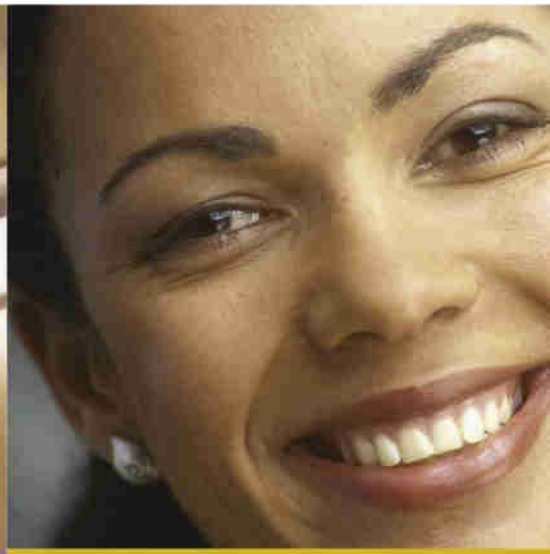
Soluciones de Seguridad Ricoh

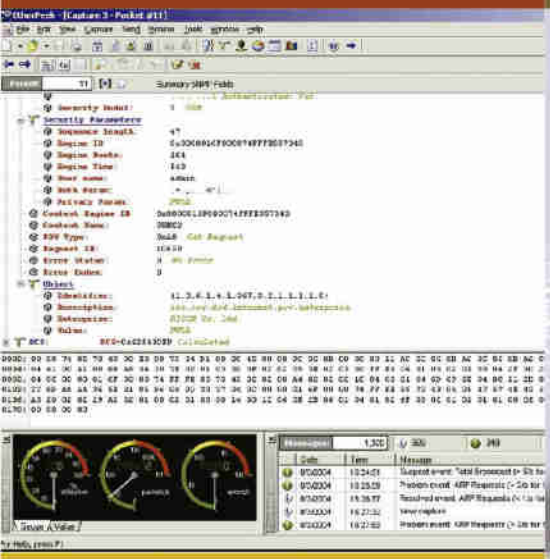
Soluciones completas y confiables para proteger información sensible

RICOH

Versión 9

controlar





monitorear

proteger

Soluciones de Seguridad Ricoh

No subestime los riesgos y los costos por el robo de información

La información es su activo más valioso. Por "la información" queremos decir clasificada, confidencial, u otro tipo de documentos sensibles, cualquier cosa que desde la confidencialidad se planee para revisión personal. La recopilación no autorizada de información confidencial, "espionaje económico", significan pérdidas entre $53 billones y $59 billones anualmente[1]. Si es generada dentro del gobierno, negocio o establecimiento privado, existe la urgente necesidad de contar con estrategias eficaces para proteger los activos de la información.

Mientras la tecnología digital ha transformado las prácticas de negocios permitiendo un intercambio cercano e instantáneo de datos, esto ha traído nuevos retos en términos de seguridad. Específicamente, quienes pretenden debilitar sus intereses pueden rápida y fácilmente interceptar información cuando se encuentra en forma digital. Este riesgo puede exponerlo a una disminución de su ventaja competitiva, posibles litigios o erosionar la confianza de los accionistas. A continuación se enumeran algunos sectores de alto riesgo:

Sectores de Alto Riesgo	Información en Riesgo
Gobierno	Seguridad Nacional, Militar y Secretos Comerciales
Financiero	Fusiones y Adquisiciones, Transacciones de Valores o Acciones
Farmacéutico	Pruebas Clínicas, Solicitudes de Patentes, Resultados Financieros
Oficinas en General	Listas de Clientes, Compensaciones Ejecutivas, Planes de Reestructuración
Alta Tecnología	Diseño de Nuevos Productos (R&D), Propiedad Intelectual
Laboratorios	Métodos de Prueba, Informes de Investigación
Bufetes de Abogados	Expedientes, Declaraciones, Contratos
Bufetes Contables	Reportes de Auditoría, Reportes Financieros
Hospitales/Médico	Facturación, Registros Médicos

Liderazgo en Seguridad de la Información

Ricoh, un proveedor líder en tecnología de alto desempeño para oficinas, incluyendo productos multifuncionales de color y blanco & negro, impresoras, sistemas de fax, escáneres, duplicadores y sistemas de formato amplio — está dedicado a ayudarle a enfrentar los retos de seguridad únicos y variados que van surgiendo. Al ofrecer opciones de seguridad personalizadas para nuestros clientes Ricoh ha desarrollado un conjunto completo de soluciones de seguridad. Estas soluciones de seguridad protegen los datos electrónicos e impresos de amenazas oportunistas y específicas, tanto internas como externas.

Evaluando sus vulnerabilidades, estableciendo objetivos de seguridad, y tomando las medidas adecuadas minimizará el riesgo potencial de fallas serias en la seguridad, y al mismo tiempo le permitirá cumplir con los requerimientos rigurosos de seguridad.

1 De acuerdo a un estudio publicado en el 2002 por la Sociedad Americana de Seguridad Industrial, U.S., Cámara de Comercio, y PricewaterhouseCoopers, de una encuesta realizada a las 1000 empresas de Fortune y 600 pequeñas y medianas empresas E.E.UU.

Esta guía detalla las Soluciones de Seguridad de Ricoh que fueron diseñadas para el mayor cumplimiento de sus objetivos al asegurar los sistemas digitales de oficina. Este enfoque multi-nivel cerrará de forma efectiva la puerta a quienes deseen explotar las vulnerabilidades. De hecho, si sus sistemas Ricoh están en red o no, éstas soluciones totalmente integradas, rentables lo protegerán de las violaciones de seguridad prevalecientes, sin interrupción del flujo normal (autorizado) de documentos.

Guía de Soluciones de Seguridad Ricoh

Nivel de Riesgo	**Bajo**			**Alto**
Nivel de Seguridad	**1**	**2**	**3**	**4**
Objetivo de Seguridad...	• Restringir Acceso No Autorizado al Dispositivo • Control de Salida del Dispositivo…	Además… • Asegurar Dispositivos de la Red • Asegurar la Impresión de Datos en la Red • Destrucción de Datos Latentes…	Además… • Asegurar Físicamente Datos/Puertos • Cifrar Comunicaciones en la Web • Autenticación de Usuarios…	Además… • Monitorear y Controlar Recursos • Auditar la Actividad de Todos los Dispositivos
Soluciones de Seguridad de Ricoh	• Códigos de Usuario • Bloqueo de Impresión • Seguridad de la Memoria RAM Además…	• Códigos de Usuario • Bloqueo de Impresión • Seguridad de la Memoria RAM • SmartDevice Monitor • Cifrado de Disco Rígido • Cifrado de Datos • DataOverwrite Security System • Web Image Monitor • Web SmartDevice Monitor	• Códigos de Usuario • Bloqueo de Impresión • Seguridad de la Memoria RAM • SmartDevice Monitor • Cifrado de Datos • DataOverwrite Security System • Disco Rígido Extraíble • Seguridad de los Puertos de Red • Cifrado de Disco Rígido • Cifrado de 128 bits en SSL/HTTPS • Autenticación NT • Web Image Monitor • Web SmartDevice Monitor	• Códigos de Usuario • Bloqueo de Impresión • Seguridad de la Memoria RAM • SmartDevice Monitor • Cifrado de Datos • DataOverwrite Security System • Disco Rígido Extraíble • Seguridad de los Puertos de Red • Cifrado de 128 bits en SSL/HTTPS • Autenticación NT • Control & Impresión de Copiado • Web Image Monitor • Web SmartDevice Monitor • Cifrado de Disco Rígido • IPv6 • Kerberos • Bloqueo de Impresión Mejorado • Print Director • Paquete de Autenticación de Tarjetas

Soluciones de Seguridad Ricoh

Restricción de Acceso No Autorizado a Dispositivos

Códigos de Usuario

Los Códigos de Usuario (estándar en casi todos los sistemas Ricoh) permiten a los administradores administrar y rastrear el uso de los dispositivos digitales de salida Ricoh. Un Código de Usuario puede ser asignado a un individuo basándose en la(s) función(es) a las que tiene autorización para acceder. Este nivel de control le permite monitorear el uso del sistema (p.e. generar reportes del contador de impresión por función y Código de Usuario).

Control de Salida del Dispositivo

Bloqueo de Impresión

El Bloqueo de Impresión (disponible a través de los drivers avanzados de impresión de Ricoh) mantiene la confidencialidad deteniendo la impresión del documento hasta que un usuario autorizado (autor/creador) ingrese el NIP correcto (Número de Identificación Personal) en el panel de control del dispositivo. Esto elimina la posibilidad de que alguien más vea o retire el documento de la bandeja de papel. (El Bloque de Impresión requiere un disco rígido que puede ser opcional, dependiendo del modelo.)

Cifrado de Contraseña de Bloqueo de Impresión

Como una nueva función la contraseña utilizada para bloquear la impresión puede cifrarse para su protección contra la intervención vía cable o teléfono.

Bloqueo de Impresión Mejorado

El Bloque de Impresión Mejorado le permite capturar todos los beneficios de los MFP´s compartidos y centralizados sin comprometer la seguridad de los documentos. Los usuarios almacenan, liberan y administran documentos confidenciales con la seguridad del ID de usuario y la autorización de la contraseña. Es una solución rápida y sencilla para la protección de los datos confidenciales y propietarios de su organización.

- Los usuarios pueden enviar documentos de manera segura a las impresoras donde se mantienen seguros hasta que el usuario autorizado los libere.
- Los documentos no pueden ser recogidos en la impresora por otro usuario, protegiendo la información confidencial.
- Los documentos almacenados en la impresora están cifrados (la información no puede ser comprometida si el disco rígido es robado).
- El Bloqueo de Impresión Mejorado es instalado en el dispositivo de impresión Multifuncional a través de firmware integrado (Tarjeta SD) o vía remota a través de una Interfaz Web.
- Los administradores y usuarios pueden configurar el Bloqueo de Impresión Mejorado a través de una interfaz para un navegador web.

Seguridad de la Memoria RAM

Seleccione un sistema MFP de Ricoh MFP que utilice memoria RAM (Random Access Memory) para el procesamiento de tareas de documentos como copiadora, no un disco rígido. Aunque el disco rígido está disponible como una opción, hay un beneficio de seguridad para la configuración base en los trabajos procesados aunque la memoria RAM sea volátil (p.e. cuando un sistema es apagado, los datos son inmediatamente eliminados). Sin un medio para almacenar los datos permanentemente, como un disco rígido, se elimina la amenaza a la seguridad. Como tales, estos sistemas MFP pueden ser propuestos para entornos de bajo volumen donde la seguridad de la información es de alta prioridad.

Seguridad de los Dispositivos de Red

SmartDeviceMonitor (para Admin*)

SmartDeviceMonitor es una utilidad de software que viene en paquete con todas las impresoras Ricoh, MFP´s habilitados para impresión y el Kit opcional de Impresora/Escáner. Este conjunto versátil de software simplifica los aspectos de la instalación, monitoreo y administración de los sistemas de salida de Ricoh que se encuentran en red, mientras soporta funciones clave de seguridad.

- **Cambio del Nombre General (Nombre de Grupo)**
  Para enfrentar la vulnerabilidad de SNMP (Simple Network Management Protocol), el administrador del sistema puede cambiar el Nombre General (Nombre de Grupo) de los dispositivos de hardware de "Publico" a un nombre más seguro. Si ésta medida de seguridad se toma, el Nombre General (para el software) debe ser idéntico al del dispositivo de salida Ricoh que esté conectado.

- **Acceso Restringido a Usuarios**
  Los administradores del sistema pueden controlar los privilegios del usuario a través de las Herramientas de Administración del Usuario. Este activa un menú para revisar los periféricos autorizados para el usuario por Código de Usuario y Nombre del Usuario. Todos los periféricos de Ricoh soportados en la red son listados, y un simple click en el dispositivo, da acceso al menú que restringe o habilita el dispositivo para usuarios de forma individual.

Web Image Monitor

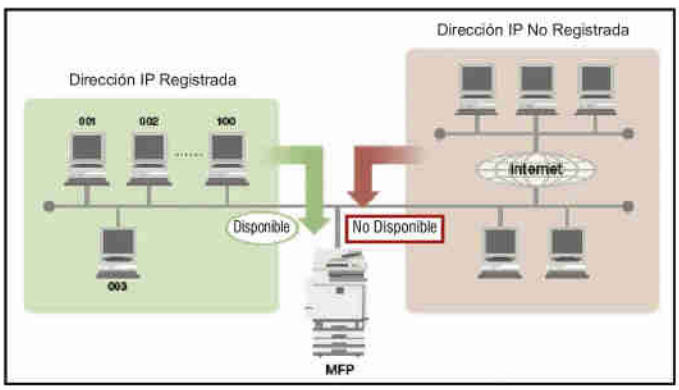
Web Image Monitor es una utilidad basada en web integrada para la administración de dispositivos.

- **Definir Rango de la Dirección IP (Filtros IP)**
  Los administradores del sistema pueden restringir las autorizaciones de las conexiones al controlador de impresión desde los hosts cuyas direcciones IP se encuentren en un determinado rango. Comandos o trabajos enviados por direcciones IP no-autorizadas son ignoradas por el controlador de impresión.
- **Seguridad del Puerto de Red**
  Los administradores del sistema pueden activar o desactivar los puertos IP, así controlar los diferentes servicios de la red que son provistos por el controlador de impresión a un usuario específico.

*Nota: SmartDeviceMonitor para Admin reside en la computadora "cliente" y permite a los usuarios determinar el estado y disponibilidad de los periféricos de Ricoh que están en red, un icono es colocado en la Barra de Tareas de Windows de la computadora del usuario, el cual muestra el estado del sistema en una vista general.

Filtros para Direcciones IP (Internet Protocol)

En una LAN (Red de Área Local), una Dirección IP es un número único de identificación del hardware de las computadoras conectadas a red. Justo como una dirección postal con un número de casa u apartamento, ésta dirección ayuda a dirigir correos electrónicos y archivos adjuntos, enviar faxes a los destinatarios adecuados, y enviar datos de de impresión a los dispositivos de salida conectados a una red desde las PC´s que los origina. La habilidad de los dispositivos de Ricoh de bloquear/restringir a un usuario en particular o configurar a usuario basándose en la dirección IP mejora la administración de las PC´s y de los usuarios, ayuda a balancear los volúmenes de salida entre múltiples dispositivos, y mejora la seguridad de la red limitando el acceso a archivos almacenados en los dispositivos.

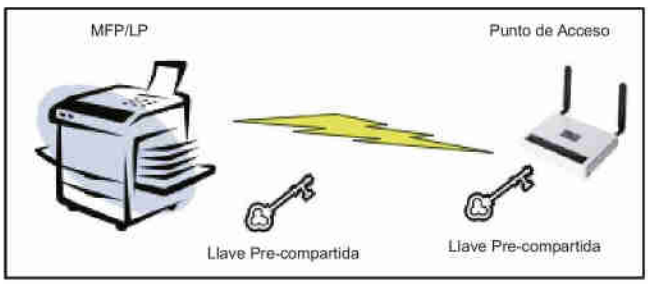


Registros de Trabajos/Registros de Acceso

Una lista complete de cada trabajo procesado por el dispositivo es almacenado en memoria. Esta lista puede ser visualizada via Web SmartDeviceMonitor para dar seguimiento y rastrear el uso del dispositivo por trabajo y/o usuario. Cuando se utiliza en conjunto con los modos de autenticación de un usuario externo, será posible determinara específicamente cual usuario pude estar haciendo mal uso o abusando del dispositivo. También es posible determinar cual dispositivo fue utilizado y por quién en el rastreo de una transmisión no autorizada.

Soporte WPA (Acceso Protegido Wi-Fi)

Utilizado en conjunto con la opción de red inalámbrica IEEE 802.11a/b/g, WPA es una especificación de seguridad que direcciona las vulnerabilidades en comunicaciones inalámbricas. Provee un alto nivel de seguridad a las empresas, pequeños negocios, y también a los usuarios que trabajan en casa de que sus datos permanezcan protegidos permitiendo solo a usuarios autorizados acceder a sus redes. Las funciones de autenticación y cifrado "Personal" y de "Empresa" bloquean a intrusos con computadoras portátiles con capacidades inalámbricas de hacer uso de las redes en cualquier entorno, previniendo la intercepción de cadenas de datos y contraseñas, o del uso de conexiones inalámbricas como un punto de entrada a la red de datos del usuario.



Autenticación de Cableado 802.1X

802.1X provee autenticación de red basada en el puerto para comunicaciones punto-a-punto entre los dispositivos de red y un puerto de una red de área local (LAN), la comunicación finalizara si la autenticación falla.

Cifrado de Datos

Como una misión crítica los datos atraviesan la red y es posible que hackers expertos intercepten cadenas puras de datos, archivos, y contraseñas. La llegada de la tecnología de redes inalámbricas, mientras incrementan la conveniencia de navegar e imprimir por millones, también deja a las redes vulnerables de ser atacadas por intrusos que están equipados con computadoras portátiles inalámbricas para acceder por cualquier punto dentro de un rango a la red. Sin protección, la información inteligible puede ser fácilmente robada, o modificada/falsificada y volver a colocarla dentro de la red. Los dispositivos de Ricoh están equipados con las siguientes funciones de cifrado para reducir estos riesgos.

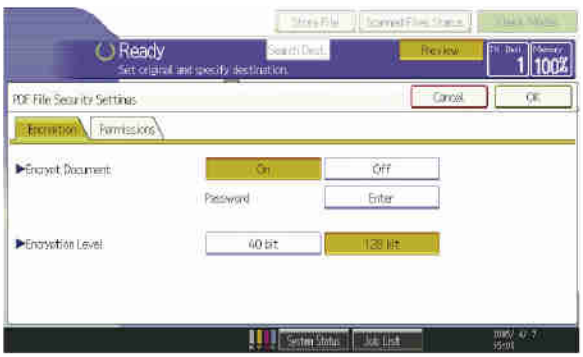
Soluciones de Seguridad Ricoh

Cifrado de la Libreta de Direcciones

El Cifrado de la Libreta de Direcciones protege la información del contacto por el cifrado de los datos almacenados en un sistema de libreta de direcciones. Aun si el HDD (disco rígido) es físicamente removido de la unidad, los datos no pueden ser leídos. Esta función elimina el peligro de que los empleados, clientes o proveedores de una compañía o departamento sean objeto de mensajes maliciosos de correo electrónico o de contaminación por virus en una PC. Además, como los datos de la libreta de direcciones corresponden usualmente a los nombres de usuarios y contraseñas utilizados en cualquier punto de la red, protegiendo los datos de las libretas de direcciones de impresoras/MFP´s incrementa la seguridad general de la red.

Transmisión Cifrada de PDF

El formato de archivos PDF de Adobe se ha convertido en el estándar universal en la creación de documentos que pueden ser fácilmente abiertos y compartidos por cualquier usuario en cualquier plataforma. Adobe provee la aplicación de Acrobat® Reader® como una descarga sin cargo desde la web. Un archivo PDF es esencialmente un documento instantáneo. Es inmutable (aunque los archivos sean editables con la aplicación complete de Adobe Acrobat) y por lo tanto atractiva para los propietarios de documentos que desean compartirlos, pero limitarlos para ser alterados, y aprobados. Parte de lo atractivo del formato PDF es el tamaño de los archivos que es drásticamente menor en comparación a los archivos generados en la aplicación nativa, haciendo que su transmisión via correo electrónica sea más fácil y rápida.



Mientras Adobe ofrece una serie de funciones relacionadas con la seguridad con la aplicación de Acrobat para bloquear y proteger los documentos con una contraseña, no hay nada para prevenir que el archivo sea interceptado en una forma descifrable mientras viaja a través de la red. Aquí es donde la función de la Transmisión Cifrada de PDF de Ricoh agrega valor, codificando y cifrando los datos que de otra manera pueden ser documentos transparentes durante su transmisión. Los usuarios pueden elegir entre un cifrado de 40 bits y de 128 bits, y configurar los derechos del destinatario para permitir cambios o extraer el contenido del documento. (Ver también Cifrado de Contraseña de PDF).

Cifrado del Disco Rígido (HDD)

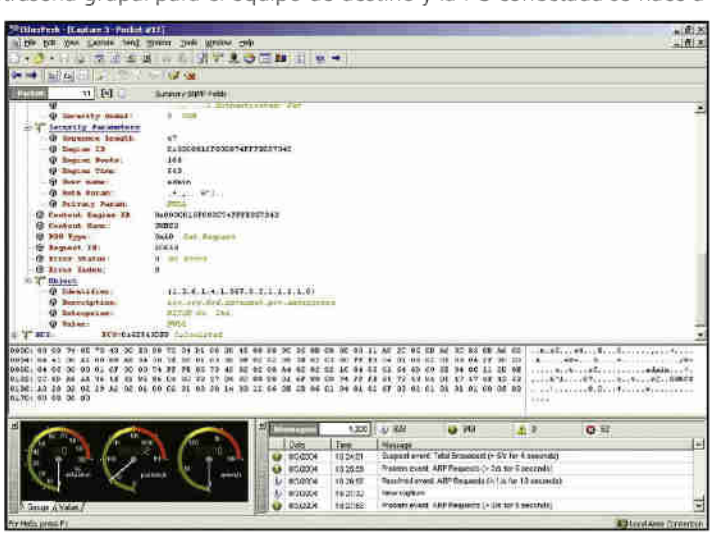
Esta función puede cifrar el sistema del disco rígido contra el robo de datos. Aun si el disco rígido es robado, los datos no podrán ser divulgados. La metodología de cifrado utilizada es Estándar Avanzado de Cifrado (Advanced Encryption Standard (AES)) a 256.

Llave de Cifrado para el Driver

Los dispositivos de Ricoh ofrecen una función que mezcla las contraseñas de autenticación de usuario utilizando los drivers PCL o RPCS de tal forma que otros no pueden acceder de manera fraudulenta al sistema utilizando una contraseña de usuario robada.

Cifrado de la Contraseña de PDF

Esta función corrige una vulnerabilidad en la Transmisión Cifrada de PDF en la que una ventana para el ingreso de la contraseña del usuario despliega dicha contraseña en texto claro. Esta función cifra las contraseñas hasta de 32 caracteres para más seguridad en la transmisión y almacenamiento de un PDF. La asignación de una contraseña grupal para el equipo de destino y la PC conectada se hace a través de DeskTopBinder Lite.



Comunicación Cifrada SNMP v3

Simple Network Management Protocol versión 3 (SNMP v3) es un estándar de administración de red ampliamente utilizado en entornos TCP/IP. SNMP provee un método para la administrar dispositivos en red tal como impresoras, escáneres, estaciones de trabajo o servidores, y grupos de puentes (bridges) y concentradores (hubs) juntos en una "comunidad" desde una computadora central que ejecuta un software para administración de red. Esto permite a los administradores, por ejemplo, realizar cambios a las configuraciones del dispositivo a través de SmartDeviceMonitor desde una PC conectada a red con comunicación cifrada para mantener el entorno seguro. Versiones anteriores (v1 y v2) de SNMP fueron utilizadas para configurar y monitorear dispositivos remotos. Las versiones recientes, de SNMP v3, ofrecen mejoras en la autenticación de usuarios y cifrado de datos que brindan mejores funciones de seguridad

para proteger los datos de los clientes y los activos de red. Al activar SNMP v3 impide que usuarios no autorizados vean las contraseñas y/o el contenido actual del archivo en una forma legible de texto, protegiendo así la información valiosa.

Kerberos

Kerberos es un protocolo de autenticación de red diseñado para proveer una solida autenticación para aplicaciones cliente/servidor por la implantación de criptografía secreta de llaves. Muchos protocolos de internet no ofrecen ninguna seguridad para sus contraseñas. Los hackers emplean programas llamados "sniffers" (succionadores) para extraer contraseñas y ganar el acceso a las redes. Enviando una contraseña que no está cifrada en una red es riesgoso y puede dejar a la red abierta para ser atacada. La autenticación Kerberos ayuda a limitar los riesgos causados por contraseñas no cifradas y mantener a las redes más seguras.

Comunicación IPsec

IPsec (IP security) es un conjunto de protocolos para asegurar las comunicaciones del Protocolo de Internet (IP) por la autenticación y/o cifrado de cada paquete IP en una cadena de datos. IPsec también incluye protocolos para el establecimiento de la llave criptográfica. Las organizaciones que requieren altos niveles de seguridad tienen redes con protección de datos IPsec. Estas organizaciones requieren impresión utilizando IPsec.

S/MIME para Escaneo a Correo Electrónico

S/MIME (Secure/Multipurpose Internet Mail Extensions) es un estándar para el cifrado público de llaves y para la salida de un correo electrónico encapsulado en MIME (Multipurpose Internet Mail Extensions). MIME es un Estándar de Internet que extiende el formato de correo electrónico para soportar texto en juegos de caracteres distintos a los US-ASCII, adjuntos sin-texto, cuerpos de mensajes en múltiples partes, e información de encabezados en juegos de caracteres diferentes a los ASCII.

Esta función es utilizada para cifrar datos confidenciales transmitidos por la función de Escaneo a Correo Electrónico para la protección de datos contra la intrusión a las líneas telefónicas.

Impresión Segura de Datos en la Red

Cifrado de Datos a través de IPP

Otra manera efectiva de lograr la seguridad de los datos es a través del cifrado. Utilizando SmartDeviceMonitor para Cliente de Ricoh, los datos a imprimir pueden ser cifrados a través de Secure Sockets Layer/Transport Layer Security (SSL/TLS) via Internet Printing Protocol (IPP), y por lo tanto asegurar los datos entre las estaciones de trabajo y las impresoras/MFP´s conectados a la red. (TLS es un protocolo que garantiza la integridad y privacidad de los datos entre la comunicación de aplicaciones cliente/servidor en Internet.). Esto significa que cualquier intento de intervenir los datos a imprimir fallará, i.e., los datos interceptados son indescifrables. Por favor vea las gráficas de especificaciones de producto incluidas para el soporte a cada modelo.

Destrucción de Datos Latentes

DataOverwriteSecurity System (DOSS) de Ricoh:

A fin de contrarrestar la perdida de datos, las medidas de seguridad de la información de una organización deben incorporar tecnología que destruya imágenes digitales latentes en un disco rígido de un MFP. DataOverwriteSecurity System de Ricoh cumple con ese objetivo al destruir datos almacenados temporalmente en el disco rígido de un MFP sobre-escribiendo la imagen latente con secuencias aleatorias de "1's" y "0's."

- El proceso de tres pasos para la sobre-escritura aleatoria de datos de Ricoh hace que cualquier intento de acceder y reconstruir archivos almacenados para impresión/copiado sea virtualmente imposible.
- Opera en conjunto con el Removable Hard Drive Security Systems (Sistemas de Seguridad del Disco Rígido Extraíble), proporcionando un enfoque multi-capas para el aseguramiento de documentos sensibles.
- Un simple icono del panel proporciona información visual referente al proceso de sobre-escritura, e.g., terminada o en proceso.
- Cumple con los métodos recomendados para la administración de información clasificada por la Agencia Nacional de Seguridad (NSA).
- **Presta asistencia en el cumplimiento de los requerimientos de HIPAA, GLBA y FERPA.**
- DOSS Tipo A, B, C, D, F, H e I son ISO 15408 Certificados para un EAL de 3.

Seguridad en el Cumplimiento de Requisitos Legales

Mediante el empleo de DataOverwriteSecurity de Ricoh o de los Sistemas Extraíbles de Disco Rígido (RHD), las empresas que participan en la recolección y difusión de registros médicos, e.g., hospitales, organizaciones de salud, y recursos humanos protegen la privacidad del paciente. Específicamente los datos relativos a la condición médica de un individuo no pueden ser sustraídos o robados, ayudando así al cumplimiento de los requisitos necesarios de la **HIPAA (Health Insurance Portability and Accountability Act- Ley de Portabilidad y Responsabilidad en los Seguros de Salud)** que es una ley diseñada para proteger a los trabajadores Americanos y sus familias de la discriminación basada en condiciones médicas pre-existentes. Además las opciones de DOSS y RHD de Ricoh también ayudan al cumplimiento de la privacidad financiera **(Ley Gramm-Leach-Bliley)** y la privacidad de estudiantes **(Ley para los Derechos de la Privacidad de la Educación Familiar)**.

Soluciones de Seguridad Ricoh

Seguridad Física de Datos/Puertos

Sistemas de Seguridad de Disco Rígido Extraíble (RHD)

Conveniente y fácil de utilizar, la interfaz de los Sistemas de Disco Rígido Extraíble de Ricoh con un sistema estándar digital de disco rígido. Esta solución asegura el sistema interno del disco rígido dentro de un depósito solido utilizando un sistema de bloqueo de llaves. Un sistema de etiquetado numérico asegura que el Disco Rígido Extraíble se fácil de identificar durante el almacenamiento o cuando sea reemplazado en el sistema. También se proporciona una cubierta libre de estática para proteger al Disco Rígido Extraíble durante el tránsito o almacenamiento.

Para proveer aun mayor seguridad y flexibilidad cuando se trata de documentos clasificados y no clasificados, un Disco Rígido Extraíble adicional opcional está disponible. Esto permite a los sistemas digitales de Ricoh manejar dos Discos Rígidos Extraíbles separados e intercambiables, uno para documentos clasificados y el otro para documentos no clasificados. Después de que los documentos clasificados han sido copiados o impresos, la unidad para documentos clasificados puede ser extraída y colocada en un lugar seguro y la unidad para documentos no clasificados puede ser instalada nuevamente para el copiado o impresión de documentos no clasificados.

- El Disco Rígido Extraíble es colocado en un área estratégicamente accesible para el retiro y almacenamiento sencillo y autorizado.
- Maximiza la seguridad permitiendo la separación física de los datos del dispositivo de entrada/salida, impidiendo el acceso a datos remanentes.
- El Disco Duro Extraíble de los sistemas Ricoh opera de forma transparente con las funciones robustas de copiado, impresión y escaneo.
- Opera conjuntamente con el Sistema DataOverwriteSecurity de Ricoh, proporcionando un enfoque multi-capas para el aseguramiento de documentos sensible.
- Todas las funciones están disponibles (copiado, impresión, escaneo, envío de fax y el Servidor de Documentos*) cuando el Disco Rígido Extraíble es instalado.

***Servidor de Documentos**, una capacidad al seleccionar los sistemas de salida de Ricoh para almacenar trabajos, (escanear, imprimir, enviar faxes, o copiar) en el sistema de disco rígido, también soporta Secure Document Release.

Seguridad en los Puertos de Red

Típicamente, los sistemas habilitados para red son entregados al cliente con todos los puertos "abiertos", permitiendo que la integración de estos sistemas a redes diferentes sea tan sencilla como sea posible. Sin embargo, permitir que estos sistemas habilitados para red sean fáciles de instalar, los puertos de red abiertos y sin utilizar tienen un riesgo de seguridad.
Para proveer seguridad de red mejorada, los Administradores pueden deshabilitar un protocolo específico como el SNMP o FTP utilizando Web Image Monitor o SmartDeviceMonitor. Esto impide el robo de los nombres de usuarios y contraseñas, así como la eliminación de amenazas externas incluyendo la destrucción/falsificación de datos almacenados, Denial of Service (DoS) ataca y los virus entran a la red a través de un puerto sin utilizar de una impresora o MFP.

Comunicación Cifrada de Datos

Cifrado de 128-bits sobre SSL

GlobalScan y DocumentMall, ambos soportan cifrado de 128-bits sobre SSL (Secure Sockets Layer). La tecnología SSL trabajo utilizando una llave privada para cifrar los datos que son escaneados en MFP de Ricoh hacia GlobalScan o el Servidor DocumentMall, creando una conexión segura. Cualquier URL (Uniform Resource Locator) que requiera una conexión SSL, como GlobalScan y Document Mall, empezara con https:, con una "s" posicionada para "secure" (seguro).

Autenticar Usuarios

Impide el Uso No Autorizado del Sistema:

La Autenticación es una función de seguridad en el MFP que restringe a usuarios no autorizados, o a un grupo de usuarios, el acceso a las funciones del sistema o al cambio de la configuración del equipo. Esta importante capacidad permite a los administradores del sistema emplear "Administración del Acceso Limitado," ayudando a proteger así su MFP ya instalado de un uso o manipulación no autorizada.

GlobalScan es una solución basada en web para la Administración de Documentos y su Contenido que permite al seleccionar los sistemas de Ricoh realizar funciones de escaneo en red, específicamente, escaneo a correo electrónico o carpeta, así como realizar OCR, envío de fax y funciones de administración de documentos a través de sistemas opcionales "plug-in" (de conexión). Esta poderosa, pero fácil de utilizar, captura de documentos en papel y sistema de distribución se integra perfectamente con su actual infraestructura de correo que impulsa significativamente la productividad de los grupos de trabajo, combinando la funcionalidad de escaneo con una plataforma accesible de copiado. **Las funciones mejoradas de seguridad de GlobalScan's incluyen:** Seguridad LDAP, Seguridad SMTP, Autenticación Kerberos y Contraseña de Protección para

DocumentMall, es una aplicación de host de bajo costo y bajo riesgo que provee seguridad para el acceso a Internet para sus documentos desde cualquier parte del mundo, 24 horas al día, 7 días a la semana, permitiendo compartir fácilmente así como la colaboración a través de fronteras geográficas.

- **La Autenticación de Usuario** le permite restringir el acceso al equipo de tal forma que solo aquellos con un nombre de usuario y contraseña validos pueden acceder a las funciones del MFP.
- **La Autenticación de Windows** verifica la identidad del usuario del MFP comparando las credenciales de entrada (nombre de usuario/contraseña) contra la base de datos de usuarios autorizados en el Servidor de Red de Windows, por lo tanto conceder o negar el acceso a las funciones del MFP.
- **La Autenticación LDAP** valida a un usuario contra el Servidor LDAP (Light-weight Directory Access Protocol), de tal forma que solo aquellos con un nombre de usuario/contraseña validos pueden acceder a la libreta global de direcciones, i.e., buscar y seleccionar direcciones de correo electrónico almacenadas en el Servidor LDAP.
- **Autenticación del Administrador** – Un administrador registrado administra las configuraciones del sistema y el acceso de usuarios a las funciones del MFP. Hasta cuatro Administradores pueden compartir las tareas administrativas, permitiendo repartir la carga de trabajo y limitar la operación no autorizada a un solo administrador, aunque la misma persona puede asumir todos los roles. Además, un Supervisor separado puede establecerse para configurar y cambiar las contraseñas de los administradores.
- **Autenticación Básica** – Autentifica a un usuario utilizando el nombre del usuario/contraseña registrados localmente en la Libreta de Direcciones del MFP. Nadie sin un nombre de usuario/contraseña validos puede acceder al equipo.
- **Autenticación del Código de Usuario** – Utiliza el sistema estándar de Ricoh de Código de Usuario, el cual es comparado para registrar datos en la libreta de direcciones del MFP. Nadie sin un Código de Usuario valido puede acceder al equipo.
  La Autenticación Básica y la Autenticación de Código de Usuario pueden ser utilizadas en entornos de oficina que no sean Windows y/o que no estén en red.
- **Autenticación (Tarjeta Común de Acceso) US Department of Defense Common Access Card (CAC)** – La Tarjeta Común de Acceso (CAC) es una solución de US DoD especializada en la autenticación de sistemas basados en tarjetas, diseñada para cumplir con el Homeland Security Presidential Directive -12 (HSPD-12). Esta Directiva requiere que todos los empleados federales y contratistas mejoren la eficiencia en la seguridad reduciendo el fraude de identidad a través del incremento en la protección de la privacidad personal. El único cliente de Ricoh para la Solución de Autenticación CAC es el Departamento de Defensa de los Estados Unidos (DoD) [Ejército, Fuerza Aérea, Marines, Guardia Costera y organismos afiliados de los Estados Unidos].

Monitoreo y Control de Recursos

Print Director

Print Director es una solución completa para la administración de impresión, la cual permite analizar, comprender y en última instancia ahorrar costos asociados con la impresión y el fotocopiado. Esta solución puede ser instalada para que de manera discreta se de seguimiento a las actividades de impresión, limita el número de impresiones y copias que un usuario puede procesar, así como asegura el cumplimiento de las "reglas base" de las metodologías de impresión, para reducir el Costo Total de Propiedad.

Print Director identifica y controla los costos asociados a la impresión en toda la empresa.

Audita la Actividad de Todos los Dispositivos

Print and Copy Control v3 de Ricoh para Equitrac Office and Express

Print and Copy Control de Ricoh le permite a los clientes tener un mejor control del acceso de usuarios y rastrear información de copiado/impresión a través del software integrado en las unidades de disco rígido de los sistemas de salida seleccionados de Ricoh. Estas ventajas incluyen:

Opciones de Autenticación Segura

Protege datos sensibles e impide el uso no autorizado mediante un método de autenticación que se adapta a su negocio.

- Definitivamente simplicidad y seguridad. Los empleados acceden al MFP utilizando sus tarjetas de identificación (ID) de la empresa y lectores de tarjetas opcionales que se instalan en minutos. PCC de Ricoh acepta MIFARE®, Legic®, HID® Prox (125 KHz) y tarjetas con bandas magnéticas.
- Cómodo acceso personalizado. Fácil seguimiento a la salida del documento utilizando un NIP (Número de Identificación Personal) — por usuario, proyecto o inclusive por grupo de trabajo.
- Amplio acceso instantáneo para toda la empresa. Los usuarios simplemente ingresan sus ID de red y contraseña para "desbloquear" el MFP.

Soluciones de Seguridad Ricoh

Uso Amigable y Seguro

- Conveniente, impresión segura. La producción de documentos Follow-You™ le permite dar salida a sus documentos desde cualquier MFP de la red, de tal forma que puede evitar los equipos que están ocupados o no disponibles, o enviar múltiples documentos e imprimirlos como requiera en diferentes departamentos, oficinas o edificios.
- Control temporizado. Los administradores pueden programar la eliminación de trabajos del servidor después de un límite de tiempo establecido.
- Seguridad reforzada. Los trabajos residen en un servidor seguro — no en los sistemas de disco rígido. Además, menos documentos se quedan sin atención en las bandejas de salida ya que se retienen hasta que son liberados por el usuario.

Control del Copiado No Autorizado

El driver de impresión innovador de Ricoh RPCS soporta una función única que ningún otro fabricante ofrece, el Control del Copiado No Autorizado. Lo que hace ésta función es integrar patrones y texto debajo del texto impreso, eliminando el riesgo del copiado no autorizado de documentos sensible.
Esta nueva función es ideal para pequeñas empresas que principalmente utilizan el sistema para enviar faxes, copiar o imprimir, por ejemplo, empresas que generan reportes de personal, planes de compensación, registros médicos, reportes financieros, etc.

El Control de Copiado No Autorizado consiste en dos funciones:
1. Tipo de Máscara para Copiado[2] es una función estándar del RPCS que integra un patrón de enmascaramiento y mensaje en la impresión original de salida. Si las copias son hechas, ya sea en un equipo Ricoh o en un sistema digital de la competencia, el mensaje integrado aparece; el nombre del autor, por ejemplo, ayuda a identificar al que lo originó.


Driver de Impresión RPCS de Ricoh

2. Al seleccionar Copy Data Security for Copying[1] (Seguridad de Datos para Copiado[1]) en el driver RPCS, todas las copias de salida que son generadas en un MFP equipado con la Unidad de Seguridad de Datos Copiados (Copy Data Security Unit) serán en un tono gris, dejando solo 0.16" (4mm) de margen para el patrón de enmascaramiento.

Notas:
1 Requiere Unidad Opcional de Copy Data Security. No es soportada en algunas configuraciones con la función de Fax. La función de Escáner debe ser desactivada en algunas configuraciones con el Escaneo activo. El rango de reducción en el copiado menor al 50% será desactivado.
2 Algunos MFP´s digitales pueden no detector patrones de enmascaramiento.

Oficinas en General Funciones de Seguridad para el Facsímil Comercial

Fax Comercial Standalone

Acceso Restringido
Acceso Restringido le permite rastrear de forma cercana el uso del equipo y disuadir a personas que pasan de forma eventual de utilizar el equipo. Los usuarios autorizados deben ingresar un código antes de que puedan utilizar el equipo. Además, ésta función puede estar ligada a la función del Temporizador Nocturno de tal forma que el Acceso Restringido es encendido/apagado a ciertas horas, impidiendo el acceso después de esos horarios.

Autenticación del Dominio del Servidor
Cuando el rastreo de la seguridad y usuario son un punto importante para los Administradores TI, la Autenticación del Dominio del Servidor es estándar en FAX4420NF y FAX5510NF. La autenticación limita el acceso a los sistemas de fax incrementando la seguridad por el monitoreo del uso del equipo. El acceso al equipo está dado solo a usuarios con una cuenta de controlador del dominio Windows. La Autenticación del Servidor limitará el acceso al sistema de fax no solo para el escaneo a correo electrónico, sino también para el envío estándar de fax, fax IP y fax LAN.

Seguridad en la Protección del Código NIP (Número de Identificación Personal)
Para evitar que un Código NIP o un ID Personal sean expuestos, cualquier caracter después de cierta posición el número de marcación del destinatario se ocultará, tanto en la pantalla como el Reporte de Comunicaciones.

Red Cerrada
Con Redes Cerradas, los códigos ID de los equipos de comunicación son verificados. Si no son idénticos, la comunicación finaliza, esto evita que documentos confidenciales sean transmitidos de forma intencional o accidental a la(s) ubicación(es) incorrecta(s), i.e., fuera de la red. (Nota: Redes Cerradas requiere que todos los sistemas de fax sean sistemas de Ricoh con la función de redes cerradas.)

Transmisión/Recepción Confidencial
Esta función permite al usuario transmitir/recibir hacia un buzón de correo que está protegido con un código de entrada. Los mensajes solo son impresos después de que el destinatario ingresa el código apropiado, proporcionando un nivel de seguridad mejorado cuando se realizan comunicaciones entre equipos.

Bloqueo de Memoria
Cuando el Bloqueo de Memoria es activado, los documentos de todos los remitentes (o remitentes específicos) son retenidos en la memoria. Cuando el ID del Bloqueo de Memoria es ingresado en el panel de control, los documentos se imprimen, otra forma de seguridad que impide que los documentos permanezcan en una bandeja expuestos a ser leídos por personas que pasan de forma eventual.

Fax Comercial de Red

Subdirección de Enrutamiento ITU-T
Utilizando una sub-dirección, anexa a un número de fax, hace posible enrutar directamente el fax a las computadoras destinatarias, a través de su dirección de correo electrónico. Cuando se ha recibido en una PC (computadora), la confidencialidad se mantiene, i.e., solo el destinatario puede ver el mensaje.

Fax IP
Los Sistemas de Fax de Ricoh, con la Unidad NIC FAX instalada, soportan seguridad T.38 en tiempo real en Fax IP a través de una Intranet corporativa, no solo evitando las costosas líneas telefónicas, sino también la operación segura detrás del firewall.

Gráfica de Compatibilidad de las Soluciones de Seguridad de Ricoh

	Funciones de Seguridad del Facsímil Comercial							
	Red Cerrada	Transmisión/Recepción Confidencial	Fax IP	Sub-dirección de Enrutamiento ITU-IT	Bloqueo de Memoria	Acceso Restringido	Seguridad en la Protección del Código NIP	Autenticación del Servidor de Dominio
Facsímil Súper G3								
FAX1180L		■				■		
FAX2210L		■						
FAX3320L	■	■			■	■	■	
FAX4430L	■	■			■	■	■	
FAX4430NF	■	■	■	■	■	■	■	■
FAX5510L	■	■			■	■		
FAX5510NF	■	■	■	■	■	■		■

Soluciones de Seguridad Ricoh

Tablas de compatibilidad de Soluciones de Seguridad Ricoh

	Protección de Red			Acceso a Dispositivo										Cifrado de Datos										Protección del Documento						
	Web Image Monitor	SmartDeviceMonitor	Protocolos de Red ENCENDIDO/APAGADO	Autenticación del Administrador	Registro de Trabajo/Registro de Acceso	Filtro de Dirección IP	Registro de Cuenta del Usuario	Autenticación del Usuario	Protección de Acceso Wi-Fi (WPA)	Kerberos	Autenticación de Cableado 802.1X	Autenticación de Tarjeta de Acceso (U.S. DoD Common Access Card (CAC))	Cifrado de 128-bit Secure Socket Layer (SSL)	Cifrado de la Libreta de Direcciones	Transmisión Cifrado de PDF	Llave de Cifrado del Driver	Cifrado de Contraseña del PDF	Cifrado SNMP v3	S/MIME para Escaneo a Correo Electrónico	Comunicación Ipsec	Cifrado de HDD	Cifrado de Contraseña de Bloqueo de Impresión	DataOverwriteSecurity System (DOSS)	Bloqueo/Impresión Segura/Bloqueo de Impresión Mejorado	Protección de Contraseña de Documentos Almacenados	Seguridad de memoria RAM* (Si el Disco Rígido es Opcional)	Disco Rígido Extraíble	Control de Copiado No Autorizado	Tipo Mascara para Copiado	Opción de Seguridad de Copiado de Datos (Copy Data Security)
Multifunción a Color																														
AficioGX3000S	■	■				■																				■		■		
AficioGX3000SF	■	■	■			■																				■		■		
AficioGX3050SFN	■	■	■			■																				■				
AficioSPC220S	■	■	■																							■				
AficioSPC231SF/ C232SF	■	■	■																					■		■				
Aficio615C	■	■	■	■	■	■	■	■	■				■	■	■	■	■	■						■	■	■		■		
AficioMPC2030	■	■	■	■	■	■	■	■		■	■		■	■		■		■		■						■	■	■	■	■
AficioMPC2050/SPF	■	■	■	■	■	■	■	■	■	■	■		■	■	■	■	■	■	■	■	■	■	■	■	■	■			■	■
AficioMPC2550/SPF	■	■	■	■	■	■	■	■	■	■	■		■	■	■	■	■	■	■	■	■	■	■	■	■	■			■	■
AficioMPC2000/SPF	■	■	■	■	■	■**	■	■	■			■	■	■	■	■	■	■						■	■	■		■	■	
AficioMPC2500/SPF	■	■	■	■	■	■**	■	■	■			■	■	■	■	■	■	■						■	■	■		■	■	
AficioMPC3000/SPF	■	■	■	■	■	■**	■	■	■			■	■	■	■	■	■	■						■	■	■		■	■	
AficioMPC2800/SPF	■	■	■	■	■	■	■	■	■	■	■		■	■	■	■	■	■	■	■	■	■	■	■	■	■			■	■
AficioMPC3300/SPF	■	■	■	■	■	■	■	■	■	■	■		■	■	■	■	■	■	■	■	■	■	■	■	■	■			■	■
AficioMPC3500/SPF	■	■	■	■	■	■**	■	■	■			■	■	■	■	■	■	■						■	■	■				
AficioMPC4500/SPF	■	■	■	■	■	■**	■	■	■			■	■	■	■	■	■	■						■	■	■		■		
AficioMPC2500EFI			■	■	■	■**	■	■				■	■	■				■						■***	■	■		■		
AficioMPC3000EFI			■	■	■	■**	■	■				■	■	■				■						■***	■	■		■		
AficioMPC3500EFI			■	■	■	■**	■	■				■	■	■				■						■***	■	■		■		
AficioMPC4500EFI			■	■	■	■**	■	■				■	■	■				■						■***	■	■		■		
AficioMPC4000/SPF	■	■	■	■	■	■	■	■	■	■	■		■	■	■	■	■	■	■	■	■	■	■	■	■	■			■	■
AficioMPC5000/SPF	■	■	■	■	■	■	■	■	■	■	■		■	■	■	■	■	■	■	■	■	■	■	■	■	■			■	■
Aficio3260C*	■	■	■		■	■	■	■					■	■	■	■	■	■						■	■	■				
AficioColor5560*	■	■	■	■	■	■	■	■					■	■	■		■	■						■	■	■				
AficioMPC6000	■	■	■	■		■	■	■		■		■	■	■	■		■	■	■	■	■	■	■	■	■	■			■	■
AficioMPC7500	■	■	■	■		■	■	■		■		■	■	■	■		■	■	■	■	■	■	■	■	■	■			■	■
ProC550EX/ C700EX****	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■		■	■	■
ProC900s	■	■	■	■	■	■	■	■					■	■	■		■		■	■				■						

* *Con el 3260C/AC5560, estas funciones de seguridad solo están disponibles cuando son configurados con el control de Arquitectura de la Siguiente Generación.*

** *Con estos productos, solo el Filtro de la Dirección IP está disponible. El filtro para Mac no está disponible en éstos productos.*

*** *Con las versiones de EFI, la función del Sistema DataOverwriteSecurity se conoce como Borrado Seguro*

**** *Nota: La Pro C550EX/Pro C700EX y los controladores Fiery tienen funciones de seguridad separadas. Las funciones de seguridad descritas arriba son para el controlador GW del sistema principal (mainframe) solamente. Si el sistema principal está configurado con un Fiery, las funciones de seguridad del Fiery tienen prioridad.*

SeguridadControlMonitoreoProtección

	Protección de Red			Acceso a Dispositivo									Cifrado de Datos										Protección del Documento						
	Web Image Monitor	SmartDeviceMonitor	Protocolos de Red ENCENDIDO/APAGADO	Autenticación del Administrador	Registro de Trabajo/Registro de Acceso	Filtro de Dirección IP	Registro de Cuenta del Usuario	Autenticación del Usuario	Protección de Acceso Wi-Fi (WPA)	Kerberos	Autenticación de Cableado 802.1X	Autenticación de Tarjeta de Acceso (U.S. DoD Common Access Card (CAC))	Cifrado de 128-bit Secure Socket Layer (SSL)	Cifrado de la Libreta de Direcciones	Transmisión Cifrado de PDF	Llave de Cifrado del Driver	Cifrado de Contraseña del PDF	Cifrado SNMP v3	S/MIME para Escaneo a Correo Electrónico	Comunicación Ipsec	Cifrado de HDD	Cifrado de Contraseña de Bloqueo de Impresión	DataOverwriteSecurity System (DOSS)	Bloqueo/Impresión Segura/Bloqueo de Impresión Mejorado	Protección de Contraseña de Documentos Almacenados	Seguridad de memoria RAM* (Si el Disco Rígido es Opcional)	Disco Rígido Extraíble	Control de Copiado No Autorizado	Tipo Máscara para Copiado	Opción de Seguridad de Copiado de Datos (Copy Data Security)
Multifunción Blanco & Negro																														
AC104		■			■																					■				
AC204		■			■																					■				
AC205L		■	■		■																					■				
AficioSP1000SF	■	■	■																							■				
AficioSP3200SF		■	■		■																					■				
AficioSP4100SFL/ SP4100SF/SP4110SF	■	■	■	■	■	■	■	■	■				■					■				■	■	■	■	■		■	■	■
Aficio1515/1515F/ 1515MF		■	■		■																					■				
AficioMP161/F/ SPF	■	■	■[1]	■[1]		■[1]		■[1]	■[3]				■[1]	■[1]	■[1]	■[1]	■[1]	■[1]								■			■	
AficioMP171/F/ SPF	■	■	■[1]	■[1]	■[1]	■[1]	■[1]	■[1]	■[3]	■[1]	■[1]		■[1]	■[1]	■[1]	■[1]	■[1]	■[1]	■[1]	■[1]	■[1]	■[1]		■[1]	■[1]	■[1]	■				
Aficio2015		■	■		■																					■				
Aficio2016		■	■		■																					■				
AficioMP1600/SPF	■	■	■[1]	■[1]		■[1]		■[1]	■[3]				■	■[4]	■[1]	■[1]	■[1]	■[1]										■		
Aficio2018/2018D		■	■		■																					■				
Aficio2020/2020D		■	■		■																					■				
AficioMP2000/SPF	■	■	■[1]	■[1]		■[1]		■[1]	■[3]				■	■[4]	■[1]	■[1]	■[1]	■[1]								■			■	
AficioMP2500	■[1]	■[1]	■	■[1]		■[1]	■	■[1]	■[3]				■[1]	■[4]	■[1]	■[1]	■[1]	■[1]								■		■	■	
AficioMP2500SPF2	■	■	■	■		■	■	■	■[2]				■	■	■	■	■	■								■		■	■	
AficioMP2510/P/ SP/SPF/SPI	■	■	■	■	■	■	■		■			■	■	■		■		■					■	■	■	■				
AficioMP3010/P/ SP/SPF/SPI	■	■	■	■	■	■	■		■			■	■	■		■		■					■	■	■	■		■		
Aficio3025/P/SP/ SPF/SPi	■	■	■	■	■	■	■	■					■	■	■	■	■	■					■	■	■	■		■		
Aficio3030/P/SP/ SPF/SPi	■	■	■	■	■	■	■	■					■	■	■	■	■	■					■	■	■	■		■		
AficioMP2550B/ MP2550/SPF	■	■	■	■	■	■	■	■	■	■		■	■	■		■	■	■	■	■	■	■	■	■	■	■			■	■
AficioMP3350B/ 3350/SPF	■	■	■	■	■	■	■	■	■	■		■	■	■		■	■	■	■	■	■	■	■	■	■	■			■	■

[1] Kit de Impresora/Escáner es requerido. *[2]Se requiere IEEE 802.11b* *[3]Kit de Impresora/Escáner e IEEE 802.11b son requeridos.*
[4] Kit de Impresora/Escáner o Kit de Fax es requerido.

Soluciones de Seguridad Ricoh

	Protección de Red			Acceso a Dispositivo									Cifrado de Datos										Protección del Documento							
	Web Image Monitor	SmartDeviceMonitor	Protocolos de Red ENCENDIDO/APAGADO	Autenticación del Administrador	Registro de Trabajo/Registro de Acceso	Filtro de Dirección IP	Registro de Cuenta del Usuario	Autenticación del Usuario	Protección de Acceso Wi-Fi (WPA)	Kerberos	Autenticación de Cableado 802.1X	Autenticación de Tarjeta de Acceso (U.S. DoD Common Access Card (CAC))	Cifrado de 128-bit Secure Sockket Layer (SSL)	Cifrado de la Libreta de Direcciones	Transmisión Cifrado de PDF	Llave de Cifrado del Driver	Cifrado de Contraseña del PDF	Cifrado SNMP v3	S/MIME para Escaneo a Correo Electrónico	Comunicación Ipsec	Cifrado del HDD	Cifrado de Contraseña de Bloqueo de Impresión	DataOverwriteSecurity System (DOSS)	Bloqueo/Impresión Segura/Bloqueo de Impresión Mejorado	Protección de Contraseña de Documentos Almacenados	Seguridad de memoria RAM* (Si el Disco Rígido es Opcional)	Disco Rígido Extraíble	Control de Copiado No Autorizado	Tipo Mascara para Copiado	Opción de Seguridad de Copiado de Datos (Copy Data Security)
Multifunción Blanco & Negro (continuación)																														
AficioMP3500/P/SP/SPF/SPI/G	■	■	■	■	■	■	■	■	■			■	■	■	■	■	■	■					■	■	■		■	■	■	■
AficioMP4000B/4000/SPF	■	■	■	■	■	■	■	■	■	■		■	■	■	■	■	■	■	■	■	■	■	■	■	■	■		■	■	■
AficioMP4500/P/SP/SPF/SPI/G	■	■	■	■	■	■	■	■	■			■	■	■	■	■	■	■					■	■	■		■	■	■	■
AficioMP5000B/5000/SPF	■	■	■	■	■	■	■	■	■	■		■	■	■	■	■	■	■	■	■	■	■	■	■	■	■		■	■	■
Aficio5500/SP	■	■	■	■	■	■	■	■				■	■	■	■	■	■	■					■	■	■		■			
Aficio6500/SP	■	■	■	■	■	■	■	■				■	■	■	■	■	■	■					■	■	■		■			
Aficio7500/SP	■	■	■	■	■	■	■	■				■	■	■	■	■	■	■					■	■	■		■			
AficioMP6000	■	■	■	■	■	■	■	■	■			■	■	■	■	■	■	■					■	■	■		■	■	■	■
AficioMP7000	■	■	■	■	■	■	■	■	■			■	■	■	■	■	■	■					■	■	■		■	■	■	■
AficioMP8000	■	■	■	■	■	■	■	■	■			■	■	■	■	■	■	■					■	■	■		■	■	■	■
AficioMP6001/7001/8001/9001	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■			■	■	■
Aficio2090	■	■	■		■	■															■	■	■		■					
Aficio2105	■	■	■		■	■															■	■	■		■					
AficioPro906EX	■	■	■	■	■	■	■	■	■				■	■	■	■	■	■				■	■	■	■		■	■	■	■
AficioPro1106EX	■	■	■	■	■	■	■	■	■				■	■	■	■	■	■				■	■	■	■		■	■	■	■
AficioPro1356EX	■	■	■	■	■	■	■	■	■				■	■	■	■	■	■				■	■	■	■		■	■	■	■

	Protección de Red			Acceso a Dispositivo										Cifrado de Datos										Protección del Documento								
	Web Image Monitor	SmartDeviceMonitor	Protocolos de Red ENCENDIDO/APAGADO	Autenticación del Administrador	Registro de Trabajo/Registro de Acceso	Filtro de Dirección IP	Registro de Cuenta del Usuario	Autenticación del Usuario	Protección de Acceso Wi-Fi (WPA)	Kerberos	Autenticación de Cableado 802.1X	Autenticación de Tarjeta de Acceso (U.S. DoD Common Access Card (CAC))	Cifrado de 128-bit Secure Socket Layer (SSL)	Cifrado de la Libreta de Direcciones	Transmisión Cifrado de PDF	Llave de Cifrado del Driver	Cifrado de Contraseña del PDF	Cifrado SNMP v3	S/MIME para Escaneo a Correo Electrónico	Comunicación Ipsec	Cifrado de HDD	Cifrado de Contraseña de Bloqueo de Impresión	DataOverwriteSecurity System (DOSS)	Bloqueo/Impresión Segura/Bloqueo de Impresión Mejorado	Protección de Contraseña de Documentos Almacenados	Seguridad de memoria RAM* (Si el Disco Rígido es Opcional)	Disco Rígido Extraíble	Control de Copiado No Autorizado	Tipo Mascara para Copiado	Opción de Seguridad de Copiado de Datos (Copy Data Security)
Impresoras a Color																																
AficioSPC311N/ C312DN	■	■	■																							■						
AficioSPC220N/ C221N/C222DN	■	■	■																							■						
AficioSPC231N/ C232DN	■	■	■																							■						
AficioSPC420DN	■	■	■	■	■	■	■	■	■				■		■		■	■			■		■	■	■	■		■	■	■		
AficioSPC420DN-KP HotSpot	■	■	■	■	■	■	■	■	■				■		■		■	■			■		■	■	■	■		■	■	■		
AficioSPC820DN	■	■	■	■	■	■	■	■	■	■	■		■		■		■	■		■	■	■	■	■	■	■		■	■	■		
AficioSPC821DN	■	■	■	■	■	■	■	■	■	■	■		■		■		■	■		■	■	■	■	■	■	■		■	■	■		
AficioGX2500	■	■																								■						
AficioGX3000*	■	■	■	■		■																				■		■				
AficioGXe3300N*	■	■	■	■		■																				■		■				
AficioGX3050N*	■	■	■	■		■																				■		■				
AficioGXe3350N*	■	■	■	■		■																				■		■				
AficioGX5050N*	■	■	■	■		■																				■		■				
AficioGX7000	■	■																								■						
ProC900	■	■	■	■	■	■	■	■					■	■	■		■		■	■				■								
Impresoras Blanco & Negro																																
AficioSP3300D/ SP3300DN	■	■	■																							■						
AficioSP4100NL	■	■	■	■	■	■	■	■	■				■					■					■	■	■	■	■		■	■	■		
AficioSP4100N-KP HotSpot	■	■	■	■	■	■	■	■	■				■					■					■	■	■	■	■		■	■	■		
AficioSP4110N-KP HotSpot	■	■	■	■	■	■	■	■	■				■					■					■	■	■	■	■		■	■	■		
AficioSP4210N	■	■	■				■	■	■		■		■					■		■			■	■		■		■	■	■		
AficioSP5100N	■	■	■			■	■	■					■		■		■									■						
AficioAP610N	■	■	■			■	■	■					■		■		■							■	■	■						
AficioSP8200DN	■	■	■	■	■		■	■	■					■				■		■	■	■	■	■	■	■		■	■	■		
AficioSP9100DN	■	■	■			■	■	■	■				■		■		■						■	■	■		■		■			

GX3000/3050N/5050N no utilizan el mismo Web Image Monitor que las otras impresoras de Ricoh. El navegador está desarrollado por Silex Technology y será ligeramente diferente al de los otros modelos.
**El GX3000/GXe3300N/GX3050N/GXe3350N/GX5050N solo soporta la función de "Filtro de Dirección IP".*
"Filtro par Dirección Mac" no es soportada.
Bloqueo/Impresión Segura solo está disponible si el Disco Rígido está instalado.

Inprint
Soluciones Avanzadas

Chihuahua:
Gabino Barreda 4509- C,
Col. Granjas, C.P. 31100
(614) 400 26 66

Cd. Juárez:
Av. A. López Mateos 924,
Col. La Playa, C.P. 32317,
dentro de Technology Hub
(656) 676 26 99

RICOH
www.inprint.mx
contacto@inprint.mx
/InprintCUU