KONICA MINOLTA

SEGURIDAD

Konica Minolta líder en los estándares de seguridad

En la era digital, hemos visto cómo las comunicaciones globales experimentan un crecimiento sin precedentes y los riesgos potenciales y brechas de seguridad también se han disparado paralelamente. En cualquier entorno empresarial, el uso en el día a día de copias, impresiones, escaneos y sistemas de fax, como componentes elementales de los procesos y flujos de trabajo, hacen que los MFP (periféricos multifuncionales) sean indispensables en muchos aspectos. Como consecuencia, es fundamental que estos dispositivos ofrezcan la protección necesaria para resistir las amenazas a la seguridad.

KONICA MINOLTA
ESTÁNDARES DE SEGURIDAD

Konica Minolta amplía su gama de características de seguridad estándares y las opciones en las que los profesionales se pueden apoyar: soluciones para detectar y prevenir violaciones de seguridad y evitar daños financieros y / o de reputación tanto a nivel corporativo como particular.
Konica Minolta ha sido pionera en este campo y se mantiene como líder de la industria.

Generalmente los dispositivos multifunción ofrecen una amplia gama de funciones y opciones. Por lo tanto, suponen del mismo modo un amplio espectro de agujeros de seguridad potenciales. El alcance de aspectos relativos a la seguridad para los MFP se puede agrupar en tres secciones principales:

- **Control de acceso / Seguridad de Acceso**
- **Seguridad de los datos / Seguridad Documental**
- **Seguridad de Red**

Funciones de Seguridad de Konica Minolta en un vistazo

Control de acceso	Accounting de Copia /Impresión
	Restricción de funciones
	Impresión Segura (bloqueo de trabajos)
	Protección buzón de usuario mediante contraseña
	Autenticación de usuario (ID + contraseña)
	Escaneo venas del dedo
	Lector de tarjetas IC
	Registro de eventos
Seguridad de datos	Cifrado de datos (disco duro)
	Sobre escritura de datos en disco
	Disco duro protegido por contraseña
	Borrado automático de datos
Seguridad de Red	Filtrado IP
	Control de acceso a puertos
	Encriptación SSL / TLS (HTTPS)
	Soporta IP sec
	S / MIME
	Soporta 802.1x
Seguridad de scan	Autenticación de usuario
	POP antes de SMTP
	Autenticación SMTP (SASL)
	Bloqueo de destinos manual
Otros	Modo protección de Servicio Técnico
	Modo protección de Administrador
	Captura de Datos
	Bloqueo de acceso no autorizado
	Protección de copia con marca de aguas
	PDF Encriptado
	PDF Firmado
	PDF Encriptado con ID digital
	Control de copia/ copia password

CRITERIOS COMUNES E ISO 15408 EAL3

Los dispositivos Konica Minolta están certificados casi sin excepción, de acuerdo con los criterios comunes del estándar ISO 15408 EAL3

Estas son las únicas normas internacionalmente reconocidas en materia de IT testeadas con pruebas de seguridad para los productos digitales de oficina. Las impresoras, copiadoras y softwares compatibles con la certificación ISO 15408 EAL3 han pasado por una evaluación estricta de seguridad y son capaces de satisfacer y ofrecer el tipo de nivel de seguridad que cualquier negocio espera de acuerdo a los marcos legalmente establecidos.

Konica Minolta es el líder del sector, estableciendo el punto de referencia para las características estándares de seguridad

Common Criteria Validated

"La seguridad es el elemento clave de la estrategia general de Konica Minolta ...

Konica Minolta tiene una amplia gama de funciones de seguridad orientadas a la impresión y gestión del documento, la mayoría incluidas en la gama de dispositivos bizhub. En lugar de certificar sus kits de seguridad opcionales, Konica Minolta tiene la más amplia gama de multifuncionales totalmente certificados del mercado, atendiendo a la norma ISO 15408".

Fuente: Quocirca (2011), Estudio de mercado "Cerrar la brecha de seguridad de impresión. El panorama del mercado de seguridad de impresión", p. 11. Este informe independiente fue escrito por Quocirca Ltd., una compañía principal de investigación y análisis especializada en el impacto en el negocio de la tecnología de la información y las comunicaciones (TIC).

CONTROL DE ACCESO/ SEGURIDAD DE ACCESO

A pesar de que los aspectos relativos a la seguridad tienen prioridad en la agenda de las compañías, en los ámbitos público y privado, el riesgo de seguridad que plantea un MFP es a menudo ignorado por completo. Aunque sí hay consciencia de los riesgos, a menudo se obvian, especialmente cuando hablamos de documentos e información sensible para las compañías. Esto es especialmente peligroso para los dispositivos multifunción e impresoras ubicadas en las zonas comunes, donde el personal, contratistas e incluso visitantes pueden acceder.

Debido a las avanzadas características disponibles en los MFP actuales, es fácil copiar y distribuir la información dentro y fuera de las fronteras corporativas reales y virtuales. El primer paso lógico es evitar que personas no autorizadas sean capaces de operar en un dispositivo multifunción. En primer lugar, se necesitan medidas preventivas para controlar el acceso a los dispositivos multifunción y en segundo lugar, establecer algún tipo de política de seguridad que refleje cómo se utilizan los dispositivos en el día a día y en un entorno real - Konica Minolta lo consigue asegurando al mismo tiempo que ninguna de estas medidas restrinja o limite la facilidad de uso de los sistemas.

Autenticación del usuario

Es necesario definir y establecer una política concreta y una configuración de usuarios y grupos de usuarios que puedan trabajar con un dispositivo MFP. Esto puede incluir limitaciones en los derechos de acceso, básicamente que algunos usuarios estén autorizados, mientras que otros no, para utilizar las distintas funciones, como por ejemplo la impresión en color.

Konica ofrece tres tecnologías básicas para la autenticación de usuarios:

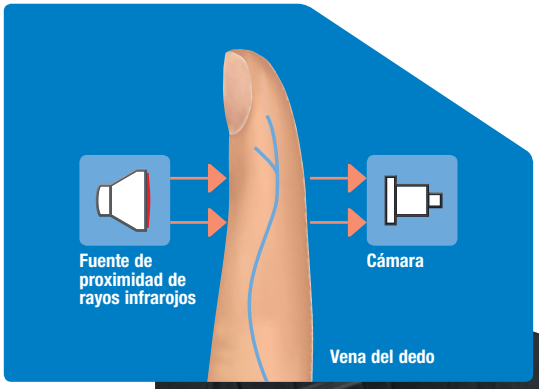
1. **Contraseña personal:**
   La contraseña, un código alfanumérico de hasta 8 caracteres, se introduce en el panel de la impresora multifunción. Estos códigos los pueden crear los administradores y usuarios. Un aspecto importante es que se pueden gestionar de forma centralizada.

2. **Autenticación de tarjeta IC**
   La mayoría de los dispositivos Konica Minolta pueden estar equipados con un lector de tarjetas IC. Están diseñados para la comodidad y velocidad, solo es necesario colocar la tarjeta IC cerca de la interfaz del lector.

Autenticación de usuario

3. **Escáner biométrico**
   Este diseño es pionero en los sistemas comunes de huellas digitales. Funciona mediante la comparación de la imagen de los patrones venosos escaneada en los dedos, con los que tiene almacenados en la memoria. La configuración venosa de un individuo es casi imposible de falsificar y es por lo tanto un medio de identificación inequívoco basado en una característica física individual. A diferencia de los sistemas de huellas dactilares, la configuración biométrica del dedo no se puede escanear sin que la persona esté presente y viva. El escáner biométrico ofrece la ventaja al usuario de no necesitar recordar contraseñas o llevar tarjetas.

La información de autenticación se puede almacenar encriptada en el dispositivo multifunción o recurrir a los datos existentes del Directorio Activo de Windows.
La información registrada del acceso y uso de cada dispositivo individual permite detectar inmediatamente errores de seguridad y solventarlos.



Seguimiento de Cuentas

Dado que el control de usuario/seguridad requiere que cada usuario inicie sesión en el dispositivo, los datos generados representan un medio eficaz de registro de actividad a varios niveles, como usuario, grupo y/o departamento. Se registra cualquiera de las funciones del dispositivo: copia en color o monocromo, escaneado o fax, impresión en b/n o color… , todo ello se puede rastrear individualmente, en el MFP o de forma remota. Mediante el análisis y tendencias de estos datos, se proporciona información sólida sobre el uso del MFP desde diferentes puntos de vista: los datos se pueden utilizar para garantizar el cumplimiento y rastrear accesos no autorizados; sobre todo, permite el registro de control y monitorización del parque completo de impresoras y dispositivos multifunción en una oficina, entorno de negocios o corporativo.

Control/ Restricción de funciones

Es posible limitar algunas funciones de un MFP a un usuario o grupo. Todo el control de acceso de Konica Minolta y funciones de seguridad no sólo ofrecen una mayor seguridad frente a las amenazas que pueden dar lugar a daños en términos financieros y de reputación, sino que también puede ser utilizados como la base para una mejor gestión y una mayor responsabilidad.

SEGURIDAD
DATOS/DOCUMENTOS

Partiendo del hecho que los dispositivos multifunción e impresoras se encuentran a menudo en las zonas comunes, donde el personal, contratistas y visitantes pueden acceder fácilmente, es necesario aplicar las políticas de seguridad a los datos. La situación es que datos confidenciales, por ejemplo almacenados en el disco duro del MFP durante un período de tiempo o simplemente documentos confidenciales que se imprimen y acumulan en la bandeja de salida del MFP, se encuentran sin protección y podrían caer en las manos equivocadas. Konica Minolta ofrece una amplia gama de medidas de seguridad a medida para garantizar la seguridad de los documentos y datos.

Seguridad HDD

La mayoría de las impresoras y multifuncionales están equipados con discos duros y memoria que pueden almacenar muchos gigabytes de datos posiblemente confidenciales, recopilados durante largos períodos. Es necesario por tanto dotar de las garantías y fiabilidad para salvaguardar y proteger la información confidencial de la empresa. Con Konica Minolta dispondrá de un conjunto de funciones que aportan esta seguridad:

- **Función Auto Borrado**
  La función de borrado automático borra los datos almacenados en el disco duro después de un período determinado

- **Protección del HDD mediante contraseña**
  Para poder acceder a la lectura de los datos, incluidos los datos confidenciales, obviamente, será necesario introducir una contraseña, incluso después de extraer el disco duro del MFP. La contraseña está relacionada con dispositivo. Los datos por lo tanto no son accesibles después de retirar el HDD del MFP.

- **Sobre escritura del HDD**
  El método más seguro de formatear un disco duro es la sobre escritura de datos. Esto se realiza de acuerdo con una serie de estándares.

- **Encriptación del HDD**
  En discos duros instalados en los dispositivos Konica Minolta los datos se pueden almacenar de forma cifrada sobre la base de un sistema de encriptación y algoritmo de 128-bit. Esta función cumple con las políticas corporativas de seguridad de datos. Una vez que una unidad de disco duro está cifrado, los datos no pueden ser leídos / recuperados, incluso si el disco duro se extrae físicamente del MFP.

Impresión segura

Los dispositivos de salida se consideran un riesgo potencial de seguridad que no debe subestimarse: como ejemplo, los documentos almacenados en la bandeja de salida pueden ser vistos o leídos por cualquier persona. No hay manera más simple para personas no autorizadas de obtener acceso a información confidencial. La función de impresión segura garantiza la confidencialidad del documento, ya que el autor de cualquier trabajo de impresión debe definir una contraseña como un candado de seguridad que se activa antes de que el documento se imprima. La función de impresión segura requiere introducir la contraseña directamente en el dispositivo de salida, cuando el usuario está presente; de lo contrario la impresión no se iniciará. Esta es una manera simple y eficaz para prevenir que los documentos confidenciales caigan en manos equivocadas.

Tocar e Imprimir/ID e imprimir

Tocar e Imprimir se basa en la autenticación biométrica o lector de tarjetas IC. Para utilizar esta función se requiere la autenticación de usuario mediante ID y contraseña. La impresión del documento se realiza inmediatamente en el dispositivo, pero sólo después de que el usuario se haya autenticado en el dispositivo multifunción con una tarjeta o utilizando el lector biométrico. La ventaja de esta característica es que los trabajos de impresión asociados se imprimen automáticamente cuando el usuario está delante del dispositivo y se autentica.

Protección contra copia

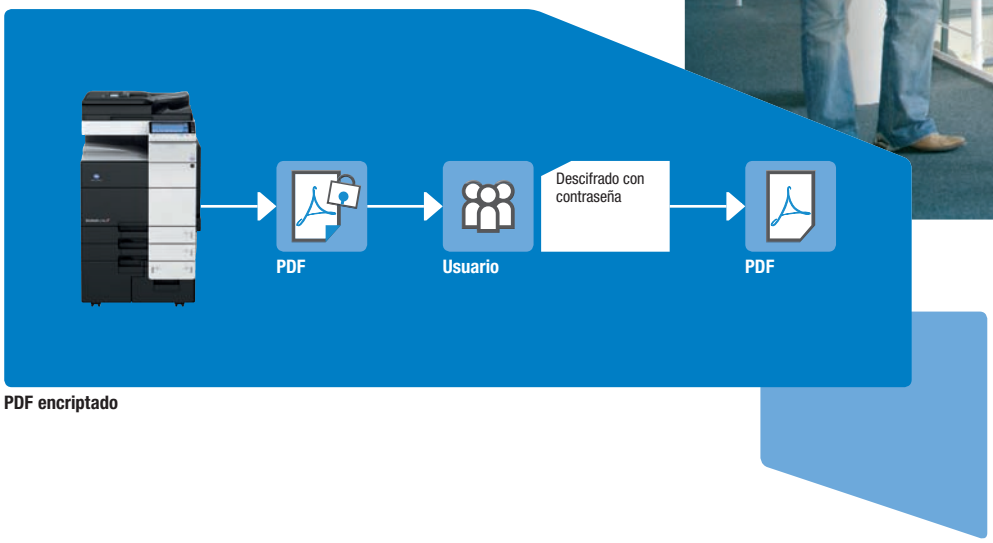
La función de protección contra copias añade una marca de agua a las impresiones y copias durante el proceso de impresión. La marca de agua es prácticamente invisible, pero si el documento se copia, aparece en primer plano en la reproducción para indicar que es una copia.

Protección de copia/Contraseña

Esta característica añade una marca de agua de seguridad oculta al original durante la impresión para evitar que se realicen copias del documento. Esta marca de aguas es prácticamente invisible y evita copiar este documento de nuevo, ya que el dispositivo está bloqueado para esta operación. La función de copia con contraseña puede anular la protección contra copia y permite realizar copias cuando se anote correctamente la contraseña en el panel de la impresora multifunción.

PDF cifrado

Los PDF encriptados están protegidos por una contraseña de usuario: Durante la fase de creación del documento PDF es posible definir si será posible imprimir, copiar e incluso añadir contenido al PDF.



PDF encriptado

PDF firmado digitalmente

Esta característica permite añadir una firma digital al fichero PDF durante el escaneo. Después de escribir el PDF, culquier cambio será monitorizado.

Recepción de Fax

Cuando está activado, los faxes recibidos se almacenan confidencialmente en un buzón de usuario.

Buzón de usuario seguro

Las carpetas de usuario están disponibles tanto para individuos como para grupos y permiten que todos los documentos se almacenen de forma segura en el disco duro del MFP antes de imprimirlos o copiarlos. Las carpetas de usuario se pueden proteger con una contraseña de ocho caracteres alfanuméricos. Una vez anotada la contraseña correcta, es posible acceder y visualizar los documentos en el buzón. Este sistema garantiza que los documentos confidenciales y los datos sólo pueden ser vistos por personas autorizadas.

SEGURIDAD DE RED

En el entorno empresarial de hoy en día, de hecho, en el mundo empresarial actual, las comunicaciones y la conectividad son indispensables. Los dispositivos Konica Minolta de oficina están diseñados para integrarse en entornos de red. Por ejemplo, las impresoras de red y periféricos multifuncionales (MFP) han evolucionado hasta el punto de que actúan como sofisticados procesadores documentales, como puntos centralizados de gestión documental dentro de la red, con la posibilidad de imprimir, copiar y escanear documentos y datos a destinos de red, así como enviar e-mails. Este escenario también significa que esta tecnología de oficina debe hacer frente y cumplir con los mismos riesgos de seguridad y las políticas que cualquier otro dispositivo de red, y representa un riesgo si no está convenientemente protegida. Con el fin de evitar cualquier vulnerabilidad de ataques de red internos y externos, Konica Minolta asegura que los equipos cumplen con las más estrictas normas de seguridad. Esto se consigue gracias a una serie de medidas que incluyen:

Bloqueo de direcciones IP

Un firewall interno básico proporciona la capacidad de filtrado IP, controlando el protocolo de red y el acceso a puertos.

Desactivación de Puerto

El modo de administración permite gestionar los puertos y protocolos para dejarlos abiertos, cerrados, activados y desactivados, ya sea directamente en el MFP o desde una ubicación remota.

S/MIME

La mayoría de los MFP de Konica Minolta soportan S/MIME (secure/multi- purpose internet mail extensions) para garantizar las comunicaciones por correo electrónico desde el MFP a los destinatarios especificados. S/MIME se utiliza para proteger de forma segura el tráfico de correo electrónico mediante la encriptación del mensaje y su contenido mediante un certificado de seguridad.

Comunicación SSL/TLS

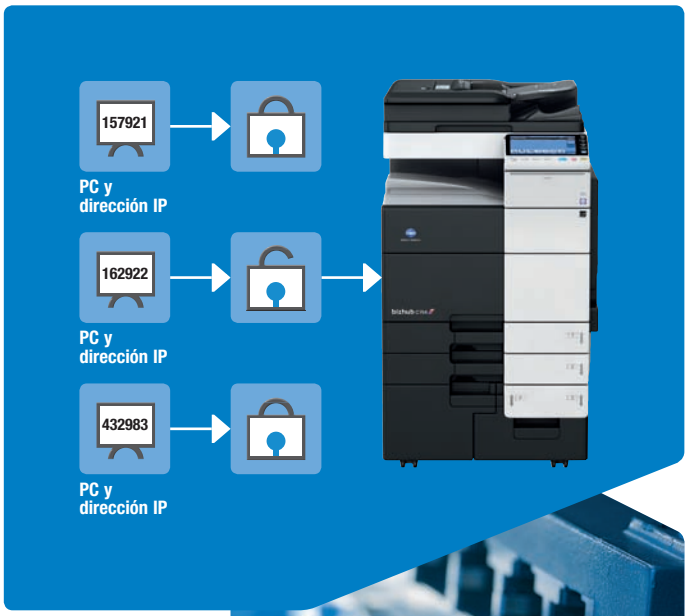
Este protocolo proporciona protección para las comunicaciones desde y hacia el dispositivo, abarca las herramientas de administración en línea y las conexiones con el Directorio Activo de Windows.

Soporte IPsec

La mayoría de los dispositivos bizhub también son compatibles con IPsec para asegurar el cifrado completo de todos los datos de la red de comunicaciones hacia y desde un MFP. El protocolo de seguridad IP encripta toda la red de comunicaciones entre la intranet local (servidor, cliente PC) y el propio dispositivo.

Soporte IEEE 802.1x

Las normas que se describen en la familia IEEE802.1x están reconocidas como estándares de autenticación y control de acceso para las redes WAN y LAN. Estos estándares garantizan una red segura por el cierre de cualquier método de comunicaciones (por ejemplo, DHCP o HTTP) a dispositivos no autorizados con la excepción de las solicitudes de autenticación.



Filtrado de direcciones IP