanzadas.

Busque a Ricoh para obtener ayuda con sus principales desafíos de seguridad

Pérdida/robo de datos

La pérdida de datos es el núcleo de las inquietudes sobre el liderazgo del nivel C, y mantener los datos confidenciales y seguros es una lucha constante. Los atacantes buscan continuamente una brecha en su armadura que pueda ser explotada. El equipo de imágenes de Ricoh puede ser un componente clave de la prevención de pérdida de datos.

Corrupción/alteración de datos

Los ataques de virus que aparecen en los titulares mundiales destacan cuán vulnerables son todas las organizaciones a los ciberataques. Malware, Virus, Troyanos y Gusanos atacan plataformas ampliamente implementadas con vulnerabilidades bien conocidas. Las plataformas de Ricoh, aunque ampliamente implementadas, utilizan sistemas operativos propietarios para frustrar los intentos de alteración.

Disponibilidad de los datos

La disponibilidad de información y datos es un acto de equilibrio multifacético entre permitir e impedir el acceso. Los productos de Ricoh abordan tanto al acelerar el intercambio de información sancionado a través de la impresión, copiado, escaneo y enrutamiento, aplicando controles de esos procesos, encriptando datos en tránsito y determinando quién puede consumir la información procesada por nuestro equipo.

Entender las normativas

Las organizaciones deben observar numerosas regulaciones globales, nacionales e industriales, sin mencionar las políticas de seguridad interna de la compañía y los requisitos de auditoría. Ricoh proporciona herramientas y experiencia para respaldar las necesidades relacionadas con el cumplimiento de nuestros clientes.

Probar el cumplimiento

Las sanciones por incumplimiento pueden ser severas, y las nuevas reglamentaciones están elevando el nivel de posibles impactos comerciales adversos. La documentación adecuada es fundamental para demostrar efectivamente el cumplimiento. La certificación IEEE 2600 proporciona validación independiente por parte de terceros de que los reclamos de seguridad de TI operan según lo anunciado. Ricoh puede proporcionar esta certificación, junto con otra documentación, para ayudar a nuestros clientes.

Inicie una evaluación de riesgos de seguridad

Una evaluación de riesgos de seguridad realizada por Ricoh abarca hardware, software y datos, y se basa en estándares NIST* aceptados. Los puntajes de riesgo de bajo a alto se calculan en base a los estándares del Gobierno Federal de EE. UU. y del Departamento de Defensa**, junto con una expectativa de pérdida anual (annual loss expectancy, ALE) para los activos de datos, hallazgos y recomendaciones. La evaluación de riesgos de seguridad informa el posterior plan de gestión de riesgos, la creación de políticas, las acciones de corrección de riesgos y la auditoría externa independiente.

Comprometa a nuestros profesionales de seguridad

Los clientes buscan organizaciones en las que puedan confiar y que puedan ayudarlos a mantenerse seguros y demostrar el cumplimiento. Ricoh se compromete a proporcionar a nuestros clientes la mejor tecnología, servicios, programas y recursos, junto con la voluntad de ayudar a nuestros clientes a cumplir con sus requisitos de política de seguridad. Si tiene alguna pregunta o desea obtener más información, contacte a su profesional de ventas de Ricoh o visite nuestro sitio web.

Conozca más en **www.Ricoh-USA.com**.

** Instituto Nacional de Estándares y Tecnología*

*** Departamento de Defensa*

RICOH
imagine. change.