# Xerox y la seguridad de la información

Sus datos, su empresa:
colaborar para proteger
lo más importante

# Índice

# Descripción general

La información es el principal activo de toda organización, por lo que la seguridad es crucial en la oficina —tanto para los documentos como para los dispositivos, ya sean impresoras o equipos multifunción conectados en red. En el siglo XXI, la red es el núcleo de prácticamente toda la actividad empresarial.

Casi todas las empresas y las personas que trabajan en ellas están conectadas a Internet. Su empresa —al igual que todas las organizaciones con las que colabora— forma parte de un sistema global de redes y servidores informáticos interconectados. Hay en todo momento una cantidad ingente de usuarios realizando tareas, accediendo a la información y compartiéndola, comprando y vendiendo bienes y servicios y comunicándose por correo electrónico, mensajería instantánea, Skype™, Twitter y muchos otros servicios.

La amenaza para la seguridad es muy real y lo que está en juego crece a un ritmo exponencial. La vulneración de la seguridad de los documentos de una organización puede dar como resultado la compra o el uso no autorizados de información sensible o privada. Esto puede provocar daños como consecuencia de la divulgación, el robo o la modificación de propiedad intelectual y secretos comerciales. En el caso de muchas organizaciones, estas vulneraciones de la seguridad pueden traducirse en multas elevadas y procesos judiciales costosos que pueden alcanzar cientos de miles o incluso millones de dólares.

Hoy en día las amenazas para la seguridad pueden darse de formas muy diversas y presentar diferentes niveles de gravedad. La proliferación exponencial de dispositivos conectados en red supone un número creciente de puntos potencialmente vulnerables por los que pueden colarse intrusos. Asimismo, la amenaza de los «hackers» es constante, dada la existencia de programas que se ejecutan de forma permanente para detectar y explotar automáticamente las deficiencias existentes en la seguridad de las redes.

Las amenazas para la seguridad pueden ser desde mensajes de spam relativamente inofensivos hasta amenazas persistentes capaces de dejar fuera de servicio a redes enteras.

Esta actividad constante en Internet le obliga a asegurarse de que la información confidencial de su empresa se mantiene segura. Pero las necesidades cambian a diario.

Las impresoras y equipos multifunción conectados en red, con capacidad para imprimir, copiar, escanear con destino a carpetas de red, enviar archivos adjuntos por correo electrónico y gestionar el envío y la recepción de faxes, resultan particularmente vulnerables.

Para los responsables de la seguridad de la información, la seguridad de la red de una organización precisa como requisito crucial que no puedan producirse infracciones de seguridad a través de las impresoras y los equipos multifunción conectados en red —ni en los propios dispositivos. Los ataques pueden producirse de formas inesperadas:

- La línea telefónica conectada a un equipo multifunción podría ser utilizada para acceder a la red.
- El servidor web utilizado para gestionar los equipos multifunción y las impresoras puede ser vulnerable a ataques.
- Podría accederse sin autorización a datos electrónicos no protegidos mientras se encuentran en el disco duro o mientras se están transfiriendo desde/hacia el dispositivo.
- Pueden enviarse correos electrónicos malintencionados desde un equipo multifunción sin que quede ningún rastro para auditarlo.

Las impresoras y los equipos multifunción son sofisticados, por lo que las plataformas informáticas de los múltiples subsistemas y las medidas de seguridad deben comprender cada elemento de la plataforma.

**Las impresoras y los equipos multifunción de hoy en día difieren bastante de los PC y los servidores.**

- Las impresoras y los equipos multifunción son dispositivos compartidos con múltiples usuarios y administradores.
- Las impresoras y los equipos multifunción son dispositivos con sistemas incorporados:
  - Pueden tener un sistema operativo real dentro del sistema.
  - El sistema operativo puede contar con una interfaz externa directa.
  - El sistema operativo puede ser propio de la empresa.
  - El sistema operativo puede ser Microsoft® Windows®.

# Descripción general

- Las impresoras y los equipos multifunción cuentan con los siguientes elementos, todos ellos normalmente asociados a nodos informáticos más avanzados:
  - Pilas de protocolos de red
  - Funciones de autenticación y autorización
  - Cifrado
  - Gestión de dispositivos
  - Servidores web

**La heterogeneidad de las implementaciones de impresoras y equipos multifunción plantea problemas.**

- Existe mucha más diversidad que entre los PC tradicionales.
- Existe un alto grado de diversidad entre los sistemas operativos subyacentes utilizados por los diferentes fabricantes e incluso dentro de la gama de productos de un mismo fabricante.

**Los controles tradicionales de PC y servidor no están optimizados para impresoras y equipos multifunción.**

- Enfoque de antivirus
  - Puede no estar disponible para el tipo de sistema operativo utilizado en la impresora o el equipo multifunción
  - En cualquier caso suele perder la batalla contra el malware
  - Complejidad de la gestión de la actualización de archivos de datos en un entorno distribuido
- Aplicación de parches a impresoras y equipos multifunción
  - El control de las versiones del software de impresoras y equipos multifunción no es riguroso
  - La gestión de la configuración genera gastos operativos
- Security Information and Event Management (SIEM)
  - Las alertas y la notificación de impresoras y equipos multifunción se producen de forma desigual
  - La aplicación de soluciones para impresoras y equipos multifunción no está estandarizada

**Esto supone un cambio radical con respecto a las impresoras y copiadoras del pasado.**

Prácticamente cualquiera puede lanzar ataques contra una red o contra los activos de información de una empresa si el acceso físico y electrónico a una impresora o equipo multifunción no se controla y protege de forma segura. Dichos ataques pueden consistir simplemente en que alguien se lleve documentos que se han dejado en la bandeja de salida de la impresora o el equipo multifunción, o bien pueden ser gusanos malintencionados que extraen documentos sensibles de la red.

Todo el sistema de una impresora y un equipo multifunción, así como el software de gestión de los dispositivos de la red, deben evaluarse y certificarse de forma que la seguridad de la información y todos los trabajadores de la organización tengan la certeza de que sus documentos y la red son seguros y están protegidos frente a los depredadores de la información —o incluso frente a vulneraciones internas de la seguridad.

En este sentido, no todas las impresoras y equipos multifunción son iguales. Por consiguiente, es crucial contar con un enfoque amplio basado en una seguridad funcional, de fundamentos, avanzada y útil para proteger los activos de información de las empresas de hoy en día.

Afortunadamente, Xerox cuenta con prestaciones de seguridad que pueden ayudarle. Xerox lleva 20 años liderando el mercado de soluciones de documentos protegidos para diversos sectores en todo el mundo. De hecho, todos los productos y servicios Xerox® que ofrecemos han sido diseñados teniendo en cuenta la seguridad y su integración armonizada en los entornos de seguridad ya existentes. Además, la seguridad se gestiona durante todo el ciclo de vida de los productos, comenzando con el análisis de requisitos, continuando con el diseño, el desarrollo, la fabricación y el despliegue y terminando con el desecho del producto, lo que les ofrece a usted y a sus clientes mayor protección y tranquilidad.

En Xerox contribuimos a proteger sus datos en todos los puntos potencialmente vulnerables para que usted no tenga que hacerlo. Al centrarnos en lo que mejor sabemos hacer, usted puede centrarse igualmente en su actividad de negocio.

### Objetivos de seguridad de Xerox

Hemos identificado cinco objetivos de seguridad principales en nuestra cruzada por ofrecer soluciones seguras a todos y cada uno de nuestros clientes:

**CONFIDENCIALIDAD**

- Ausencia de divulgación no autorizada de datos durante su procesamiento, transmisión y almacenamiento

**INTEGRIDAD**

- Ausencia de modificaciones no autorizadas de los datos
- Los sistemas funcionan de la forma prevista y sin manipulaciones no autorizadas

**DISPONIBILIDAD**

- El sistema funciona correctamente
- No se producen denegaciones de servicio a los clientes autorizados
- Protección contra el uso no autorizado del sistema

**RENDICION DE CUENTAS**

- Es posible mantener la trazabilidad de las acciones realizadas por una entidad

**ACEPTACIÓN**

- Garantía mutua de que se mantienen la autenticidad e integridad de las comunicaciones de la red

# Vulnerabilidades de seguridad: riesgos y costes para el sector

Las empresas, con independencia de su tamaño, cuentan con información sensible que los ciberdelincuentes valoran y que debe ser protegida. El panorama de las amenazas cambia constantemente. Dado el avance de las estrategias BYOD (Bring Your Own Devices), de los dispositivos corporales para datos de supervisión de la salud, de los sistemas de pago mediante móvil, del almacenamiento en la nube y de Internet de las Cosas, la amenaza es real y continúa creciendo.

Los ciberdelincuentes se centran cada vez más en las pymes debido a que son más fáciles de atacar que las grandes empresas y a que las pymes normalmente carecen de los recursos necesarios para protegerse de ataques. Las vulneraciones de la seguridad de los datos de las grandes empresas se convierten en titulares de prensa. Sin embargo, los medios no se hacen eco de los ciberataques a las pymes.

Las pymes se juegan mucho más que las grandes corporaciones. Los datos de los clientes que almacenan las pymes es una mercancía cada vez más valiosa, por lo que los costes de estas vulneraciones de la seguridad pueden devastar a una empresa pequeña o mediana. Según un estudio realizado en 2015 por IBM y Ponemon Institute, el coste medio total de una vulneración de la seguridad de los datos para las empresas encuestadas aumentó un 23% en dos años hasta alcanzar 3.79 millones de dólares.1 El coste medio pagado por cada registro perdido o robado con información sensible o confidencial aumentó de 145 dólares en 2014 a 154 dólares en 2015.[1]

Esto no incluye las posibles sanciones, el deterioro de la imagen de la empresa y la interrupción de su actividad de negocio. Puede que la seguridad no siempre sea una prioridad absoluta para la empresa, pero mantener la información protegida es crucial para la salud de la organización.

**Qué está en juego**


## Salud

Los avances en la tecnología informática —incluido el uso de ordenadores de mano— ha originado la necesidad de compartir electrónicamente datos médicos e información de pacientes, un área en la que la seguridad se convierte en un problema de primer orden.

La ley HIPAA (Health Insurance Portability and Accountability Act) fue aprobada en 1996 por el gobierno federal de EE.UU. para obligar a todas las organizaciones sanitarias a aplicar prácticas de gestión de datos uniformes con el fin de proteger la información y la privacidad de los pacientes en todo momento. La ley HIPAA exige una pista de auditoría para mantener la trazabilidad de quién vio determinados datos, cuándo los vio y si tenía autorización para ello.

Con la ley HITECH (Health Information Technology for Economic and Clinical Health), el gobierno de EE.UU. redobló sus esfuerzos por establecer un sistema nacional de conservación de registros electrónicos para el sector sanitario. La ley HITECH entró en vigor como parte de la American Recovery and Reinvestment Act de 2009 para promover la adopción y el uso racional de la tecnología informática sanitaria.

El incumplimiento de la ley HIPAA puede acarrear sanciones civiles y penales incluso en el caso de que no se produzca ninguna vulneración de la seguridad de los datos.

## Administración del Estado

Las administraciones de ámbito local, estatal y federal se afanan actualmente por simplificar los procesos y mejorar la colaboración entre las administraciones con el fin de obtener mejores resultados para los ciudadanos a los que dan servicio. Aplican para ello diversas iniciativas con el objetivo de utilizar las tecnologías más recientes, al tiempo que imponen normas estrictas para garantizar que la información compartida se mantenga segura. Ejemplo de ello es la ley contra vulneraciones de datos del Estado de Massachusetts, una de las ambiciosas del país. Los sistemas, software y servicios de Xerox® cumplen estas estrictas directrices, entre otras.

En 2014, el Departamento de Defensa de EE.UU. adoptó los estándares 800-53 del NIST (National Institute of Standards and Technology), una publicación que recomienda la aplicación de controles de seguridad a sistemas informáticos y organismos federales, así como de controles de seguridad de documentos a todos los sistemas informáticos federales salvo a los destinados a la seguridad nacional.

1. 2015 Cost of Data Breach Study: Global Analysis, IBM and Ponemon Institute, mayo de 2015.

# Vulnerabilidades de seguridad: riesgos y costes para el sector

Asimismo, el Departamento de Defensa de EE.UU. ha adoptado medidas de seguridad adicionales mediante el uso de CAC (Common Access Cards) y las tarjetas equivalentes del gobierno civil, las PIV (Personal Identity Verification). Dichas tarjetas requieren una infraestructura PKI para garantizar una autenticación y un entorno de comunicaciones seguros. La mayoría de las agencias del gobierno federal han adoptado también el estándar FIPS 140-2 para certificar módulos de cifrado empleados en impresoras y equipos multifunción. Por último, numerosos clientes del gobierno federal exigen que los productos cuenten con certificado de la norma Common Criteria.

## Servicios financieros

Los depósitos directos, la banca online, las tarjetas de débito y otros avances informáticos están revolucionando el sector de los servicios financieros. Aunque ofrecen mayor comodidad a clientes y empresas, este uso intensivo de la tecnología plantea problemas de seguridad específicos.

Resulta crucial que el intercambio de los datos de tarjetas de crédito tenga lugar de forma segura. Por ello, el cumplimiento de la norma DSS (Data Security Standard) de PCI (Payment Card Industry) contribuye a evitar vulnerabilidades y a proteger los datos de los titulares de tarjetas. DDS de PCI es un estándar de seguridad informática propio para organizaciones que gestionan tarjetas de crédito, incluidas Visa®, Mastercard®, American Express®, Discover® y JCB.

La ley GLBA (Gramm-Leach-Bliley Financial Services Modernisation Act) de EE.UU. se aprobó en 1999 con el objetivo de garantizar que las instituciones financieras que recopilan o reciben datos privados de clientes dispongan de un plan de seguridad para protegerlos. Para cumplir esta ley, las organizaciones deben realizar un análisis de riesgos de sus actuales procesos e implementar firewalls, restringir el acceso de los usuarios y supervisar la impresión, entre otras medidas.

La Dodd-Frank Wall Street Reform and Consumer Protection Act de 2010 aumenta la necesidad de recopilar e informar sobre datos financieros de forma precisa. A través de la Office of Financial Research y de las agencias que forman parte de ella, los datos se recopilarán y analizarán para identificar y supervisar los riesgos emergentes para la economía y divulgar esta información en informes periódicos y mediante testimonio anual al Congreso.

## Educación

Las instituciones educativas –ya sean de educación primaria, secundaria o universitaria– facilitan expedientes académicos, solicitudes de becas e incluso apuntes de clases a través de Internet. Dado que algunos colegios disponen de centro médico propio, también almacenan y comparten información médica electrónicamente. Este entorno interactivo mejora la experiencia de los alumnos y la productividad del personal, pero también expone a las instituciones educativas a amenazas de seguridad.

Dada la variedad de información que gestionan estas instituciones, les son de aplicación numerosos reglamentos de ámbito estatal y federal, incluidas las leyes Computer Fraud and Abuse Act, USA Patriot Act, HIPAA y GLBA. No obstante, el reglamento más aplicable al sector educativo se estipula en la ley FERPA (Family Education Rights and Privacy Act). Esta ley prohíbe la divulgación de datos de identificación personal sin permiso por escrito del alumno o el tutor del alumno.

Dada la profusión de reglamentos a los que es necesario atender, Xerox ha tomado los requisitos del gobierno federal, entre otros, como directrices. Al desarrollar soluciones que se esfuerzan por cumplir los estándares de seguridad más exigentes, podemos ofrecer soluciones altamente seguras a todos nuestros clientes —con independencia del sector económico en el que operen.

# Descripción general de la seguridad

Xerox basa el desarrollo de productos, servicios y tecnologías en su filosofía «Security = Safety», que infunde en ellos seguridad a todos los niveles.

La seguridad es nuestra prioridad absoluta cuando diseñamos nuestros «equipos multifunción inteligentes». Como líder en el desarrollo de la tecnología digital, Xerox ha demostrado su compromiso por mantener la seguridad de la información digital identificando vulnerabilidades potenciales y atajándolas proactivamente para limitar el riesgo. Los clientes han respondido eligiendo a Xerox como su proveedor de confianza de soluciones seguras que ofrecen amplias prestaciones de seguridad avanzada tanto de serie como opcionales.

## Nuestra estrategia de seguridad

El desarrollo de los productos Xerox® se realiza con arreglo a un proceso de ciclo de vida de desarrollo seguro (Secure Development Life Cycle) en el que se tienen en cuenta las directrices del Open Web Application Security Project (OWASP), el Software Assurance Maturity Model (SAMM) y el SANS Institute. Esto implica la definición de requisitos de seguridad, la evaluación de riesgos, el análisis de vulnerabilidades y la realización de pruebas de penetración, así como la integración de la información obtenida del OWASP y el SANS Institute. Esta estrategia se basa en tres pilares:

### Las prestaciones de seguridad más avanzadas

Las impresoras y los equipos multifunción son sofisticados, con múltiples subsistemas y plataformas de red, por lo que Xerox ofrece la gama más amplia de funcionalidad de seguridad del mercado, incluidos cifrado, autenticación, autorización por usuario y auditoría.

### Certificación

La única norma de certificación de seguridad reconocida internacionalmente es ISO 15408 (criterios comunes para la evaluación de la seguridad de las tecnologías de la información). Xerox fue el primer fabricante en solicitar y obtener certificaciones para equipos multifunción «completos». Puesto que cada elemento de la plataforma multifunción es un punto de entrada potencial, una certificación de seguridad seria debe abarcar todos los elementos, incluidos los sistemas operativos, la interfaz de red, el disco o discos duros, el servidor web, el intérprete o intérpretes de PDL, la interfaz de usuario del equipo multifunción, los puertos de hardware locales y el sistema de fax.

### Mantenimiento

Para Xerox, el mantenimiento de la seguridad de nuestras impresoras y equipos multifunción durante todo su ciclo de vida exige diligencia permanente para garantizar la protección continua frente a las amenazas que se van descubriendo continuamente. Esto se consigue:

- Asegurándose de que se publiquen regularmente actualizaciones del software
- Mediante notificación de nuevos boletines de seguridad con feeds RSS
- Respondiendo a las vulnerabilidades identificadas
- Facilitando directrices para una instalación y utilización seguras
- Proporcionando información sobre Common Criteria
- Facilitando parches en www.xerox.com/security

El modelo de seguridad de Xerox (Xerox Security Model), conjuntamente con el ciclo de vida de desarrollo seguro (Secure Development Life Cycle), suponen el compromiso de que todas las prestaciones y funciones del sistema, no solo una o dos de ellas, sean seguras.

## Enfoque integral de la seguridad de las impresoras y los equipos multifunción

Hace mucho tiempo que Xerox reconoció y se adaptó a este cambio tecnológico y a las necesidades cambiantes de los centros de trabajo. Ofrecemos un amplio conjunto de prestaciones de seguridad para mantener la seguridad de sus impresoras/equipos multifunción y sus datos. Xerox protege todos los factores de la cadena de datos, incluidos la impresión, copia, escaneado, fax, descarga de archivos y software del sistema. Nuestro enfoque de múltiples capas consta de cuatro aspectos fundamentales.

### 1. Prevención de intrusiones

La primera y más evidente vulnerabilidad es la interfaz de usuario: quién dispone de acceso físico a su impresora y a las funciones de esta. La autenticación del usuario es la base para conceder acceso a las impresoras y equipos multifunción Xerox® a usuarios autorizados tanto locales como de la red. Una vez autenticado, el usuario puede interactuar con el dispositivo o acceder a datos de clientes, actividad que se limita en función del rol del usuario. Las impresoras y equipos multifunción Xerox® emplean diversas tecnologías para garantizar el acceso autorizado a las prestaciones y funciones del dispositivo por parte de los usuarios y de otros dispositivos de la red. Posteriormente atajamos otros puntos de intrusión menos evidentes —lo que se envía a la impresora y la forma en que la tecnología Xerox® ConnectKey® intercepta los ataques de archivos dañados y de software malintencionado. El software de nuestros sistemas, incluidos DLM y weblets, está firmado digitalmente: todo intento de instalar versiones infectadas no firmadas provoca el rechazo automático del archivo. Los archivos de impresión también se eliminan si alguna parte de ellos se identifica como ilegítima.

#### AUTENTICACIÓN DE RED

La autenticación de red permite al usuario autenticarse en el dispositivo validando su nombre de usuario y su contraseña antes de utilizarlo. La autenticación de red autoriza a una persona a acceder a uno o varios de los siguientes servicios: Impresión, Copia, Fax, Fax de servidor, Reimpresión de trabajos guardados, Correo electrónico, Fax de Internet y Servidor de escaneado de flujo de trabajo. Asimismo, los usuarios pueden estar autorizados a acceder a una o varias de las siguientes rutas de acceso de la máquina: Servicios, Estado de trabajos o Estado de la máquina.

**1. Prevención de intrusiones**

Prevenir el acceso general a dispositivos restringidos mediante acceso de usuarios y firewall interno en la impresora.

**2. Detección de dispositivos**

Recepción de alertas al arrancar o a petición si se detectan cambios dañinos en la impresora.

**3. Protección de datos y documentos**

Mantenimiento de la seguridad de datos personales y confidenciales mediante disco duro cifrado (AES de 256 bits, con validación FIPS para muchos productos) y sobrescritura de imagen.

**4. Alianzas externas**

Proteja sus datos y dispositivos de intrusiones malintencionadas con tecnología de listas blancas de McAfee, integración de Cisco® Identity Services Engine (ISE), organismos de certificación y organizaciones de comprobación de cumplimiento.

#### MICROSOFT® ACTIVE DIRECTORY® SERVICES

La función Microsoft Active Directory Services (ADS) permite al dispositivo autenticar cuentas de usuario cotejándolas con una base de datos centralizada de cuentas de usuario, en lugar de utilizar exclusivamente la base de datos de cuentas de usuario gestionada localmente en el dispositivo.

#### AUTENTICACIÓN LDAP

Se ofrece autenticación LDAP (BIND) para autenticar con servidores LDAP la consulta de información y el acceso a esta. Cuando un cliente LDAP conecta con el servidor, el estado de autenticación predeterminado de la sesión se establece como anónimo. La utilización de BIND permite establecer el estado de autenticación de una sesión.

#### AUTENTICACIÓN SMTP

Esta función valida la cuenta de correo electrónico del usuario e impide que usuarios no autorizados puedan enviar correo electrónico desde el dispositivo. Los administradores del sistema pueden activar TLS para todas las operaciones de envío y recepción de SMTP.

# Descripción general de la seguridad

## AUTENTICACIÓN POP3 PREVIA A SMTP

Como capa de seguridad adicional, los equipos multifunción Xerox® permiten a los administradores del sistema activar o desactivar la autenticación POP3 previa a la utilización de la función SMTP. La autenticación POP3 previa a SMTP obliga a iniciar sesión en un servidor POP3 para poder enviar correo a través de SMTP.

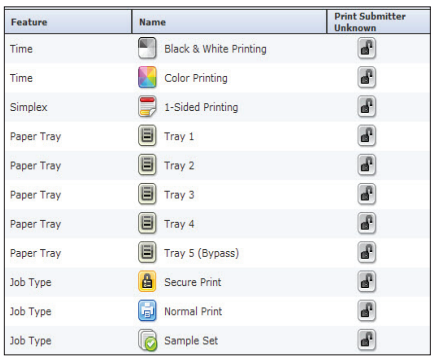
## CONTROL DE ACCESO BASADO EN ROLES (RBAC)

La función RBAC garantiza la asignación de los usuarios autenticados a un rol: usuario con sesión iniciada/sin sesión iniciada, administrador del sistema o administrador de contabilidad. Cada rol tiene asociados privilegios con niveles adecuados de acceso a las funciones, los trabajos y los atributos de la cola de impresión. Permite a los administradores elegir con precisión qué funciones se permiten para un rol determinado. Una vez que el usuario inicia sesión en el dispositivo con su nombre y contraseña, el dispositivo determina los roles asignados al usuario en cuestión. Las restricciones se aplican en función de los roles asignados. Si se restringe una función completa, esta puede mostrarse al usuario como bloqueada tras la autenticación o no mostrarse.

| Usuario con sesión iniciada/ sin sesión iniciada | Administrador del sistema | Administrador de contabilidad |
|---|---|---|

## PERMISOS DE USUARIOS DE IMPRESIÓN

Los permisos de usuario de Xerox le dan la posibilidad de restringir el acceso a funciones de impresión por usuario, grupo, hora y aplicación. Pueden configurarse usuarios y grupos con distintos niveles de acceso a funciones de impresión. Por ejemplo, pueden establecerse límites que solo permitan los trabajos de impresión en color durante determinadas horas del día; que las presentaciones de Microsoft® PowerPoint® se impriman automáticamente a doble cara; o que los correos electrónicos de Microsoft Outlook® siempre se impriman en blanco y negro.




Defina permisos de usuario para color y otras limitaciones de impresión mediante interfaces gráficas intuitivas.

## AUTENTICACIÓN MEDIANTE TARJETA INTELIGENTE

La autenticación mediante tarjeta inteligente, también conocida como autenticación mediante tarjeta de proximidad o tarjeta inteligente sin contacto, protege su impresora o equipo multifunción contra el acceso local no autorizado. Los dispositivos Xerox® admiten las principales tarjetas inteligentes (CAC/PIV, .NET, Rijkspas y otras tarjetas inteligentes y de proximidad), alrededor de 30 tipos de lectores de tarjetas y 65 tarjetas de proximidad distintas. La autenticación mediante tarjeta inteligente permite autenticar a los usuarios empleando un sistema de identificación de dos factores — posesión de la tarjeta y un número de identificación personal que se introduce en la interfaz de usuario del dispositivo— para obtener acceso a las funciones locales en el propio dispositivo y en la red.

Common Access Card/Personal Identity Verification (CAC/PIV) es una tarjeta inteligente del Departamento de Defensa de EE.UU. que se expide como identificación estándar para personal militar en activo, personal en la reserva, empleados civiles, otros empleados no gubernamentales y personal de determinadas contratas. La CAC/PIV puede utilizarse para identificación general, acceso controlado a edificios y autenticación de ordenadores personales, además de impresoras/equipos multifunción y las redes que los conectan.

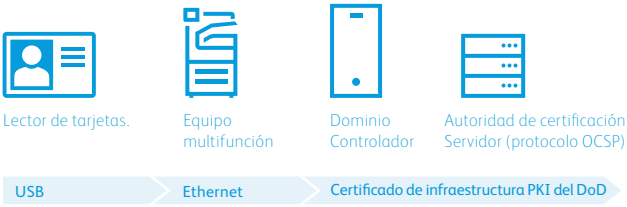
# Descripción general de la seguridad

La CAC/PIV 144k es una versión de la tarjeta inteligente. Los usuarios pueden autenticarse mediante identificación de dos factores para obtener acceso a los servicios locales del dispositivo.

La CAC/PIV 144k brinda las siguientes ventajas:

- Cifrado S/MIME de Escaneado a e-mail para sí mismo o para cualquier destinatario de la libreta de direcciones local del equipo multifunción o global de LDAP
- Firma digital mediante certificado de firma de correo electrónico de la tarjeta del usuario
- Relleno automático del campo «Para:» al utilizar la función Escanear a e-mail del equipo multifunción
- Clave de certificado de hasta 2048 bits
- Restricción de transmisiones salientes a destinatarios con certificados válidos
- Recepción de informes de confirmación de correo electrónico y mantenimiento de registros de auditoría
- Inicio de sesión único para Escaneado a destino predefinido y LDAP

## Diagrama de configuración para Common Access Card (CAC)/ Personal Identity Verification (PIV)




1. Se introduce una tarjeta en el lector y se indica al usuario que introduzca un PIN en el equipo multifunción.
2. El equipo multifunción consulta al servidor OCSP para confirmar que el certificado de la tarjeta no ha caducado y luego acredita de nuevo la «cadena de confianza» a una autoridad de certificación conocida.
3. El equipo multifunción inicia un diálogo cifrado de pregunta/respuesta entre el controlador de dominio y la Common Access Card. Si se realiza correctamente, el controlador de dominio emite un ticket que da derecho a obtener tickets («Ticket Granting Ticket») y finaliza la autenticación.
4. La autorización desbloquea las funciones locales del equipo multifunción:
   - Escaneado a e-mail
   - Copia
   - Fax
   - Servicios personalizados
   - Escaneado de flujo de trabajo

### SOFTWARE XEROX® PRINTSAFE

El software Xerox® PrintSafe proporciona autenticación de impresión protegida para datos impresos en la mayoría de impresoras y equipos multifunción, ya sean de marca Xerox® o de otros fabricantes. Este software es abierto y permite trabajar con varios de los lectores y tarjetas estándar del sector.

**Flujos de trabajo de impresión seguros, cómodos y flexibles**

El usuario envía el documento.

Simplemente pulsando «imprimir», el documento queda retenido hasta que se produce la autenticación.

El usuario puede acudir a cualquier impresora o dispositivo multifunción de la red que esté habilitado para aceptar un trabajo de PrintSafe y se autentica pasando una tarjeta o mediante un PIN.

Una vez autenticado el usuario, este puede optar por liberar un solo trabajo o todos los trabajos en la impresora o equipo multifunción.

El software Xerox® PrintSafe no está limitado a dispositivos Xerox®. Cualquier impresora o equipo multifunción* registrado en el software Xerox® PrintSafe puede generar trabajos de PrintSafe.

La flexibilidad de los flujos de trabajo permite al usuario cargar software en su PC para impresión directa o en un servidor de impresión, que puede configurarse fácilmente para el software Xerox® PrintSafe.

*Los dispositivos no Xerox® requieren un accesorio de red; consulte al comercial de Xerox para obtener detalles de las marcas y modelos compatibles.

### ACCESO MEDIANTE LA INTERFAZ DE USUARIO DEL DISPOSITIVO Y MEDIANTE INTERFAZ DE USUARIO REMOTA

Los administradores del sistema pueden bloquear el acceso de usuarios no autorizados a las pantallas de configuración del dispositivo desde el panel de control y la utilidad de interfaz de usuario remota con el fin de proteger la información de configuración.

## 2. Detección de dispositivos

En el caso improbable de que se eludan sus defensas de datos y de red, la tecnología Xerox® ConnectKey® realizará una comprobación exhaustiva de verificación del firmware, bien durante el arranque* o bien al ser activada por usuarios autorizados. Recibirá una alerta si se han detectado cambios dañinos en la impresora o en el equipo multifunción.
En el caso de que se detecten anomalías, el dispositivo mostrará un mensaje en el que aconsejará al usuario que vuelva a cargar el firmware. Nuestras soluciones integradas más avanzadas utilizan tecnología de listas blancas** de McAfee® que supervisa constantemente el sistema e impide automáticamente la ejecución de software malicioso.

En colaboración con Cisco, Xerox ha implementado su tecnología de creación de perfiles de dispositivos en Cisco® Identity Services Engine (ISE). La integración con Cisco Identity Services Engine (ISE) detecta automáticamente los dispositivos Xerox® en la red y los clasifica como impresoras para la implementación y el cumplimiento de las políticas de seguridad.

Para obtener más información, consulte los siguientes informes:

Informe de listas blancas de McAfee (solo en inglés):
**http://www.office.xerox.com/latest/SECWP-03.PDF**

Informe de Cisco ISE (solo en inglés):
**http://www.office.xerox.com/latest/SECWP-04.PDF**

*Impresoras y equipos multifunción Xerox® VersaLink®
**Equipos multifunción Xerox® AltaLink® e i-Series

## 3. Protección de datos y documentos

### Protección de documentos

Aunque se disponga de todas las medidas de seguridad de red necesarias para proteger de forma efectiva datos críticos cuando se transmiten entre los ordenadores de los usuarios y los dispositivos de impresión, las tecnologías de seguridad también deben garantizar que los documentos impresos que contengan información sensible solo puedan ser recibidos y vistos por sus legítimos destinatarios. Xerox emplea las tecnologías más recientes para proteger sus documentos, con independencia de si los imprime o los distribuye electrónicamente.

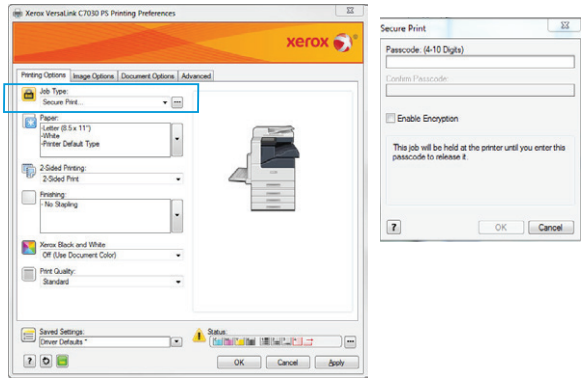
#### CIFRADO DE DATOS ESCANEADOS

Los usuarios de nuestros equipos multifunción inteligentes i-Series y de las series VersaLink® y AltaLink® habilitados para la tecnología Xerox® ConnectKey® también ofrecen la posibilidad de cifrar los archivos PDF con una clave al utilizar el servicio Escanear a e-mail.

- Protección fuera del firewall
  - Seguridad de los datos en un entorno inseguro
  - Uso de protocolos estándar del sector como TLS y Secure PDF

#### CIFRADO DE LOS DATOS DE IMPRESIÓN

Xerox® Global Print Driver® y algunos controladores de productos admiten el cifrado de documentos al enviar trabajos de Impresión protegida a dispositivos habilitados para la tecnología ConnectKey. Los equipos multifunción Xerox® AltaLink e i-Series también admiten el cifrado de documentos para trabajos de impresión normales. No se precisa hardware adicional para el cifrado del controlador de impresión.




#### IMPRESIÓN PROTEGIDA

Los trabajos de impresión que contienen información sensible se retienen en la impresora o equipo multifunción hasta que el propietario de los documentos los libera introduciendo su PIN exclusivo mediante la interfaz de usuario del dispositivo. Esto garantiza que el destinatario del documento esté presente físicamente a la hora de imprimir información sensible para recoger el documento en la impresora o el equipo multifunción. De este modo otros usuarios del dispositivo no podrán tener acceso a los documentos.


La impresión protegida basada en tecnologías de tarjetas Common Access Card (CAC)/Personal Identity Verification (PIV) adjunta al trabajo de impresión el certificado de identidad del remitente del trabajo de impresión. El usuario debe autenticarse en el dispositivo con su tarjeta CAC/PIV para que se libere el trabajo.

#### PDF CIFRADO/PDF PROTEGIDO CON CLAVE

Al escanear un documento impreso para su distribución electrónica a través de la función Escanear a e-mail, los equipos multifunción Xerox® pueden crear PDF con cifrado AES de 128 o 256 bits o PDF protegidos con clave, que posteriormente se transmiten de forma segura a través de la red y solo pueden ser abiertos, impresos o modificados por quienes dispongan de la clave correcta.

#### REENVÍO DE FAXES A CORREO ELECTRÓNICO Y RED

Los equipos multifunción Xerox® con capacidad de reenvío de fax pueden enviar los faxes entrantes a las bandejas de entrada de correo electrónico de destinatarios concretos y/o a un depósito seguro de la red, donde solo podrán acceder a ellos los usuarios autorizados.

#### CONFIRMACIÓN DE DESTINO DE FAX

El remitente de un fax recibe confirmación automática de que el fax que ha enviado ha sido recibido correctamente por su destinatario.

# Descripción general de la seguridad

### FIRMAS DIGITALES

Una firma digital es un esquema matemático para demostrar la autenticidad de un mensaje o documento digital. Se utiliza firma digital para evitar que el firmware del dispositivo pueda ser modificado sin que se detecte dicha actividad y para facilitar la autenticación del origen de los datos. La utilización de tarjetas inteligentes permite firmar digitalmente correos electrónicos con el certificado del remitente. Una firma digital válida ofrece al destinatario la garantía de que el mensaje fue creado por un remitente conocido y que no ha sido modificado en tránsito.

### MARCAS DE AGUA SEGURAS

Algunas impresoras y equipos multifunción Xerox® disponen de una función de Marca de agua segura que contribuye a impedir la copia de impresiones originales con información sensible. Si se copia un documento con marca de agua segura, la imagen de la marca de agua resulta visible, lo que deja constancia de que el documento contiene información sensible que ha sido reproducida ilegalmente.

### SELLO DE USUARIO / HORA / FECHA

Empleando controladores de Xerox®, es posible aplicar un sello de usuario/hora/fecha a cualquier documento impreso en cualquier dispositivo conectado a la red. Esto permite mantener una pista de auditoría para conocer quién imprimió cada documento y a qué hora lo imprimió.

### FILTRADO DE DIRECCIONES IP

El filtrado IP (Internet Protocol) permite a los administradores del sistema crear reglas para aceptar o rechazar la información que llega al equipo multifunción en función de si procede o no de direcciones o rangos de direcciones IP concretos. Esto permite al administrador del sistema controlar quién puede acceder al dispositivo y quién no.


**Direcciones IP registradas:**
Disponible




**Direcciones IP no registradas:**
No disponible

### SECURE SOCKETS LAYER (SSL) / TRANSPORT LAYER SECURITY (TLS)

Muchas organizaciones están obligadas a cumplir políticas de seguridad que exigen que todas las transacciones entre el cliente y la impresora o equipo multifunción estén protegidas mediante transacciones web seguras, transferencias de archivos seguras y correos electrónicos seguros. Los datos que se transmiten sin cifrar a través de la red pueden ser leídos por cualquier persona que espíe la red. Xerox mitiga este problema mediante la utilización de Secure Sockets Layer/Transport Layer Security para transmisiones de datos a través de determinados protocolos como HTTPs e IPP.

### CIFRADO IPSEC

IPsec (Internet Protocol Security) protege todas las comunicaciones en la capa de IP y se utiliza principalmente para cifrar los trabajos enviados a imprimir al dispositivo. Cifra todo el tráfico entre un punto A y un punto B de tal forma que solo los usuarios de confianza puedan enviar y recibir la información, los datos no se modifiquen durante su transmisión y solo los usuarios autorizados puedan recibir y leer la información.

IPsec está diseñado para ofrecer los siguientes servicios de seguridad:

- Cifrado del tráfico (impide la lectura de comunicaciones privadas por parte de personas que no sean sus legítimas destinatarias)
- Validación de la integridad (garantiza que el tráfico no haya sido modificado a lo largo de la ruta)
- Autenticación de par (garantiza que el tráfico proceda de una fuente de confianza)
- Antirreproducción (protección contra la reproducción de la sesión protegida)

### ACTIVACIÓN / DESACTIVACIÓN DE PUERTOS DE LA RED

Gracias a la prestación de activación/desactivación de puertos de la red, es posible desactivar los puertos y servicios que no son necesarios para evitar accesos no autorizados o malintencionados. En dispositivos de sobremesa pequeños, estas opciones pueden ajustarse a través del panel de control o de software de configuración para PC. Los equipos multifunción grandes facilitan herramientas para establecer niveles de seguridad y desactivar puertos y servicios específicos.

# Descripción general de la seguridad

### CERTIFICADOS DIGITALES

Los certificados digitales son documentos electrónicos que utilizan una firma digital para vincular una clave pública a una identidad — datos tales como el nombre de una persona o una organización, su dirección, etc. El certificado puede utilizarse para verificar que una clave pública pertenece a una persona.

Los equipos multifunción pueden añadir firmas digitales para verificar el origen y la autenticidad de un documento PDF. Cuando el destinatario abre un archivo PDF que ha sido guardado con una firma digital, puede ver las propiedades del documento para revisar el contenido de la firma, incluida la autoridad de certificación, el nombre de producto del sistema, el número de serie y el sello con la fecha/hora de creación. Si la firma es una firma de dispositivo, también contendrá el nombre del dispositivo que creó el documento, mientras que una firma de usuario verifica la identidad del usuario autenticado que envió o guardó el documento.

Es posible cargar en los equipos multifunción Xerox® un certificado firmado por una autoridad de certificación como VeriSign. Asimismo, el administrador del sistema puede crear un certificado autofirmado en el propio dispositivo. Configurando un certificado en su dispositivo, puede activar el cifrado de tipos específicos de flujos de trabajo.

### SNMPV3

SNMP (Simple Network Management Protocol) es un protocolo estándar de Internet para la gestión de dispositivos en redes IP que proporciona mayor seguridad a través de la protección de datos contra manipulaciones, garantizando la restricción del acceso exclusivamente a los usuarios autorizados a través de autenticación y cifrado de datos enviados a través de una red.

Los dispositivos que normalmente admiten SNMP son routers, switches, servidores, estaciones de trabajo, impresoras y racks modernos, entre otros. Se utiliza principalmente en sistemas de administración de redes para supervisar en los dispositivos conectados a la red condiciones que requieran la atención de los administradores. SNMP es un componente de Internet Protocol Suite, conforme a la definición establecida por IETF (Internet Engineering Task Force). El protocolo SNMPv3 proporciona funciones de seguridad con mejoras significativas, como cifrado de mensajes y autenticación.

### CADENAS DE NOMBRES DE COMUNIDAD SNMP

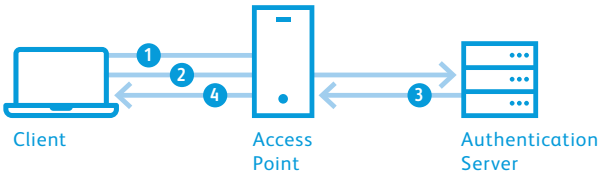
Los datos MIB (Management Information Base) de solo lectura típicos utilizan la cadena «pública», mientras que las cadenas de comunidad de lectura-escritura se configuran como «privadas». Mediante el uso de cadenas de nombres de comunidad de lectura-escritura, una aplicación puede cambiar los parámetros de configuración del dispositivo empleando variables MIB. Los administradores del sistema pueden modificar las cadenas de nombres de comunidad de lectura-escritura de los dispositivos Xerox® para aumentar la seguridad al gestionar equipos multifunción que utilizan SNMP.

### AUTENTICACIÓN 802.1X

IEEE 802.1X es un estándar IEEE para control de acceso a red basado en puerto (PNAC). Forma parte del grupo de protocolos de red IEEE 802.1. Proporciona un mecanismo de autenticación para dispositivos que quieran conectarse a una red de área local (LAN) o red de área local inalámbrica (WLAN). La funcionalidad IEEE 802.1X es compatible con numerosos switches Ethernet e impide que puedan conectar con la red sistemas invitados, no autorizados o no gestionados que no pueden realizar con éxito la autenticación.

**Cómo funciona: Autenticación 802.1X**

La autenticación 802.1X para LAN inalámbricas proporciona autenticación centralizada mediante servidor de usuarios finales.




1. Un cliente envía un mensaje de «inicio» a un punto de acceso, que solicita la identidad del cliente.
2. El cliente responde mediante un paquete de respuesta que contiene una identidad, tras lo cual el punto de acceso reenvía el paquete al servidor de autenticación.
3. El servidor de autenticación envía un paquete de «aceptación» al punto de acceso.
4. El punto de acceso pone el puerto del cliente en estado autorizado y se permite el inicio del tráfico.

# Descripción general de la seguridad

El uso del protocolo 802.1X se ha hecho extensivo debido a la popularidad de las redes inalámbricas. Muchas organizaciones bloquean el puerto de acceso a sus redes internas mediante este protocolo. Esto impide que pase información a la red hasta que sea autenticado el dispositivo. Desde el punto de vista de la gestión de riesgos, esto permite que los dispositivos tanto inalámbricos como con conexión de cable acrediten su identidad antes de que pase información por la red. Si se intenta acceder sin autorización, el puerto queda bloqueado hasta que el administrador del sistema lo desbloquee.

EAP (Extensible Authentication Protocol) es un marco de autenticación que realiza sus funciones como parte de la autenticación 802.1X. Los tipos de EAP actualmente compatibles con los equipos multifunción Xerox® son:

- EAP-MD5
- PEAPv0/EAP-MS-CHAPv2
- EAP-MS-CHAPv2
- EAP-TLS (productos AltaLink® e i-Series)

**FIREWALL**

Un firewall es un elemento de un sistema informático o una red diseñado para aislar al dispositivo de amenazas externas y del acceso no autorizado, al tiempo que permite las comunicaciones autorizadas. El dispositivo puede configurarse para que permita o deniegue transmisiones de red en función de una serie de reglas y otros criterios. Los administradores de la red pueden restringir el acceso a segmentos y servicios de la red y a puertos de los dispositivos para proteger los dispositivos.

**SEPARACIÓN ENTRE RED Y FAX**

Separar la interfaz de fax de la controladora de red evita el riesgo de que alguien logre acceder a la red de la oficina a través de la línea de fax.

El equipo multifunción no proporciona ninguna función para acceder a la red a través de la línea telefónica del fax. El protocolo Fax Class 1 utilizado en el equipo multifunción solo responde a los comandos de fax que permiten el intercambio de datos de fax. Los datos transferidos desde el PC cliente solo pueden ser datos de imágenes comprimidos con información de destino. Cualquier dato que no sea información de imágenes (como virus, código de seguridad o código de control que acceda directamente a la red) se abandona en esta fase y el equipo multifunción interrumpe la llamada de inmediato. Por consiguiente, no existe ningún mecanismo para acceder al subsistema de la red a través de la línea de fax.

## Protección de datos

La tecnología ha transformado la forma de trabajar de los empleados. Hoy en día los documentos no son exclusivamente formularios impresos tradicionales, con notas manuscritas y versiones de borrador de comunicaciones en papel, sino también formularios electrónicos de escritorio y en correo electrónico. Puesto que los empleados crean, almacenan, comparten y distribuyen estos documentos electrónicos de forma distinta a los documentos en papel tradicionales, esta información puede estar sujeta a nuevos tipos de riesgos. Para mantener la competitividad, la empresa debe atajar estas amenazas protegiendo los documentos y los sistemas de gestión de documentos que contienen su activo más valioso: el conocimiento.

La seguridad de los documentos y de los sistemas de gestión de documentos está amenazada por numerosos frentes. Entre dichas amenazas se encuentran actos de espionaje intencionados, ya sea la actividad de hackers o el robo, frade o sabotaje informáticos, y actos no intencionados como los errores humanos y los desastres naturales. La seguridad de la información va más allá de la protección. Implica el acceso puntual al contenido de los documentos y la disponibilidad del mismo para mejorar los procesos y el rendimiento empresarial. También implica la gestión de contenidos originales y el cumplimiento de la normativa.

Desde que lanzó al mercado los primeros productos digitales, Xerox ha reconocido el riesgo de que los datos almacenados sean recuperados indebidamente del almacenamiento no volátil, por lo que incorpora en los dispositivos funciones tanto proactivas como defensivas para ayudar a los clientes a proteger sus datos.

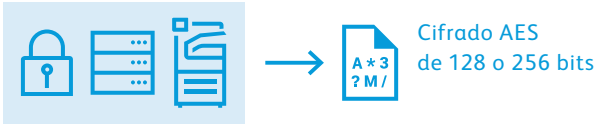
**CIFRADO DE DATOS DE IMÁGENES**

Muchos dispositivos Xerox® utilizan cifrado AES de 128 o 256 bits para cifrar datos de trabajos, imágenes y clientes, lo que protege los datos almacenados en sus equipos multifunción Xerox® frente al acceso no autorizado. Cuando se utiliza cifrado de datos, el disco se particiona y solo se cifra la partición de datos del usuario. Las particiones de sistemas operativos no pueden cifrarse.

- Cifrado AES de 128 o 256 bits con validación FIPS (Federal Information Processing Standard) 140-2.
- Se cifran todos los datos de imagen de los usuarios existentes en el disco duro.

# Descripción general de la seguridad

AES es un estándar de cifrado pequeño, rápido y difícil de descifrar, por lo que resulta adecuado para una amplia gama de dispositivos o aplicaciones. Constituye la la combinación más avanzada de seguridad, rendimiento, eficiencia, facilidad de implementación y flexibilidad. Muchos dispositivos Xerox® pueden adoptar el modo FIPS 140-2, con el que solo utilizan algoritmos de cifrado con certificado FIPS 140-2.




### SOBRESCRITURA DE IMAGEN

La sobrescritura de imagen borra los datos de imágenes del disco duro del dispositivo Xerox® cuando estos ya no son necesarios. Esto puede hacerse automáticamente al acabar el procesamiento de cada trabajo, con una programación periódica o al solicitarlo el administrador del sistema. Los dispositivos Xerox® ofrecen sobrescritura de disco inmediata o a petición.


### MEMORIA VOLÁTIL Y NO VOLÁTIL

El controlador de cada equipo multifunción Xerox® incluye memoria volátil (RAM) y memoria no volátil (disco duro). Con la memoria volátil, todos los datos de imágenes se pierden al apagar o reiniciar el sistema. Con la memoria no volátil, los datos de imagen normalmente se almacenan en una memoria flash o en el disco duro del equipo multifunción, donde se conservan hasta que son borrados.

Dada la creciente preocupación por la seguridad de los datos, los clientes quieren conocer cómo y dónde pueden estar en riesgo los datos. Las declaraciones de volatilidad (Statements of Volatility) son documentos creados para identificar los lugares de los dispositivos Xerox® en los que están ubicados los datos. Una declaración de volatilidad describe las ubicaciones, capacidades y contenidos de los dispositivos de memoria volátil y no volátil de un determinado dispositivo Xerox®.

Se han elaborado declaraciones de volatilidad para numerosos dispositivos Xerox® con el fin de ayudar a los clientes preocupados por la seguridad. Estos documentos pueden obtenerse a través del equipo de asistencia local de Xerox (para clientes ya existentes), a través de un comercial de Xerox (para clientes nuevos) o en www.xerox.com/security.

### FAX PROTEGIDO

Los faxes entrantes con contenido sensible se retienen hasta que los libera el administrador del sistema.

### ESCANEADO A BUZÓN CON PROTECCIÓN MEDIANTE CLAVE

Al utilizar la función Escanear a buzón de un equipo multifunción, el buzón designado puede protegerse mediante clave para garantizar que solo las personas autorizadas puedan acceder a los documentos escaneados que se almacenan en él. La seguridad de Escanear a buzón se fortalece aún más con el cifrado de la partición de datos de imágenes del disco duro.

### S/MIME PARA ESCANEADO A E-MAIL

S/MIME (Secure/Multipurpose Internet Mail Extensions) ofrece los siguientes servicios de seguridad criptográfica para la función Escanear a e-mail: autenticación, integridad y aceptación de origen de mensaje (empleando firmas digitales) y privacidad y seguridad de los datos (empleando cifrado).

Al enviar datos a la red con la comunicación S/MIME, se añade una firma al mensaje de correo electrónico basada en la información del certificado conservado en el dispositivo. El cifrado se realiza al enviar los datos partiendo del certificado correspondiente a la dirección designada para cada mensaje de correo. El certificado se verifica cuando se introduce la información de transmisión de los datos y cuando se van a enviar los datos. La comunicación S/MIME solo se utiliza si se ha confirmado la validez del certificado.

### CIFRADO DE ESCANEADO A E-MAIL

El cifrado de correo electrónico con autenticación mediante tarjeta inteligente permite a los usuarios enviar hasta 100 correos electrónicos cifrados a múltiples destinatarios del directorio LDAP de una organización empleando las claves públicas de los destinatarios. La mayoría de los equipos multifunción Xerox® que utilizan autenticación mediante tarjeta inteligente también ofrecen la posibilidad de firmar digitalmente los correos electrónicos. Los usuarios pueden ver certificados de destinatarios potenciales antes de enviar el correo electrónico. El equipo multifunción impide el envío a usuarios que carezcan de certificado de cifrado. Asimismo, el equipo multifunción registra todos los correos electrónicos enviados y ofrece una opción para que el administrador reciba informes de confirmación.

### REGISTRO DE TRABAJOS OCULTO

La función estándar de registro de trabajos oculto garantiza que los trabajos procesados mediante el dispositivo no estén visibles para un usuario local ni a través de la interfaz de usuario remota. La información del registro de trabajos, aunque oculta, continúa estando accesible para el administrador del sistema, que puede imprimir un registro de trabajos en el que se indique el uso de las funciones de copia, fax, impresión y escaneado del dispositivo.

### OFERTA DE RETENCIÓN DE DISCO DURO

Con los dispositivos Xerox® se proporciona una oferta de retención de disco duro para aquellos clientes preocupados por el carácter sensible o incluso clasificado de los datos almacenados en el disco duro. Este servicio de pago permite al cliente retener sus discos duros y vaciarlos o destruirlos de la manera que consideren oportuna para mantener la seguridad de los datos de imágenes.

### VALIDACIÓN DE DATOS DE SERVICIOS REMOTOS

Muchos dispositivos Xerox® obtienen autorización del cliente antes de transmitir a Xerox datos de identificación personal (PII) y datos de identificación de clientes (CII) a través de servicios remotos.

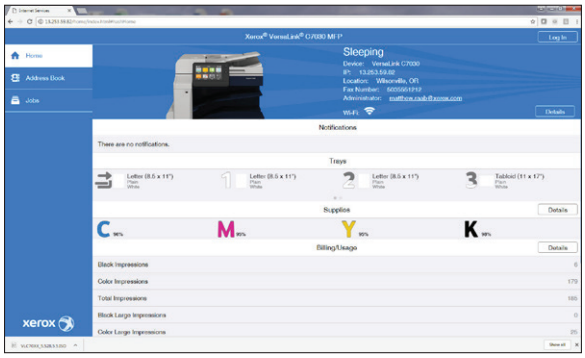
### CLAVES POSTSCRIPT

Otra área de riesgo relacionada con la impresión es cuando se imprime con el lenguaje de descripción de página (PDL) Adobe® PostScript®. PostScript incluye comandos que permiten que los trabajos de impresión modifiquen los comportamientos predeterminados del dispositivo, lo que puede poner en riesgo al dispositivo. Puesto que el lenguaje PostScript incluye utilidades muy potentes que podrían ser utilizadas para vulnerar la seguridad de un dispositivo, los administradores pueden configurar el dispositivo de forma que se exija que los trabajos PostScript incluyan una clave para cambiar los comportamientos predeterminados del dispositivo. Aunque los privilegios básicos del intérprete PostScript incluido en el controlador están limitados de fábrica, los administradores disponen de cierto margen para gestionar el funcionamiento del subsistema PostScript.

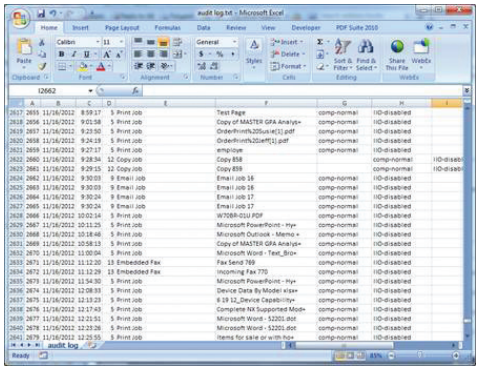
### REGISTRO DE AUDITORÍA

Los equipos multifunción Xerox®, así como muchas de sus impresoras, pueden mantener registros de auditoría para supervisar la actividad por documento, usuario y función. El registro de auditoría está activado de forma predeterminada en los dispositivos más modernos y puede ser activado o desactivado por el administrador del sistema. Permite supervisar el acceso y los intentos de acceso al dispositivo, así como transmitir registros de auditoría a un sistema SIEM o servidor de registros de auditoría. Ejemplo de entrada de un registro de auditoría: «El usuario xx inició sesión en el equipo multifunción Xerox® AltaLink® a las 12:48 AM y envió por fax 10 páginas al 888.123.1234.»

En el caso de equipos multifunción habilitados para la tecnología Xerox® ConnectKey®, el registro de auditoría puede enviarse de forma automática y segura a un sistema SIEM para disponer de una supervisión constante del equipo multifunción.




Es posible acceder a la interfaz del registro de auditoría a través de la estación de trabajo del administrador del sistema empleando cualquier navegador web estándar.



El registro puede exportarse a un archivo .txt y abrirse en Microsoft® Excel®.

## 4. Colaboraciones externas

Xerox colabora con organizaciones de comprobación del cumplimiento de la normativa y con líderes del sector de la seguridad como McAfee para armonizar sus estándares globales y conocimiento práctico con los nuestros. Las siguientes funciones de protección contra software malintencionado están disponibles en los equipos multifunción habilitados para la tecnología Xerox® ConnectKey® (equipos multifunción Xerox® AltaLink® e i-Series).

### MCAFEE® EMBEDDED CONTROL – SEGURIDAD MEJORADA

Los equipos multifunción Xerox® basados en la tecnología Xerox® ConnectKey® integran McAfee Embedded Control con tecnología Intel Security, situándose a la cabeza del sector de equipos multifunción que se autoprotegen de posibles amenazas externas. La tecnología de listas blancas de McAfee detecta intentos no autorizados de lectura, escritura o adición de archivos y directorios protegidos y envía alertas cuando esto sucede. Asimismo, la integración armonizada con el software Xerox® CentreWare® Web, el conjunto de herramientas Xerox® MPS y McAfee ePolicy Orchestrator® (McAfee ePO™) permite mantener una supervisión desde la consola que se desee.

### MCAFEE® EMBEDDED CONTROL – CONTROL DE INTEGRIDAD

El control de integridad utiliza las prestaciones de seguridad mejorada para añadir prevención de ejecución de nuevos archivos desde cualquier ubicación por medios que no sean de confianza. Solo se permite la ejecución del software aprobado, lo que evita ataques generales y específicos. La seguridad de Xerox e Intel, particularmente útil para implementaciones de seguridad en toda la empresa, ofrece tecnología de listas blancas para garantizar que la única función que desarrollan los dispositivos es prestar los servicios que usted desea. Esta misma tecnología se utiliza para proteger servidores, cajeros automáticos, terminales de puntos de venta y dispositivos incorporados tales como los dispositivos móviles.

### MCAFEE'S EPOLICY ORCHESTRATOR (EPO)

McAfee ePolicy Orchestrator (ePO) es una herramienta de software de gestión de la seguridad que facilita la gestión del riesgo y el cumplimiento a organizaciones de todos los tamaños. Presenta a los usuarios paneles aptos para arrastrar y colocar que ofrecen información de seguridad sobre todos los puntos terminales —datos, móviles y redes— para disponer de conocimiento profundo e inmediato y tiempos de respuesta más breves. ePocily aprovecha la infraestructura de IT existente mediante la conexión de la gestión de McAfee y soluciones de seguridad de terceros para sus operaciones de IT, LDAP y herramientas de configuración y gestión.

Como prueba externa independiente de que alcanzamos niveles óptimos de conformidad, organismos de certificación como Common Criteria (ISO/IEC 15408) y FIPS 140-2 evalúan nuestro rendimiento en relación con estándares internacionales. Dichos organismos valoran muy positivamente nuestra estrategia integral para la seguridad de las impresoras.

### INTEGRACIÓN DE CISCO® IDENTITY SERVICES ENGINE (ISE)

Gestione e implemente de forma centralizada las directivas de seguridad de las impresoras. Nuestra alianza con Cisco proporciona mayores capacidades de detección de los dispositivos de impresión Xerox®, con la consiguiente aplicación de directivas de seguridad más exhaustivas. Cisco ISE reconoce y clasifica automáticamente los dispositivos Xerox®, lo que hace posible el control del acceso a la red y la reducción del coste administrativo al eliminar la introducción manual de atributos de impresoras. La generación de perfiles de impresoras con Cisco ISE frustra los intentos de los saboteadores de acceder libremente a sistemas sensibles. La integración de los dispositivos de impresión de Xerox® con Cisco ISE proporciona un enfoque eficiente desde el punto de vista operativo para cumplir los objetivos de las directivas de seguridad.

# Cumplimiento de políticas y de la normativa

El cumplimento de la normativa por parte de las impresoras y los equipos multifunción es objeto de especial vigilancia debido al carácter personal y sensible de los datos que almacenan y transmiten y a los que tienen acceso. El incumplimiento de la normativa puede acarrear la pérdida de oportunidades de negocio, la pérdida de clientes o incluso procesos judiciales. Los niveles de cumplimiento exigidos varían dependiendo del país y el mercado vertical de que se trate.

La ley HIPAA (Health Insurance Portability and Accountability Act) de EE.UU. y la ley de protección de datos de Reino Unido (Data Protection Act) son ejemplos de estándares que puede que haya que cumplir para desarrollar legalmente la actividad de negocio.

Common Criteria Certification es un estándar de seguridad reconocido internacionalmente que cumple las especificaciones del Departamento de Defensa de EE.UU.

Los dispositivos Xerox®, gracias a su liderazgo en prestaciones de seguridad y a su enfoque flexible de la configuración e implementación, pueden cumplir cualquier estándar y contar con los controles necesarios para atender cualquier necesidad.

Los equipos, software y servicios de Xerox® cumplen estándares de seguridad reconocidos y los reglamentos oficiales más recientes en materia seguridad. Nuestros productos ofrecen prestaciones que permiten a los clientes cumplir dichos estándares. Estos son algunos ejemplos de dichos estándares:

- Data Security Standards (DSS) de Payment Card Industry (PCI) versión 3.0
- Sarbanes-Oxley
- Basel II Framework
- Health Insurance Portability and Accountability Act (HIPAA)
- Directiva sobre intimidad en las comunicaciones electrónicas (2002/58/CE)
- Gramm-Leach-Bliley Act
- Family Educational Rights and Privacy Act
- Health Information Technology for Economic and Clinical Health Act
- Dodd-Frank Wall Street Reform and Consumer Protection Act
- ISO-15408 Common Criteria for Information Technology Security Evaluation (Criterios comunes para la evaluación de la seguridad de las tecnologías de la información)
- ISO-27001 Information Security Management System Standards (Normas para sistemas de gestión de seguridad de la información)
- Control Objectives for Information and Related Technology (Objetivos de control para la información y tecnologías afines)
- Statement on Auditing Standards No. 70 (Declaración sobre normas de auditoría nº 70)
- NIST 800-53, adoptada por el Gobierno Federal y el Departamento de Defensa de EE.UU. en 2014 Federal Risk and Authorisation Program (FedRAMP)

## Evaluación de la seguridad de los productos

La seguridad en los documentos da tranquilidad. Una de las características clave de la gama de productos Xerox® es su compromiso con la seguridad de los datos. Nuestros equipos, programas y servicios incluyen y aplican normas de seguridad reconocidas internacionalmente y cumplen las últimas normas oficiales sobre seguridad.

### Common Criteria Certification

Common Criteria Certification (certificación de criterios comunes) proporciona una validación independiente y objetiva de la fiabilidad, calidad e idoneidad de los productos informáticos. Se trata de una normativa en la que los clientes pueden basarse para tomar decisiones documentadas sobre sus compras de material informático, lo que implica cumplir requisitos relacionados con la seguridad de la información, como ciertos niveles estrictos de integridad, confidencialidad y disponibilidad de los equipos y de los datos, la asignación de responsabilidades a individuos y la validación del cumplimiento de todos estos requisitos. Common Criteria Certification es un requisito que el gobierno federal de EE.UU. aplica a los dispositivos de hardware y software de los sistemas de seguridad nacional.

### Lograr la certificación de criterios comunes (Common Criteria Certification)

La certificación de criterios comunes es un proceso riguroso que incluye la realización de pruebas de los productos por parte de laboratorios independientes acreditados por el NVLAP (National Voluntary Laboratory Accreditation Program) para la evaluación del cumplimiento de requisitos de seguridad en los productos. Se evalúa el cumplimiento de requisitos funcionales de seguridad por parte de los productos conforme a niveles de control de evaluación (EAL) predefinidos o a requisitos de control especializados.

Las necesidades de seguridad de sectores como el sanitario o el de servicios financieros, entre otros, son igualmente importantes. Ya sea para proteger la intimidad de los clientes o los activos financieros o de propiedad intelectual, resulta crucial contar con garantías de que las redes, los discos duros y las líneas telefónicas permanecen seguros y a salvo de hackers, virus y otras actividades malintencionadas. Aunque no es un requisito obligatorio fuera del ámbito del gobierno federal de EE.UU., Common Criteria Certification permite contar con validación independiente.

Xerox cuenta con aproximadamente 150 dispositivos que han superado el proceso de certificación, lo que constituye uno de los mayores grupos de equipos multifunción certificados conforme a estos criterios comunes. Asimismo, Xerox fue el primer fabricante que certificó el dispositivo completo y es el único fabricante que siempre certifica el dispositivo completo.

Visite www.xerox.com/information-security/common-criteria-certified para ver qué equipos multifunción Xerox® han obtenido la certificación Common Criteria Certification.

# Evaluación y mitigación de riesgos

## Seguridad proactiva ante amenazas emergentes

Ofrecerle los productos y soluciones más seguros del mercado en la actualidad es solo una parte de nuestra actividad. Nuestros científicos e ingenieros se afanan por desarrollar la nueva generación de tecnologías de seguridad innovadoras para combatir las amenazas del futuro y mantener protegidos sus documentos, como la microimpresión, la seguridad de impresión mediante fluorescencia e infrarrojos, Xerox® Glossmark® y la tecnología de impresión de marcas de correlación, entre otras muchas. Para obtener más información sobre estas tecnologías, visite www.xerox.com/security.

Otras actividades que desarrolla Xerox:

### Vigilar de cerca los riesgos más recientes

Supervisamos estrechamente las bases de datos de vulnerabilidades para estar al día de la información más reciente —y evitar que usted tenga que hacerlo.

### Publicar boletines de seguridad

Somos proactivos en la distribución de parches y actualizaciones de seguridad cuando son necesarios, lo que nos permite mantener sus equipos al día y proteger sus datos.

### Distribuir feeds RSS

Distribuimos automáticamente actualizaciones al minuto a los lectores de feeds RSS de los clientes.

### Proporcionarle amplia información

Si desea documentarse más, ponemos a su disposición una biblioteca en constante crecimiento que incluye artículos de seguridad, informes y guías.

Visite www.xerox.com/security para acceder a todos nuestros recursos de seguridad.

Además de realizar exhaustivas pruebas internas, Xerox supervisa regularmente las bases de datos de vulnerabilidades que publican entidades y recursos como US-CERT y el informe Oracle® Critical Patch Updates; los boletines de seguridad de Microsoft® para conocer diversas vulnerabilidades del software y los sistemas operativos; y bugtraq, SANS.org y secunia.com para conocer vulnerabilidades del código abierto. También mantiene un exhaustivo programa interno de comprobación de la seguridad que implica análisis de vulnerabilidad y pruebas de penetración para facilitar parches plenamente comprobados.
Visite www.xerox.com/security para consultar la política de gestión y divulgación de vulnerabilidades (Vulnerability Management and Disclosure Policy).

## Boletines de seguridad e implementación de parches

Los desarrolladores de Xerox siguen un proceso formal de ciclo de vida para el desarrollo de seguridad que gestiona los problemas de seguridad mediante su identificación, análisis, priorización, codificación y comprobación. Nos esforzamos por facilitar parches de la forma más apropiada posible en función de la naturaleza, origen y gravedad de la vulnerabilidad. Dependiendo de la gravedad de la vulnerabilidad, del tamaño del parche y del producto, el parche puede implementarse por separado o como nueva versión de software para el producto en cuestión.

Dependiendo del producto Xerox® que precise un parche, los clientes pueden descargar los parches de seguridad de www.xerox.com/security. Para otros productos Xerox®, el parche de seguridad se facilita como nueva versión del software del sistema. Puede registrarse para recibir los boletines regularmente. En EE.UU., los clientes deben inscribirse para obtener el feed RSS sobre seguridad. Fuera de EE.UU., póngase en contacto con el centro de asistencia local de Xerox.

En el sitio web www.xerox.com/security se facilita el acceso a información puntualmente actualizada y a recursos importantes:

- Boletines de seguridad
- Feed RSS: Obtenga los boletines de seguridad
- Preguntas frecuentes sobre la seguridad de los productos Xerox®
- Documentos de divulgación del control de la información
- Productos con certificación Common Criteria
- Política de gestión y divulgación de vulnerabilidades
- Guía sobre seguridad de los productos
- Artículos e informes
- Declaraciones de volatilidad
- Tabla de consulta rápida de versiones de software
- Guía FTC para copiadoras digitales y equipos multifunción

www.xerox.com/security es el portal que da acceso a amplia información sobre seguridad, incluidos boletines, informes, parches y mucho más.

# Prácticas de seguridad de fabricantes y proveedores

Xerox y sus principales partners de fabricación son miembros de Electronic Industry Citizenship Coalition (http://www.eicc.info). Al suscribir el código de conducta de EICC, Xerox y otras empresas demuestran que mantienen un control exhaustivo de sus procesos de fabricación.

Asimismo, Xerox mantiene relaciones contractuales con sus proveedores principales y secundarios que dan derecho a Xerox a realizar auditorías in situ para garantizar la integridad del proceso a nivel de componentes.

Xerox es también miembro de la Asociación Aduanera y Comercial contra el Terrorismo (Customs Agency Trade Partnership Against Terrorism) de EE.UU. Esta iniciativa se centra en la seguridad de la cadena de suministro. Ejemplos de prácticas adoptadas por Xerox dentro del marco de este problema son aquellas destinadas a prevenir robos y secuestros. En América del Norte, todos los tráileres que viajan entre la fábrica y los centros de distribución de productos (PDC) y entre los PDC y los centros de logísticos de transportistas (CLC) se precintan en origen. Todos los camiones disponen de localizador GPS y se supervisan constantemente.

# Devolución y eliminación de productos

## Oferta de retención de disco duro para productos Xerox®

Xerox proporciona una oferta de retención de disco duro que permite a los clientes de EE.UU. retener de forma gratuita el disco duro de los productos Xerox® arrendados. Este servicio puede ser necesario para clientes que manejen datos extremadamente sensibles, incluso clasificados, o que cuenten con políticas o estándares normativos que exijan procesos específicos para la eliminación de discos duros.

Una vez solicitado este servicio, un técnico de Xerox se desplaza a la ubicación del cliente, extrae el disco duro y lo facilita «como está» a un representante del cliente. Actualmente Xerox no presta servicios de limpieza o destrucción de discos duros en las instalaciones del cliente. Los clientes son responsables de organizar la eliminación del disco duro físico recibido del técnico.

Para determinar si su producto Xerox® contienen disco o conocer las prestaciones de seguridad disponibles para proteger datos en los discos duros, visite www.xerox.com/harddrive.

Para obtener más detalles sobre este programa, póngase en contacto con su representante comercial de Xerox o consulte los recursos de seguridad (Security Resources) bajo la sección Articles and White Papers (Artículos e informes) de www.xerox.com/security.

Asimismo, prácticamente todas las impresoras y equipos multifunción Xerox® se suministran con cifrado de disco AES de 256 bits, así como con sobrescritura de datos de imágenes en tres pasadas, lo que garantiza que los datos del cliente estén protegidos en el nuevo equipo desde el primer momento.

# Resumen

La seguridad de la red y de los datos figura entre los principales problemas a los que se enfrentan a diario las empresas. Dado que las impresoras y los equipos multifunción de hoy en día actúan como dispositivos de red cruciales para la empresa, con capacidad para recibir y enviar datos importantes mediante diversas funciones, es prioritario contar con una seguridad completa.

Todo el sistema de un equipo multifunción, así como el software de gestión de los dispositivos de la red, deben evaluarse y certificarse de forma que la seguridad de la información y todos los trabajadores de la organización tengan la certeza de que sus documentos y la red son seguros y están protegidos frente a depredadores de la información —o incluso frente a vulneraciones internas de la seguridad. Los equipos multifunción Xerox® lideran el mercado en este terreno. Es crucial contar con un enfoque amplio basado en una seguridad funcional, de fundamentos, avanzada y útil para proteger los activos de información de nuestros clientes.

Xerox es consciente de ello, por eso continúa diseñando todos sus productos de forma que se garantice el máximo nivel de seguridad posible en todos los puntos de vulnerabilidad potenciales. Tenemos el compromiso de proteger sus datos para que usted pueda centrarse en procurar que su empresa sea lo más exitosa posible.

Para obtener más información sobre las numerosas ventajas de seguridad que ofrece Xerox, visite www.xerox.com/security.

# Lista de comprobación de seguridad

Los responsables de la seguridad informática de las empresas ya están desbordados con la gestión de las necesidades de seguridad. Las empresas pequeñas necesitan sistemas y software de seguridad eficaces que se encarguen de realizar la mayor parte del trabajo. Lo último que necesitan usted y su personal son más actividades que requieran un seguimiento constante o intervención manual para supervisar y mantener actualizado cada dispositivo y cada transferencia de datos que tiene lugar en su entorno, incluidos los equipos multifunción y las impresoras.

Un plan de seguridad de red completo debe hacer hincapié en tres puntos fundamentales y contar con una estrategia para cada uno de ellos le garantice contar con un plan que funcione.

1. Dispositivos «automáticos y con autoprotección» resilientes ante nuevos ataques
2. Cumplimiento de los estándares y reglamentos de seguridad más recientes
3. Visibilidad completa de la red

## Un nuevo estándar de seguridad para una nueva era

- La seguridad no puede ser reactiva.
- La información es una propiedad intelectual cada vez más valiosa.
- No basta con disponer de firewalls; las políticas de seguridad deben ser integrales y ubicuas.
- La protección de dispositivos incorporados forma hoy en día parte de los requisitos de seguridad fundamentales.

Xerox ofrece seguridad completa en múltiples capas que resulta fácil de implementar y gestionar y que facilita que su empresa cumpla los estándares industriales y gubernamentales. La tecnología Xerox® se somete a pruebas que validan su protección frente a accesos, datos e identidades no autorizados.

Utilice la siguiente lista de comprobación para comparar los equipos multifunción Xerox® con los productos de otros fabricantes y para determinar si los dispositivos de los competidores ofrecen el mismo nivel de seguridad de extremo a extremo que ofrece Xerox.

| | | Competidor | | |
|---|---|---|---|---|
| | **Xerox** | **1** | **2** | **3** |
| Filtro de direcciones IP/MAC | ✓ | | | |
| Cifrado IPsec | ✓ | | | |
| IPv6 | ✓ | | | |
| Autenticación 802.1X | ✓ | | | |
| Impresión protegida | ✓ | | | |
| Cifrado de escaneado a correo electrónico | ✓ | | | |
| PDF cifrados/protegidos con clave | ✓ | | | |
| Firmas digitales | ✓ | | | |
| Cifrado de disco duro | ✓ | | | |
| AES de 256 bits | ✓ | | | |
| Sobrescritura de imágenes | ✓ | | | |
| Fax protegido | ✓ | | | |
| Bloqueo de puertos | ✓ | | | |
| Protección con clave del escaneado a buzón | ✓ | | | |
| Oferta de retención de disco duro | ✓ | | | |
| Restricciones de impresión | ✓ | | | |
| Registro de auditoría | ✓ | | | |
| Control de acceso basado en roles | ✓ | | | |
| Autenticación mediante tarjeta inteligente | ✓ | | | |
| Common Access Card/ Personal Identity Verification | ✓ | | | |
| Permisos de usuario | ✓ | | | |
| Homologación Common Criteria de todo el equipo | ✓ | | | |
| Integración con herramientas estándar de gestión de redes | ✓ | | | |
| Información de seguridad actualizada mediante feeds RSS | ✓ | | | |
| Protección McAfee integrada con seguridad de Intel® | ✓ | | | |
| McAfee® ePolicy Orchestrator® Integration | ✓ | | | |
| Integración de Cisco® Identity Services Engine (ISE) | ✓ | | | |

Para más información, visite **www.xerox.com**.