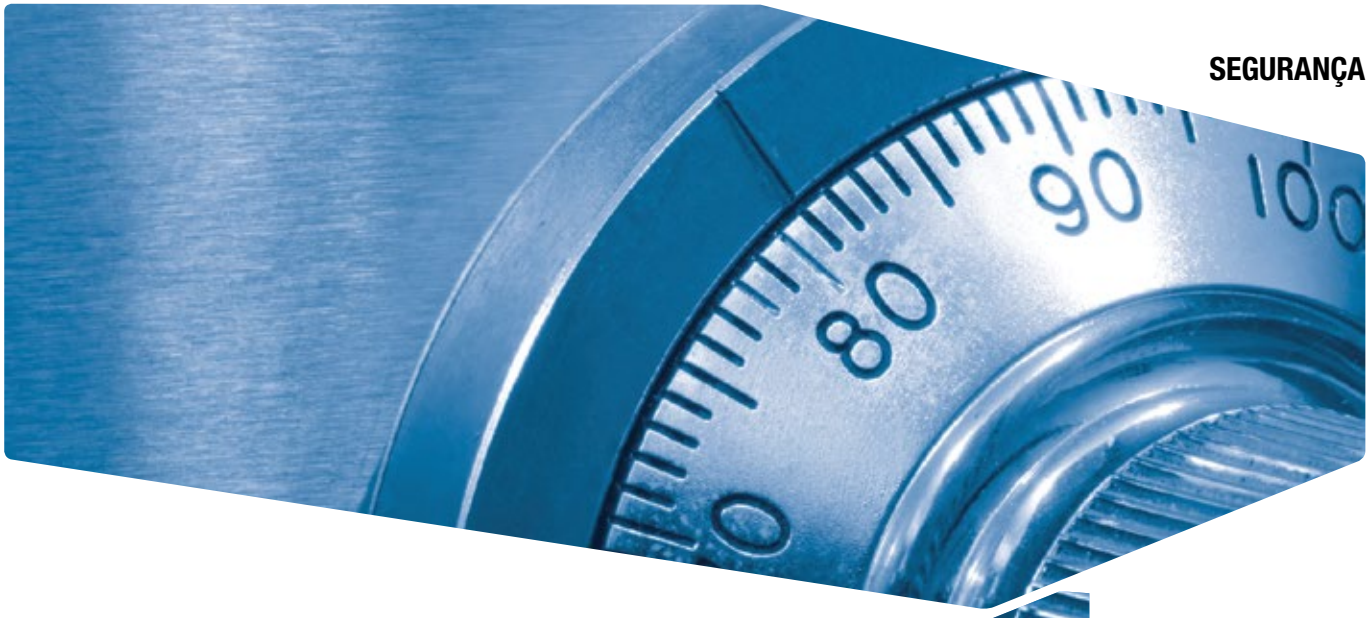
KONICA MINOLTA

SEGURANÇA

Normas de segurança da Konica Minolta líderes no sector

Na era digital, temos assistido ao crescimento sem precedentes das comunicações globais – e o potencial de quebras de segurança danosas aumentou de forma similar. Em qualquer ambiente empresarial, a utilização quotidiana de sistemas de cópia, impressão, digitalização e fax, enquanto componentes elementares de processos e fluxos de trabalho, torna os dispositivos multifuncionais indispensáveis a vários níveis. Como consequência, é de enorme importância que seja dada a proteção necessária a esses dispositivos, para que enfrentem as ameaças de segurança que são uma constante.



NORMAS DE SEGURANÇA DA KONICA MINOLTA

A gama abrangente de funções e opções de segurança padrão da Konica Minolta constitui uma base poderosa onde as soluções profissionais se podem basear: soluções que detetam e previnem violações de segurança, e evitam os danos financeiros e/ou de reputação, quer ao nível corporativo, quer individual, derivados dessas falhas. A Konica Minolta foi pioneira neste campo e continua a ser o líder do sector.

Em geral, os multifuncionais oferecem uma enorme gama de funções e opções combinadas e simples. Por isso, apresentam também um leque igualmente vasto de potenciais falhas de segurança. O âmbito da segurança dos multifuncionais pode ser dividido em três áreas principais:

- **Controlo de acesso/Segurança de acesso**
- **Segurança de dados/Segurança de documentos**

–Segurança de rede

Descrição geral das funções de segurança da Konica Minolta

Controlo de acesso	Faturação de cópia/impressão
	Restrição de funções
	Impressão segura (bloqueio de trabalhos)
	Caixa do utilizador protegida com palavra-passe
	Autenticação de utilizador (ID + palavra-passe)
	Leitor biométrico
	Leitor de cartões IC
	Registo de eventos
Segurança de dados	Encriptação de dados (disco rígido)
	Sobreposição de dados no disco rígido
	Disco rígido protegido com palavra-passe
	Auto eliminação de dados
Segurança de rede	Filtragem de IP
	Controlo de acesso de portas e de protocolos
	Encriptação SSL/TLS (HTTPS)
	Suporte de IPsec
	S/MIME
	Suporte de 802.1x
Digitalização segura	Autenticação do utilizador
	POP antes de SMTP
	Autenticação de SMTP (SASL)
	Bloqueio de destino manual
Outros	Proteção do modo de serviço
	Proteção do modo de administração
	Captura de dados
	Bloqueio de acesso não autorizado
	Proteção de cópia através de marca de água
	PDF encriptado
	Assinatura de PDF
	Encriptação de PDF através de ID digital
	Proteção de cópia/Cópia por palavra-passe

CRITÉRIOS COMUNS E ISO 15408 EAL3

Os dispositivos da Konica Minolta são todos certificados, quase sem exceção, de acordo com os Critérios Comuns/ norma ISO Norma 15408 EAL3.

São estas as únicas normas reconhecidas internacionalmente para testes de segurança na área das TI para produtos de escritório digitais. As impressoras, fotocopiadoras e softwares que estão em conformidade com a certificação ISO 15408 EAL3 passaram todos por uma avaliação de segurança extremamente rigorosa, e estão preparados para satisfazer e proporcionar níveis de segurança que uma operação comercial prudente deve procurar e tem todo o direito de esperar obter.

A Konica Minolta é líder na indústria e, como tal, estabelece o padrão de referência em tudo o que diz respeito às características de segurança padrão!

Common Criteria Validated

"A segurança é o elemento chave da estratégia global da Konica Minolta…

A Konica Minolta dispõe de uma gama abrangente de funções de segurança para documentos e impressão, muitas das quais são funções de série da gama de dispositivos bizhub da marca. em vez de certificar kits de segurança opcionais, a konica minolta afirma ter a maior gama do mercado de multifuncionais totalmente certificados com a iso 15408."

Fonte: quocirca (2011), estudo de mercado "closing the print security gap. the market landscape for print security", p. 11. este relatório independente foi redigido pela Quocirca Ltd., uma empresa de estudos e análise especializada no impacto das tecnologias de informação e comunicação nas empresas.

CONTROLO DE ACESSO/ SEGURANÇA DE ACESSO

Apesar de a segurança ocupar um lugar de destaque na agenda tanto a nível do domínio público, como a nível do domínio empresarial, o risco de segurança que os multifuncionais constituem é com frequência totalmente ignorado. Embora alguns riscos tenham sido já, talvez, identificados, são muitas vezes pura e simplesmente negligenciados, especialmente no que diz respeito a documentos e informações confidenciais. Isto pode ser especialmente arriscado no caso dos multifuncionais e das impressoras que se encontram em áreas públicas, onde podem ser acedidos por empregados, fornecedores e até visitantes.

Devido às funções avançadas disponíveis nos multifuncionais dos dias de hoje, é fácil as informações serem copiadas e distribuídas dentro e fora das fronteiras reais e virtuais das empresas. O primeiro passo lógico a dar consiste em impedir que pessoas não autorizadas consigam utilizar um multifuncional. São necessárias medidas preventivas para, em primeiro lugar, controlar o acesso aos multifuncionais, e em segundo lugar estabelecer um tipo qualquer de política de segurança que reflita a forma como os dispositivos são concretamente utilizados na vida real – a Konica Minolta consegue fazer isto, e fá-lo garantindo que nenhuma destas medidas restringe ou limita a facilidade de utilização dos sistemas.

Autenticação do utilizador

A via de autenticação começa através do estabelecimento de uma política que defina e configure os utilizadores e os grupos de utilizadores que têm autorização para trabalhar com um multifuncional. Esta política inclui limitações de direitos de acesso; basicamente, alguns utilizadores estão autorizados, enquanto outros não estão, a utilizar diferenças funções, como, por exemplo, a impressão a cores.

A Konica Minolta disponibiliza três tecnologias básicas de autenticação do utilizador:

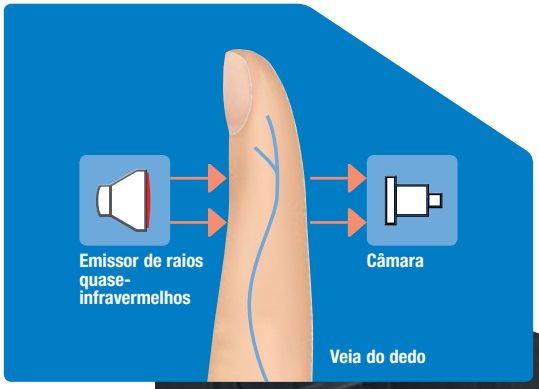
1. **Palavra-passe pessoal:**
   A palavra-passe, um código alfanumérico com um máximo de 8 caracteres, é introduzida no painel do multifuncional. Estes códigos podem ser criados para administradores e utilizadores. Um aspeto importante reside no facto de poderem ser geridos de forma centralizada.

2. **Autenticação por cartão IC**
   A maioria dos dispositivos da Konica Minolta pode ser equipada com um leitor de cartões IC. Estes leitores foram concebidos de forma a serem convenientes e rápidos; é tudo, simplesmente, uma questão de colocar o cartão IC na, ou próximo da, interface do leitor.

Autenticação do utilizador

3. **Leitor de veia do dedo biométrico**
   Este design de tecnologia de ponta constitui um grande avanço face aos mais comuns leitores de impressões digitais. Este sistema funciona comparando a imagem dos padrões das veias do dedo lido com a imagem que está guardada na memória. As veias do dedo são um dado biométrico que é quase impossível de falsificar, sendo, por isso, um meio de identificar um indivíduo com base numa característica física individual. Ao contrário dos sistemas de leitura de impressões digitais, a veia do dedo não pode ser lida sem que a pessoa esteja presente e viva.
   O leitor de veia do dedo biométrico significa que não existe necessidade de as pessoas terem de ser recordar de palavras-passe ou de trazer consigo cartões.

As informações de autenticação podem ser armazenadas no multifuncional (encriptadas) ou obtidas no Windows Active Directory, a partir de dados existentes.
O registo contínuo de informações de acesso e utilização de cada dispositivo significa que quaisquer quebras de segurança são imediatamente detetadas e assinaladas.



Monitorização de contas

Como a segurança/controlo de utilizadores requer que cada utilizador inicie sessão no dispositivo de saída, os dados gerados representam um meio eficiente de monitorizar em diversos níveis, como, por exemplo, utilizador, grupo e/ou departamento. Seja qual for a função do dispositivo utilizada, cópia monocromática ou a cores, digitalização ou fax, impressão a preto e branco ou a cores, é possível monitorizar tudo individualmente, tanto na máquina como remotamente. A análise e as tendências reveladas por estes dados são informações robustas acerca da utilização do multifuncional a partir de toda uma série de pontos de vista diferentes: os dados podem ser aplicados para garantir a conformidade e para rastrear acesso não autorizados; acima de tudo, permite que a utilização seja monitorizada em toda a frota de impressoras e multifuncionais num enquadramento empresarial/comercial/de escritório.

Controlo de funções/Restrição de funções

É possível limitar várias funções dos multifuncionais numa base de utilizador individual. Todas as funções de controlo de acesso e de segurança da Konica Minolta não só oferecem uma maior segurança contra ameaças de onde podem resultar danos em termos financeiros e de reputação, como podem ser utilizadas como base para uma melhor governação e uma prestação de contas melhorada.

SEGURANÇA DE DOCUMENTOS/DADOS

Como reflexo do facto de os multifuncionais e as impressoras estarem muitas vezes situados em zonas públicas, onde podem ser facilmente acedidos por empregados, fornecedores e visitantes, é necessário implantar políticas de segurança de dados apropriadas. O facto é que, dados confidenciais, por exemplo, dados armazenados no disco rígido do multifuncional durante um determinado período de tempo, ou simplesmente documentos confidenciais impressos que sejam deixados no tabuleiro de saída do multifuncional, se encontram inicialmente desprotegidos e podem cair nas mãos erradas. A Konica Minolta oferece um vasto leque de medidas de segurança personalizadas, para garantir a segurança de documentos e de dados.

Segurança do disco rígido

A maioria das impressoras e dos multifuncionais está equipada com discos rígidos e memória que pode guardar muitos gigabytes de dados possivelmente confidenciais, reunidos durante longos períodos de tempo.
Devem, por isso, ser implementadas medidas de salvaguarda fiáveis, para assegurar que informações empresariais confidenciais são guardadas com toda a segurança. Com a Konica Minolta, esta garantia é proporcionada por toda uma série de funções sobreponíveis e interligadas:

- **Função de auto-eliminação:**
  A função de auto-eliminação apaga os dados armazenados no disco rígido após um período de tempo definido.

- **Proteção por palavra-passe dos disco rígido interno:**
  A leitura de dados, que obviamente inclui dados confidenciais, no disco rígido requer a introdução de uma palavra-passe após a remoção do disco rígido. A palavra-passe está ligada ao dispositivo. Os dados não estão, por isso, acessíveis depois de o disco rígido ter sido removido do dispositivo.

- **Gravação sobreposta no disco rígido:**
  O método mais seguro de formatar um disco rígido consiste na sobreposição de dados no disco rígido. Esta operação é realizada de acordo com uma série de normas.

- **Encriptação do disco rígido:**
  Nos discos rígidos instalados em dispositivos da Konica Minolta, os dados podem ser armazenados numa forma encriptada baseada num sistema de encriptação algorítmica de 128 bits. Esta função satisfaz as políticas de segurança de dados empresariais. Depois de um disco rígido ter sido encriptado, os dados não podem ser lidos/obtidos, nem mesmo se o disco rígido for removido fisicamente do multifuncional.

Impressão segura

Os dispositivo de saída são considerados um risco de segurança; um risco que nunca deve ser subestimado: no nível mais simples, os documentos que ficam no tabuleiro de saída podem, pura e simplesmente, ser todos vistos e lidos por quem passa ao lado da impressora. É a forma mais simples de pessoas não autorizadas terem acesso a informações confidenciais. A funcionalidade de impressão segura é uma forma de garantir a confidencialidade dos documentos, uma vez que especifica que o autor de qualquer trabalho de impressão tem de definir uma palavra-passe como bloqueio de segurança antes de iniciar o processo de impressão propriamente dito. A função de impressão segura requer que a palavra-passe seja introduzida diretamente no dispositivo de saída, pois, caso contrário, a impressão não começa. Trata-se de uma forma simples e eficaz de impedir que documentos confidenciais caiam nas mãos erradas.

Touch & Print/ID & Print

A opção Touch & Print baseia-se na autenticação via leitor da veia do dedo ou leitor de cartão IC, ao passo que a opção ID & Print requer a autenticação pelo utilizador através de um ID e de uma palavra-passe. A impressão do trabalho em questão é imediata no dispositivo, mas só depois de o utilizador que se encontra junto do multifuncional ter sido autenticado através de um cartão IC colocado no leitor de cartões ou através de confirmação do ID, utilizando o leitor de veio do dedo. A vantagem desta função em particular reside no facto de dispensar a necessidade de um ID e de uma palavra-passe de impressão de segurança adicionais.

Proteção de cópia

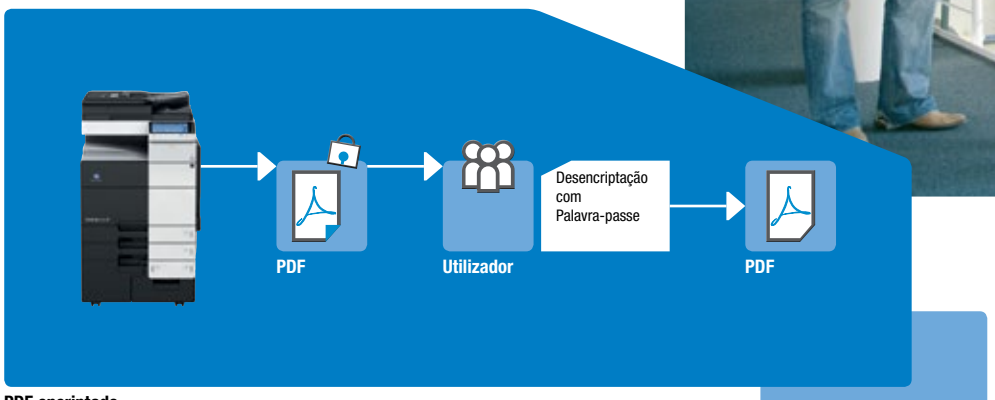
A função de proteção de cópia adiciona uma marca de água nos documentos e cópias impressos e durante o processo de impressão. A marca de água é quase invisível na impressão original, mas se o documento for copiado, passa de segundo plano para primeiro plano, para indicar que se trata de uma cópia.

Proteção de cópia/Cópia por palavra-passe

Esta função adiciona uma marca de água de segurança escondida no original durante a impressão, para impedir que sejam feitas cópias do documento. Apesar de ser praticamente invisível no documento original protegido, não é possível copiar este documento novamente, porque o dispositivo fica bloqueado e impedido de fazer esta operação. A função de cópia por palava-passe pode sobrepor-se à proteção de cópia e e permite que sejam feitas cópias quando é introduzida no painel do multifuncional a palavra-passe correta.

Encriptação de PDF

Os PDFs encriptado são protegidos por uma palavra-passe de utilizador: a autorização de imprimir ou copiar o PDF e a autorização de adicionar o conteúdo do PDF pode ser configurada durante a fase de digitalização no multifuncional.



PDF encriptado

Assinatura digital de PDF

Esta função permite que seja adicionada uma assinatura digital ao PDF durante a digitalização. Depois de um PDF ter sido escrito, isso permite que todas as alterações sejam monitorizadas.

Receção de faxes

Quando está função está ativada, todos os faxes recebidos podem ser mantidos confidenciais numa caixa de utilizador protegida.

Segurança da caixa do utilizador

As caixas de utilizador estão disponíveis quer para pessoas individualmente, quer para grupos, e permitem que qualquer documento seja armazenado com segurança no disco rígido do multifuncional antes da concretização do trabalho de impressão ou de cópia. As caixas de utilizador podem ser protegidas utilizando uma palavra-passe alfanumérica de oito dígitos. Quando é introduzida a palavra-passe correta, é possível aceder/ver documentos que se encontrem na caixa. Este sistema garante, efetivamente, que documentos e dados confidenciais só poderão ser vistos por pessoas autorizadas.

SEGURANÇA DE REDE

No atual ambiente empresarial, mais concretamente no mundo de negócios dos dias de hoje, as comunicações e a conetividade são indispensáveis. Os dispositivos de escritório da Konica Minolta foram concebidos para se integrarem em ambientes de rede. Por exemplo, as impressoras de rede e os periféricos multifuncionais evoluíram ao ponto de funcionarem como centrais sofisticadas de processamento de documentos integradas na rede, que têm a capacidade de imprimir, copiar e digitalizar documentos e dados em diferentes destinos da rede, além de enviarem emails. Este cenário significa também que esta tecnologia de escritório tem de lidar com os mesmos riscos de segurança, e de cumprir as mesmas políticas de segurança, que qualquer outro dispositivo de rede, representado também um risco se estiver desprotegida. Para evitar qualquer vulnerabilidade em termos de ataques à rede tanto internos como externos, a Konica Minolta assegura que todo o equipamento está em conformidade com as mais rigorosas normas de segurança. Isso é atingido através de várias medidas de segurança:

Bloqueio de endereço IP

Uma firewall interna básica disponibiliza uma capacidade de filtragem de endereços IP e um controlo apropriado de acesso de portas e protocolos.

Desativação de portas

O modo de administração permite que as portas e os protocolos sejam abertos, fechados, ativados e desativados tanto diretamente a partir da máquina, como a partir de uma localização remota.

S/MIME

A maioria dos multifuncionais da Konica Minolta suporta S/MIME (Secure/Multipurpose Internet Mail Extensions) para garantir a segurança de comunicações de e-mail entre o multifuncional e destinatários especificados. O S/MIME é utilizado para assegurar um tráfego de e-mail seguro encriptando a mensagem de e-mail e o respetivo conteúdo através da utilização de um certificado de segurança.

Comunicação SSL/TLS

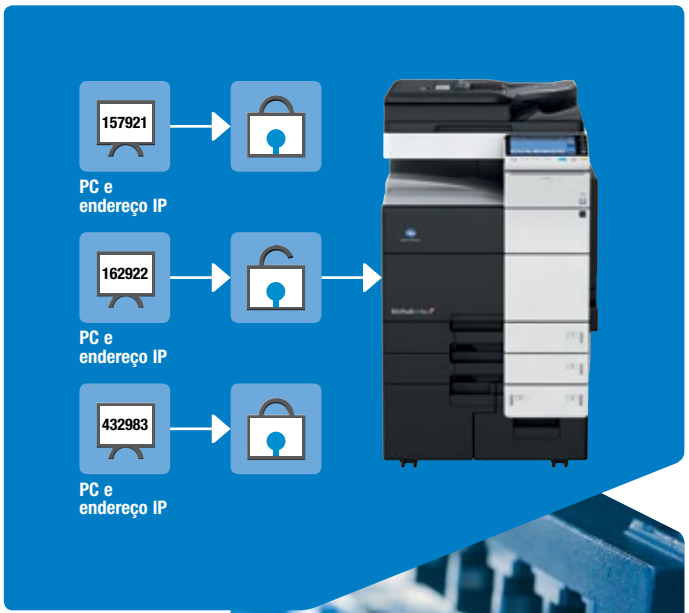
Trata-se de um protocolo que proporciona proteção para a comunicação de e para o dispositivo, abarcando as ferramentas de administração online e transmissões do Windows Active Directory, por exemplo.

Suporte de IPsec

A maioria dos dispositivo bizhub suporta também IPsec, para assegurar a encriptação completa de quaisquer dados de rede transmitidos de e para um multifuncional. O protocolo de segurança de IP encripta todas as comunicações de rede entre a intranet local (servidor, computador cliente) e o dispositivo propriamente dito.

Suporte de IEEE 802.1x

As normas descritas na família IEEE802.1x são a forma de autenticação baseada em portas reconhecida para controlo de acesso à rede para WANs e LANs. Estas normas garantem uma rede segura encerrando todas as comunicações de rede (por exemplo, DHCP ou HTTP) com dispositivos não autorizados, com a exceção de pedidos de autenticação.



Filtragem de endereço IP