White paper sobre segurança de dados do MyQ Roger 2.x

PORTUGUÊS (BRASIL)

Gerado a partir de docs.myq-solution.com
agosto/2026
Copyright © 2026 MyQ spol. s r.o. Todos os direitos reservados.

Aviso sobre a tradução

Esta tradução foi criada com o auxílio de inteligência artificial. Em caso de discrepância ou ambiguidade, prevalece o documento original em inglês.

Sumário

1 Introdução 5
2 Glossário 6
3 Segurança Operacional 7
3.1 Introdução 7
3.2 Monitoramento 7
3.3 Gerenciamento de vulnerabilidades 9
3.4 Segurança de infraestrutura 9
3.5 Fluxo de Trabalho de Desenvolvimento 10
3.6 Conclusão 11
4 Segurança de Aplicativos 12
4.1 A evolução das ameaças à segurança 12
4.2 A Abordagem de Segurança do MyQ Roger 12
4.3 Deslocamento para a Esquerda na Segurança 13
4.4 Responsabilidades de segurança da MyQ 13
4.5 Controle/Gerenciamento de Segurança do MyQ Roger 13
4.6 Microsoft Azure e conformidade 14
4.7 Responsabilidades do cliente em relação à segurança 15
4.8 Automação de segurança 15
4.9 Conclusão 16
5 Proteção de Dados 17
5.1 Visão geral 17
5.2 Segurança em nuvem multilocatária 17
5.3 Criptografia e comunicação segura 17
5.4 Conformidade e gerenciamento de identidade 18
5.5 Conformidade com o GDPR 18
5.6 Backups de dados 19
6 Política de Privacidade 20
6.1 1. Dados que coletamos ou recebemos 20
6.2 2. Como utilizamos os dados 22
6.3 3. Base legal 23
6.4 4. Períodos de retenção 24
6.5 5. Compartilhamento de seus dados pessoais para fins legais e comerciais 24
6.6 6. Estatísticas anônimas 26

6.7 7. Comunicações de marketing 26
6.8 8. Segurança e localização de seus dados 27
6.9 9. Seus direitos 27
6.10 10. Entre em contato conosco 31
7 Tempo de atividade do servidor, backup de dados e recuperação de desastres 32
7.1 Tempo de atividade do servidor 32
7.2 Monitoramento do status do sistema em tempo real 32
7.3 Estratégias de backup 32
7.4 Cenários de desastre e plano de resposta 33
8 Zero Trust 34
8.1 Entendendo a Segurança Zero Trust 34
8.2 O que é Zero Trust? 34
8.3 Como o Zero Trust se aplica ao MyQ Roger 35
8.4 Combate às ameaças cibernéticas com o Zero Trust 36
8.5 Considerações sobre conformidade e regulamentação 36
8.6 Por que o Zero Trust é importante 36
9 Login seguro com o MyQ Roger 37
9.1 Introdução 37
9.2 Autenticação segura com o MyQ Roger 37
9.3 Autenticação por PIN tradicional 37
9.4 Responsabilidade pela segurança 38
9.5 Conclusão 38
10 Impressão segura com o MyQ Roger 39
10.1 O desafio da impressão segura 39
10.2 MyQ Roger: uma solução abrangente de impressão segura 39
10.3 Métodos de impressão segura no MyQ Roger 39
10.4 Conclusão 40
11 Contatos comerciais 41

1 Introdução

O objetivo deste documento é informar os clientes do MyQ Roger sobre os processos que envolvem o estabelecimento de conexões no sistema e sobre as medidas de segurança adotadas para proteger a transferência de dados resultante.

2 Glossário

- **IPP/s (Internet Printing Protocol sobre TLS seguro)**:
  - O MyQ Roger garante a impressão segura utilizando o Protocolo de Impressão pela Internet (IPP) por meio de um canal criptografado por TLS, impedindo o acesso não autorizado e garantindo a integridade dos dados em trânsito.
  - O MyQ Roger otimiza o tráfego de rede por meio do tratamento eficiente de pacotes, reduzindo a transmissão desnecessária de dados e garantindo a comunicação segura entre os terminais.
- **TLS (Transport Layer Security)**:
  O MyQ Roger impõe o uso do TLS 1.2/1.3 para criptografia segura de dados em todas as comunicações, garantindo proteção contra interceptação e ataques do tipo “man-in-the-middle” (MITM).
- **Dados em repouso, dados em trânsito**:
  - **Dados em repouso**: O MyQ Roger criptografa os dados armazenados usando AES-256, garantindo que as informações confidenciais permaneçam protegidas contra acesso não autorizado.
  - **Dados em trânsito**: Todos os dados transferidos entre clientes, servidores e serviços em nuvem são criptografados usando TLS para manter a integridade e a confidencialidade.
- **Infraestrutura Zero Trust**:
  O MyQ Roger segue um modelo de segurança **Zero Trust**, implementando autenticação contínua, verificação de dispositivos e acesso com privilégios mínimos para usuários e serviços.
- **IAM (Gerenciamento de Identidade e Acesso)**:
  O MyQ Roger integra as melhores práticas de IAM ao impor autenticação segura de usuários, autenticação multifatorial (MFA) e controles de acesso baseados em identidade.
- **RBAC (Controle de Acesso Baseado em Função)**:
  O MyQ Roger implementa o RBAC para restringir permissões com base nas funções dos usuários, garantindo que apenas pessoal autorizado possa acessar funções críticas e dados confidenciais.
- **SSO (Single Sign-On)**:
  O MyQ Roger oferece suporte **ao SSO** por meio da integração com OAuth2, permitindo uma autenticação contínua entre aplicativos corporativos, ao mesmo tempo em que mantém a segurança e a conformidade.

3 Segurança Operacional

3.1 Introdução

A segurança é uma prioridade máxima na MyQ Roger. Adotamos uma abordagem **que prioriza a segurança** em todas as etapas de desenvolvimento, implantação e operações. Dada a natureza crítica dos ambientes em nuvem, a segurança deve ser **proativa, automatizada e monitorada continuamente** para evitar violações e acesso não autorizado.

Nossa **estratégia de Operações Seguras** integra **monitoramento contínuo, gerenciamento de vulnerabilidades, segurança de infraestrutura e conformidade** para garantir a integridade dos aplicativos e da infraestrutura.

3.2 Monitoramento

O monitoramento contínuo é essencial para detectar e responder a ameaças em tempo real. A MyQ implementa uma **abordagem de monitoramento em várias camadas:**

3.2.1 Detecção e Resposta em Terminais (EDR)

- Monitora todos os endpoints (servidores, VMs e contêineres) em busca de atividades suspeitas.
- Utiliza **análise comportamental e inteligência de ameaças** para detectar ameaças avançadas.
- Isola automaticamente os terminais comprometidos para impedir o movimento lateral.

3.2.2 Azure Defender (agora Defender for Cloud)

- Protege **o Azure AKS, o SQL Server, as máquinas virtuais e o armazenamento**.
- Oferece **detecção de ameaças em tempo real** e recomendações de configuração de segurança.
- Integra-se ao **Microsoft Sentinel (SIEM)** para alertas centralizados.

3.2.3 Verificação de hosts

- Verifica **máquinas virtuais, instâncias na nuvem e servidores locais** em busca de configurações incorretas e software desatualizado.
- Detecta **riscos de escalonamento de privilégios, pontos de acesso não autorizados e dependências desatualizadas**.

3.2.4 Coleta e análise de logs

- **Registro centralizado** em um cluster separado para escalabilidade e isolamento.
- **Os logs do Kubernetes, das aplicações e da infraestrutura** são rotulados para uma recuperação eficiente.
- **Políticas de retenção de longo prazo** garantem a conformidade e a análise de segurança.
- **Mecanismos de alerta** detectam anomalias e incidentes de segurança, integrando-se ao SIEM.
- **Correlação de logs em tempo real** para solicitações de API, eventos de autenticação, consultas a bancos de dados e tráfego de firewall.

3.2.5 Varredura de portas

- Detecta **portas abertas** não autorizadas que expõem serviços a ameaças.
- Utiliza **ferramentas automatizadas, como Nmap e ZMap,** para verificar **alterações inesperadas nas portas**.

3.2.6 Varredura de contêineres

- **Varredura estática e dinâmica** de contêineres Docker antes da implantação.
- Identifica vulnerabilidades em **imagens base, camadas de aplicativos e permissões de tempo de execução**.
- Integrado ao **Trivy** para **varredura de segurança de imagens**.

3.2.7 Monitoramento do Kubernetes

- Utiliza **o monitoramento integrado do Azure Kubernetes Service (AKS)** com **o Prometheus e o Grafana**.
- Monitora **chamadas de API do Kubernetes, políticas de RBAC e segurança de pods**.
- Gera alertas sobre **escalonamento de privilégios em contêineres, uso excessivo de recursos e tentativas de movimentação lateral**.

3.2.8 Verificações regulares de TLS

- O MyQ realiza **varreduras de segurança TLS usando o Qualys SSL Labs** para garantir o cumprimento das melhores práticas.
- As configurações de TLS são avaliadas para manter uma **classificação de segurança A+**, mitigando riscos decorrentes de protocolos fracos.
- Ferramentas automatizadas verificam **a validade dos certificados, o acompanhamento de prazos de validade e a robustez dos protocolos**.

3.3 Gerenciamento de vulnerabilidades

3.3.1 Varredura de vulnerabilidades

- **Varreduras regulares** detectam falhas de segurança em aplicativos e na infraestrutura.
- Inclui **varredura CVE automatizada** para componentes implantados na nuvem.
- Integra-se ao **DefectDojo, SonarQube e Trivy** para avaliação de riscos.

3.3.2 Testes de penetração

- Realizados regularmente para identificar pontos fracos de segurança antes que sejam explorados.
- Combina **metodologias de testes automatizados e manuais** para uma avaliação abrangente.
- As descobertas são **documentadas, priorizadas e corrigidas** de acordo com a necessidade.

3.4 Segurança de infraestrutura

Uma **infraestrutura reforçada** garante segurança que vai além do simples monitoramento. A MyQ utiliza:

3.4.1 SIEM (Gerenciamento de Informações e Eventos de Segurança)

- **O SIEM do Microsoft Sentinel** coleta eventos de segurança para detecção em tempo real.
- Analisa logs de **firewalls, sistemas de identidade, logs de aplicativos, logs de auditoria e feeds de ameaças**.
- Permite **respostas automatizadas às ameaças detectadas**.

3.4.2 Rastreamento e Gerenciamento de Segurança

- **O banco de dados de bugs do Jira** rastreia, categoriza e prioriza vulnerabilidades de segurança.
- **O DefectDojo** consolida os resultados dos testes, garantindo um acompanhamento estruturado das ações de segurança.
- **A aplicação** regular **de patches e correções** mantém uma postura de segurança robusta.

3.4.3 Gerenciamento de Identidade e Acesso (IAM)

- Aplica **o modelo Zero Trust** com **controle de acesso baseado em funções (RBAC) e autenticação multifatorial (MFA)**.
- Utiliza **o Azure AD** para governança de identidades.

- **Alertas de escalonamento de privilégios** detectam acesso administrativo não autorizado.

3.5 Fluxo de Trabalho de Desenvolvimento

O desenvolvimento seguro de software é um aspecto crítico da estratégia de segurança da MyQ. As seguintes medidas garantem a integridade do código, dos pipelines e dos ambientes em nuvem:

3.5.1 Ambiente de desenvolvimento seguro

- Os desenvolvedores da MyQ utilizam **ambientes com segurança reforçada** e proteção de terminais.
- Os desenvolvedores devem seguir **práticas seguras de codificação e participar de treinamentos regulares de segurança**.

3.5.2 Pipelines seguros do GitLab

- Os pipelines de CI/CD do GitLab incluem **verificações de segurança automatizadas, revisões de código e testes**.
- **Os testes estáticos de segurança de aplicativos (SAST)** e **os testes dinâmicos de segurança de aplicativos (DAST)** detectam vulnerabilidades.
- **A assinatura de imagens de contêineres** garante que apenas imagens confiáveis sejam implantadas.

3.5.3 IAM e Controle de Acesso

- Apenas **membros selecionados das equipes de DevOps e SecOps** têm acesso aos ambientes de nuvem do Azure.
- É aplicado **o controle de acesso baseado em funções (RBAC) com elevação de privilégios mínima no momento certo (JIT)**.

3.5.4 Segurança do Azure Kubernetes e de Contêineres

- **Os clusters AKS** da MyQ **obtêm imagens exclusivamente do Azure Container Registry (ACR)**.
- Os ambientes AKS aplicam **políticas de rede e os Padrões de Segurança de Pods (PSS)** para isolar as cargas de trabalho.

3.5.5 Gerenciamento de segredos

- **Todos os segredos e chaves de API são armazenados no Azure Key Vault**, acessível apenas a pessoal autorizado pelo IAM.
- São realizadas **varreduras no sistema de arquivos pelo Trivy** antes do commit no Git para detectar e impedir o vazamento de segredos confidenciais.

3.6 Conclusão

A estratégia de Operações Seguras da MyQ baseia-se no **monitoramento contínuo,** no **gerenciamento proativo de ameaças e** em uma **sólida segurança de infraestrutura**. Ao utilizar **ferramentas avançadas de segurança, controles de acesso rigorosos e testes automatizados**, a MyQ garante um **ambiente de nuvem seguro e resiliente**.

Com a **integração de verificações de segurança TLS, testes de penetração e registro centralizado**, a MyQ aprimora sua capacidade de **detectar, responder e mitigar riscos de segurança** de maneira eficaz.

A segurança é um **desafio em constante evolução**, e a MyQ mantém o compromisso de **aprimorar as medidas de segurança por meio de atualizações regulares, auditorias de conformidade e melhores práticas de segurança**. Ao manter uma **mentalidade que prioriza a segurança**, a MyQ preserva a **integridade e a confidencialidade** de seus serviços, garantindo **confiança e confiabilidade** para todas as partes interessadas.

4 Segurança de Aplicativos

4.1 A evolução das ameaças à segurança

Nos primórdios, antes da popularização da internet, as impressoras eram conectadas diretamente por meio de cabos LPT, e as preocupações com segurança eram mínimas. O maior risco era físico — alguém espiando por cima do ombro do usuário para ver os documentos impressos. O cenário de segurança era simples, e as ameaças cibernéticas eram praticamente inexistentes.

No entanto, à medida que impressoras e dispositivos passaram a se conectar à rede, o panorama de ameaças mudou drasticamente. Com as impressoras agora acessíveis por meio de redes locais (LANs) e até mesmo pela internet, os invasores não precisam mais de acesso físico. Ameaças como ataques do tipo “man-in-the-middle” (MITM), interceptação não autorizada de dados e explorações remotas tornaram-se comuns. Os cibercriminosos evoluíram de espiar por cima do ombro para interceptar o tráfego de rede e explorar vulnerabilidades.

Mitigar esses riscos é um desafio contínuo, já que novas ameaças surgem com frequência. Para lidar com esses desafios de segurança em constante evolução, o MyQ Roger implementa práticas de segurança contínuas, monitoramento proativo e mecanismos de defesa robustos.

4.2 A Abordagem de Segurança do MyQ Roger

O MyQ Roger foi desenvolvido com uma abordagem que prioriza a segurança, garantindo que a inovação e a experiência do usuário estejam sempre alinhadas aos mais altos padrões de segurança. Nosso compromisso com a segurança se reflete em nossos esforços contínuos para integrar medidas de segurança robustas em todas as etapas do desenvolvimento. Adotamos uma filosofia de “segurança por padrão”, incorporando a segurança em nossos produtos e serviços desde o início.

Para alcançar isso, o MyQ Roger utiliza automação, avaliações de risco baseadas em dados e as melhores práticas de segurança da categoria para identificar e mitigar ameaças de forma proativa. Ao implementar controles de segurança no início do ciclo de desenvolvimento, seguindo uma **abordagem “shift-left”**, garantimos que as vulnerabilidades sejam detectadas e corrigidas antes de chegarem à produção. Essa integração proativa nos permite escalar com eficiência, reduzir riscos e minimizar ameaças à segurança. Nossa abordagem reforça nossa dedicação em proteger os dados dos clientes, os fluxos de trabalho e a postura geral de segurança.

4.3 Deslocamento para a Esquerda na Segurança

A abordagem “shift-left” em segurança significa integrar a segurança logo no início do ciclo de vida do desenvolvimento de software (SDLC), em vez de lidar com vulnerabilidades posteriormente. Ao identificar problemas de segurança nos estágios iniciais de desenvolvimento, evitamos correções onerosas e mitigamos possíveis violações. Essa estratégia proativa garante que cada linha de código atenda aos mais altos padrões de segurança antes de chegar à produção, reduzindo riscos e fortalecendo nossa postura geral de segurança.

4.4 Responsabilidades de segurança da MyQ

A MyQ Roger está comprometida em proteger os dados dos clientes e garantir um ambiente operacional seguro. Nossas principais responsabilidades de segurança incluem:

- **Proteção de dados**: a MyQ garante que os dados dos clientes sejam armazenados e criptografados com segurança, impedindo o acesso não autorizado e garantindo a confidencialidade dos dados.
- **Aplicação regular de patches de segurança**: aplicamos proativamente patches e atualizações de segurança em todos os sistemas para eliminar vulnerabilidades antes que possam ser exploradas.
- **Gerenciamento de controle de acesso**: aplicamos políticas rígidas de acesso seguindo o princípio do privilégio mínimo, garantindo que apenas pessoal autorizado possa acessar recursos confidenciais.

Ao respeitar esses princípios de segurança, a MyQ Roger promove uma cultura de segurança, protegendo os usuários contra ameaças potenciais e, ao mesmo tempo, garantindo a conformidade com os padrões do setor.

4.5 Controle/Gerenciamento de Segurança do MyQ Roger

Embora contemos com uma infraestrutura de nuvem segura, o MyQ Roger assume a responsabilidade direta pela implementação de camadas adicionais de segurança e pela adesão às melhores práticas do setor. Nossa abordagem inclui:

- **Gerenciamento de chaves com o Azure Key Vault**: Utilizamos o Azure Key Vault para armazenar e gerenciar todos os segredos, chaves privadas e certificados de forma segura, garantindo controles de acesso rigorosos e criptografia.
- **Certificação ISO 27001**: Seguimos as normas ISO 27001 para manter uma abordagem estruturada e consistente em relação à segurança da informação.

- **Detecção e Resposta em Terminais (EDR)**: Utilizamos soluções avançadas de EDR para detectar, analisar e mitigar ameaças à segurança em tempo real, reduzindo o tempo de resposta e minimizando os riscos.
- **Práticas de desenvolvimento seguro**: Nosso ciclo de vida de desenvolvimento de software seguro inclui avaliações de vulnerabilidades, monitoramento contínuo e varreduras de segurança automatizadas para detectar e corrigir falhas de segurança.
- **Auditorias de segurança regulares**: Realizamos auditorias internas e por terceiros para garantir a conformidade e abordar proativamente os riscos de segurança.
- **SIEM com o Azure Sentinel**: Utilizamos o Azure Sentinel para detecção de ameaças em tempo real, resposta automatizada e monitoramento contínuo de segurança em todos os ambientes de nuvem e de rede.

Ao implementar essas medidas de segurança, o MyQ Roger fortalece sua estrutura geral de segurança, garantindo que os dados dos clientes permaneçam protegidos em todos os momentos.

4.6 Microsoft Azure e conformidade

O MyQ Roger é executado no Microsoft Azure, utilizando o Azure Kubernetes Service (AKS), os servidores SQL do Azure e o Azure Cosmos DB para MongoDB. Ao operar na infraestrutura do Azure, nos beneficiamos dos padrões líderes do setor da Microsoft em segurança, conformidade e confiabilidade.

4.6.1 Responsabilidades da Microsoft em relação à segurança e conformidade

- O Azure segue estruturas globais de conformidade, como a ISO 27001, o SOC 2 e o GDPR na UE, garantindo o cumprimento de rigorosos padrões regulatórios.
- A Microsoft oferece recursos de segurança integrados, como isolamento de rede, proteção de identidade e detecção contínua de ameaças, reduzindo as superfícies de ataque.
- Os serviços do Azure passam por rigorosas avaliações de segurança e testes de penetração para identificar e corrigir proativamente vulnerabilidades.

Ao aproveitar a infraestrutura segura do Azure, o MyQ Roger adiciona suas próprias camadas de segurança para criar um modelo de segurança robusto e resiliente que protege os aplicativos e os dados dos clientes.

4.7 Responsabilidades do cliente em relação à segurança

Embora o MyQ Roger ofereça uma infraestrutura segura e as melhores medidas de segurança da categoria, os clientes também têm responsabilidades fundamentais para garantir a segurança de seu ambiente. Entre elas estão:

- **Manutenção de uma lista de usuários ativos**: os clientes devem gerenciar continuamente o acesso dos usuários, utilizando a sincronização automatizada de usuários ou desativando manualmente contas inativas para minimizar riscos.
- **Aplicação do Controle de Acesso Baseado em Função (RBAC)**: Os clientes devem aplicar os princípios do RBAC para restringir o acesso dos usuários apenas às permissões necessárias, garantindo maior segurança e eficiência operacional.
- **Proteção da rede local**: Embora o MyQ Roger opere com um modelo de confiança zero, os clientes devem garantir que sua rede local siga as melhores práticas de segurança, como configurações de firewall, segmentação de rede e proteção de terminais.
- **Manutenção adequada dos recursos**: Todos os dispositivos conectados, incluindo impressoras e dispositivos multifuncionais (MFPs), devem ser atualizados regularmente com o firmware mais recente e os patches de segurança para evitar vulnerabilidades.

Ao cumprir essas responsabilidades, os clientes fortalecem sua postura de segurança e, ao mesmo tempo, se beneficiam da estrutura de segurança abrangente do MyQ Roger.

4.8 Automação de segurança

Para aprimorar ainda mais a segurança ao longo do ciclo de vida do desenvolvimento, o MyQ Roger integra testes automatizados de segurança e avaliações externas de segurança:

- **SAST (Teste Estático de Segurança de Aplicativos)**: Realizado a cada commit para detectar vulnerabilidades de segurança no início do ciclo de desenvolvimento, reduzindo a probabilidade de que código inseguro chegue à produção.
- **DAST (Teste Dinâmico de Segurança de Aplicações)**: Realizado em ambientes de sandbox para identificar e mitigar riscos de segurança em tempo de execução antes da implantação.
- **Testes de penetração externos**: contratamos especialistas em segurança independentes para realizar testes de penetração, garantindo que nossas defesas de segurança sejam capazes de resistir a cenários de ataque do mundo real.

Ao automatizar os testes de segurança e realizar avaliações externas regulares, o MyQ Roger mantém uma postura de segurança proativa e resiliente.

4.9 Conclusão

Na MyQ Roger, a segurança não é uma preocupação secundária — é parte integrante do nosso produto e do ciclo de vida do desenvolvimento. Ao combinar princípios de "segurança desde o projeto", melhores práticas do setor e uma sólida estrutura de conformidade, oferecemos uma postura de segurança robusta que protege os dados e as operações de nossos clientes. Nosso compromisso com melhorias contínuas de segurança garante que a MyQ Roger permaneça resiliente contra ameaças em constante evolução, mantendo os mais altos padrões de confiabilidade e confiança. Continuaremos a aprimorar nossa estratégia de segurança, adaptando-nos a novos desafios e aproveitando as tecnologias mais recentes para cumprir nossa missão de proporcionar uma experiência de usuário segura e integrada.

5 Proteção de Dados

5.1 Visão geral

A proteção de dados está no centro da abordagem de segurança **do MyQ Roger**, garantindo que todos os aspectos de sua solução de impressão e digitalização baseada em nuvem estejam em conformidade com os mais altos padrões do setor. Um princípio fundamental do MyQ Roger é que **nenhum dado de tarefas de impressão ou digitalização é jamais transferido por meio de seus servidores**. Em vez disso, o MyQ Roger limita estritamente sua coleta de dados a **metadados** essenciais, como **nomes de arquivos de tarefas, tamanhos de arquivos e informações sobre o número de páginas**. Isso garante eficiência operacional ao mesmo tempo em que protege a privacidade do usuário.

5.2 Segurança em nuvem multilocatária

Como um **produto em nuvem multilocatária**, o MyQ Roger oferece aos clientes um ambiente **logicamente isolado** para evitar a exposição de dados entre locatários.

Para garantir resiliência, o MyQ Roger conta com **o Azure SQL** e **o Azure Cosmos DB**, que oferecem recursos de segurança integrados, como **criptografia de dados em repouso e em trânsito, detecção automatizada de ameaças e monitoramento de acesso**. A infraestrutura em nuvem passa por avaliações contínuas de segurança para mitigar os riscos associados a ambientes multilocatários.

5.3 Criptografia e comunicação segura

A segurança está incorporada em todos os níveis das operações do MyQ Roger. Toda a comunicação entre clientes, serviços em nuvem e impressoras é **criptografada usando TLS (Transport Layer Security)** para impedir acesso não autorizado ou adulteração.

Para reforçar ainda mais a segurança, **Autoridades Certificadoras (CAs) publicamente confiáveis** assinam todos os certificados utilizados no MyQ Roger, garantindo o mais alto nível de confiança. Além disso, os certificados são **renovados a cada três meses**, reduzindo o risco de possíveis violações e mantendo a conformidade com as melhores práticas de segurança.

5.4 Conformidade e gerenciamento de identidade

O MyQ Roger está em conformidade com padrões de segurança reconhecidos internacionalmente, possuindo **a certificação ISO 27001**, o que demonstra seu compromisso com a implementação de práticas robustas de gestão da segurança da informação.

Para aplicar controles de acesso rigorosos, é implementado **o Controle de Acesso Baseado em Função (RBAC)**, garantindo que os usuários recebam **apenas as permissões necessárias para sua função**. Isso minimiza a exposição a dados confidenciais e reduz o risco de uso indevido acidental ou intencional.

5.5 Conformidade com o GDPR

Garantir a conformidade com o **Regulamento Geral de Proteção de Dados (GDPR)** é uma prioridade máxima para o MyQ Roger. De acordo com os princípios do GDPR, o MyQ Roger segue medidas rigorosas de proteção de dados para salvaguardar a privacidade do usuário:

- **Minimização de dados**: Somente metadados essenciais são coletados, eliminando o risco de armazenamento de documentos confidenciais dos usuários.
- **Direitos e controle do usuário**: os usuários têm a possibilidade de solicitar **acesso, correção, exclusão ou anonimização** de seus dados pessoais, conforme exigido pelo GDPR.
- **Transparência no processamento de dados**: políticas de privacidade claras e concisas descrevem como os metadados são tratados, armazenados e protegidos.
- **Armazenamento seguro de dados**: Todos os dados são **criptografados tanto em repouso quanto em trânsito**, garantindo total conformidade com os rigorosos requisitos de segurança do GDPR.
- **Medidas de anonimização**: quando necessário, o MyQ Roger implementa **técnicas de anonimização de dados** para garantir que os dados pessoais não possam mais ser atribuídos a um usuário específico, reforçando a proteção da privacidade.

Essas medidas garantem que o MyQ Roger esteja em total conformidade com os principais requisitos do GDPR, dando aos usuários controle sobre seus dados pessoais e, ao mesmo tempo, mantendo um ambiente seguro e em conformidade.

5.6 Backups de dados

Para proteger contra a perda de dados e garantir a confiabilidade do serviço, o MyQ Roger implementa uma **estratégia abrangente de backup de dados**. Isso inclui:

- **Backups automatizados**: **backups incrementais e completos,** agendados regularmente, garantem que os dados permaneçam recuperáveis em caso de incidente.
- **Armazenamento seguro**: os backups são criptografados usando **a criptografia AES-256**, garantindo que, mesmo na improvável eventualidade de acesso não autorizado, os dados permaneçam ilegíveis.
- **Políticas de retenção**: os backups são **armazenados por um período definido**, em conformidade com os requisitos de conformidade, permitindo uma recuperação eficiente em caso de falha do sistema ou em cenários de recuperação de desastres.
- **Testes de integridade e verificação**: **testes** regulares **de integridade dos backups** são realizados para confirmar que os backups armazenados estejam funcionais e confiáveis, garantindo a restauração contínua dos dados quando necessário.

Ao implementar essas medidas robustas de segurança, conformidade e backup, **o MyQ Roger oferece uma solução segura, privada e altamente eficiente de impressão e digitalização baseada na nuvem,** que atende aos mais altos padrões de proteção de dados do setor.

6 Política de Privacidade

Sua privacidade é uma preocupação nossa, e levamos isso muito a sério. Esta Política de Privacidade da MyQ Roger Solution (a “Política de Privacidade”) explica que tipo de informação a MyQ pode coletar, manter e processar em relação ao fornecimento de quaisquer produtos, serviços, conteúdos, aplicativos ou outros componentes que façam parte da MyQ Roger Solution (os “Serviços”), e como essas informações são utilizadas e protegidas. Ela também estabelece como você pode entrar em contato conosco caso tenha alguma dúvida ou preocupação a respeito de seus dados pessoais.

Esta Política de Privacidade é emitida pela MyQ, spol. s.r.o., com sede social no Harfa Business Center, Ceskomoravska 2532/19b, Praga, 19000, República Tcheca, CNPJ nº 615 06 133, registrada no Registro Comercial mantido pelo Tribunal Municipal de Praga, seção C, inserção 29842 (“MyQ” ou “nós”).

Reservamo-nos o direito de fazer alterações nesta Política de Privacidade a qualquer momento. Verifique a Política de Privacidade periodicamente para se manter a par das alterações; no entanto, se você for nosso cliente, também poderemos notificá-lo por e-mail sobre quaisquer alterações que, a nosso exclusivo critério, tenham impacto significativo sobre o uso dos Serviços ou sobre a forma como processamos seus dados pessoais. Seu uso continuado dos nossos Serviços abrangidos por esta Política de Privacidade significará sua aceitação de todas e quaisquer alterações nesta Política de Privacidade feitas por nós periodicamente.

6.1 1. Dados que coletamos ou recebemos

Coletamos dados pessoais de nossos clientes, na qualidade de usuários dos Serviços, e de seus usuários finais (o que inclui funcionários de nossos clientes) com o objetivo de configurar e gerenciar contas de usuário, bem como fornecer e administrar os Serviços. Também coletamos dados de uso e métricas. Somos os controladores desses dados pessoais.

No que diz respeito aos dados pessoais que possam estar incluídos nos metadados do Conteúdo, conforme definido nos Termos de Serviço https://www.myq-solution.com/en/myq-legal-documents, que os usuários ou usuários finais gerenciam por meio dos Serviços, ou no que diz respeito aos dados pessoais aos quais possamos ter acesso ao prestar serviços de suporte remoto ou local (os “Dados do Cliente”), processamos tais dados pessoais em nome de nossos clientes na qualidade de processador de dados. Ao processarmos os Dados do Cliente para prestar os Serviços

aos nossos clientes, agimos de acordo com as instruções de nossos clientes na qualidade de seu processador de dados. Sempre mantemos os Dados do Cliente que processamos em nome de nossos clientes e de acordo com suas instruções separados dos dados de nossos outros clientes e os mantemos estritamente confidenciais.

6.1.1 1.1 Dados de usuários e usuários finais de nossos Serviços

Coletamos seus dados pessoais quando:

- Você cria uma conta em nossos Serviços;
- Você faz login em nosso Serviço, digitando seu nome de usuário (e-mail) e senha;
- Você utiliza nossos Serviços ou interage de alguma outra forma com o MyQ, por exemplo, ao nos enviar quaisquer consultas;
- Você fornece voluntariamente esses dados à MyQ de outra forma.

Ao criar uma conta no MyQ, solicitaremos que você preencha um formulário de cadastro indicando seu nome, sobrenome, e-mail, empresa e cargo. Você também pode optar por adicionar um número de telefone à sua conta.

Também coletamos e processamos seu nome de usuário (e-mail) e senha.

Para fins de análise e aprimoramento de nossos Serviços, nossos servidores podem registrar automaticamente informações quando você visita nosso site ou utiliza alguns de nossos Serviços (“dados de uso”), incluindo:

- Informações sobre serviços de terceiros aos quais o usuário e seus usuários finais se conectam aos Serviços para fins de autenticação e conexão ao armazenamento em nuvem do usuário;
- Informações sobre os dispositivos do usuário, por exemplo, tipo e marca das impressoras e seus números de série;
- Informações sobre o uso de nossos Serviços, por exemplo, a quantidade de documentos impressos ou digitalizados.

Os Serviços permitem que você se conecte a aplicativos de terceiros ou outros serviços, por exemplo, o OneDrive ou o Google Drive, com o objetivo de compartilhar documentos e outros Conteúdos com os Serviços. Caso opte por se conectar a serviços de terceiros, solicitaremos sua permissão para permitir que os Serviços acessem tais serviços de terceiros; no entanto, a MyQ não processará quaisquer dados pessoais armazenados neles, exceto os Dados do Cliente, conforme definido acima.

Caso nossos Serviços sejam adquiridos por uma entidade, são os usuários individuais dentro da organização dessa entidade que fazem login em nossa plataforma de Serviços e cujos dados pessoais são coletados, conforme descrito acima. Quando tal

entidade nos fornecer diretamente quaisquer dados pessoais de seus funcionários ou de outros usuários individuais que tenha autorizado a acessar os Serviços, ela deverá possuir todos os consentimentos, permissões ou registros necessários para processar e nos fornecer os dados pessoais de seus funcionários ou usuários.

6.1.2 1.2 Dados do Cliente

Para prestar nossos Serviços aos nossos usuários e usuários finais, também podemos processar Dados do Cliente, conforme definido acima. O processamento de Dados do Cliente está sujeito à política de privacidade dos usuários, e estes são obrigados a garantir que o processamento desses dados seja lícito e esteja em conformidade com a legislação aplicável. O processamento de Dados do Cliente realizado pela MyQ é regulado pelos contratos de processamento de dados aplicáveis celebrados com os usuários.

6.2 2. Como utilizamos os dados

Utilizamos seus dados pessoais para os seguintes fins:

6.2.1 2.1 Para prestar os Serviços

Podemos processar seus dados pessoais para identificá-lo quando você faz login em sua conta e utiliza nossos Serviços, a fim de nos permitir operar os Serviços e fornecê-los a você. Isso pode incluir a verificação de seus pagamentos, ordens de compra e informações de cobrança.

6.2.2 2.2 Para nos comunicarmos com você

Podemos processar dados de nossos clientes ou de seus usuários finais individuais, em particular e-mails ou outros dados de contato, para nos comunicarmos com nossos usuários e usuários finais, por exemplo, quando os auxiliamos na configuração ou administração de suas contas, quando prestamos atendimento e suporte ao cliente, enviamos avisos técnicos, atualizações sobre mudanças ou melhorias futuras nos Serviços, lembretes, alertas de segurança e outras mensagens de suporte e administrativas.

6.2.3 2.3 Para proporcionar uma melhor experiência do usuário

Podemos processar seus dados pessoais para entender como você utiliza nossos Serviços e, assim, aprimorar continuamente a experiência do usuário, bem como oferecer atendimento ao cliente sem interrupções. Podemos processar esses dados

pessoais também para melhorar e aprimorar nossos Serviços existentes e desenvolver novas ofertas. Isso inclui estatísticas de produtos e de mercado, pesquisas e análises, comparações e outras análises para compreender melhor suas necessidades e as necessidades dos usuários de forma agregada, diagnosticar problemas e analisar tendências.

6.2.4 2.4 Para proteger nossos Serviços e defender nossos direitos ou os de terceiros

Processamos seus dados pessoais para manter o Serviço seguro, protegido e confiável. Isso inclui detectar, prevenir e responder a fraudes, abusos, riscos de segurança e problemas técnicos que possam prejudicar a MyQ, nossos clientes e usuários finais.

Podemos processar alguns dos dados especificados na Seção 1.1 quando exigido por lei ou para estabelecer, exercer ou defender nossas reivindicações legais ou, quando necessário, proteger os direitos e interesses da MyQ.

6.2.5 2.5 Para fins de marketing e vendas

Podemos processar os dados de contato das pessoas de contato designadas por você ou por seus usuários finais, a fim de fornecer a você informações relacionadas a novos recursos dos Serviços e novas ofertas de produtos. Para mais detalhes, consulte a Seção 7 abaixo.

6.3 3. Base legal

Para os fins especificados nas Seções 2.1 e 2.2, processamos seus dados pessoais com base em nosso contrato com você (caso você seja nosso cliente direto e uma pessoa física) ou com base em nosso interesse legítimo em fornecer nossos Serviços aos nossos clientes (quando nosso cliente for sua empresa ou organização e você for um usuário final autorizado designado por sua empresa ou organização).

Para os fins especificados na Seção 2.3, processamos seus dados pessoais com base em nosso interesse legítimo em desenvolver e aprimorar nossos Serviços.

Para os fins especificados na Seção 2.4, processamos seus dados pessoais com base em nosso interesse legítimo em proteger e garantir nossos direitos ou reivindicações, ou os direitos de nossos clientes ou usuários.

Para os fins especificados na Seção 2.5, processamos seus dados pessoais com base no seu consentimento voluntário, caso você tenha nos concedido tal consentimento.

Em um escopo limitado permitido pela legislação aplicável, também podemos utilizar seus dados de contato eletrônicos para informá-lo sobre nossos Serviços sem o seu consentimento explícito, com base em nosso interesse legítimo, conforme descrito em mais detalhes na Seção 7 abaixo.

Quando utilizamos seus dados pessoais para nossos interesses legítimos, garantimos que levamos em consideração qualquer impacto potencial que tal uso possa ter sobre você. Nossos interesses legítimos não se sobrepõem automaticamente aos seus, e não utilizaremos suas informações se acreditarmos que seus interesses devam se sobrepor aos nossos, a menos que tenhamos outros fundamentos para fazê-lo (como o cumprimento de contrato, seu consentimento ou uma obrigação legal). Caso tenha alguma dúvida sobre nosso tratamento de dados, consulte os detalhes sobre “Seus direitos” na Seção 9 abaixo.

6.4 4. Períodos de retenção

Quando processamos dados pessoais na qualidade de controlador de dados, retemos seus dados pessoais pelo período necessário para cumprir as finalidades descritas nesta Política de Privacidade e/ou em qualquer contrato de Serviços, a menos que uma retenção mais longa seja exigida por lei (por exemplo, para fins fiscais ou contábeis ou devido a outros requisitos legais) ou que o armazenamento dos dados seja necessário para o estabelecimento, exercício ou defesa de reivindicações legais da MyQ; nesse caso, armazenaremos apenas os dados necessários para a execução de nossas reivindicações ou para nossa defesa pelo período necessário no caso em questão, sem exceder os prazos de prescrição previstos em lei.

Quando processamos dados pessoais em nome de nossos clientes na qualidade de processador de dados, retemos tais dados durante a vigência do nosso contrato com esses clientes e os excluímos automaticamente, de acordo com nossos processos de retenção e backup, no prazo de 90 dias após o término do contrato, a menos que os clientes nos solicitem que os apaguemos antes.

6.5 5. Compartilhamento de seus dados pessoais para fins legais e comerciais

Podemos utilizar e/ou divulgar a terceiros (incluindo órgãos governamentais e autoridades de aplicação da lei, nossas afiliadas, consultores profissionais e nossos fornecedores ou subcontratados) informações sobre você quando:

- Cumprirmos um processo legal;

- Para fazer valer ou defender os direitos legais da MyQ, e em conexão com uma reestruturação corporativa, como fusão, aquisição de negócios ou situações de insolvência;
- Prevenir fraudes ou danos iminentes; e
- Para garantir a segurança e a operacionalidade de nossa rede e de nossos serviços.

Essas informações serão compartilhadas desde que, em todas essas circunstâncias, compartilhemos apenas as informações pessoais limitadas que forem necessárias para a situação específica.

Compartilhamos seus dados com nossos parceiros comerciais de confiança ou com pessoas físicas que tratam seus dados como nossos subcontratados, em nosso nome e de acordo com nossas instruções, em conformidade com esta Política de Privacidade. Selecionamos nossos fornecedores com muito cuidado e sempre garantimos que eles ofereçam proteção de dados e medidas de segurança adequadas. Para esse fim, vinculamos nossos processadores de dados a contratos de tratamento de dados celebrados nos termos do Artigo 28 do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas físicas no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, e que revoga a Diretiva 95/46/CE (Regulamento Geral de Proteção de Dados) (“RGPD”).

Se você selecionar, na interface de administração do MyQ, que seu locatário de Serviços esteja localizado na UE, seus Dados do Cliente serão tratados na UE, de acordo com os compromissos contratuais da Microsoft relativos ao Limite de Dados da UE. Se você selecionar na interface de administração do MyQ que seu locatário dos Serviços esteja localizado fora da UE, tal transferência será realizada com base nas Cláusulas Contratuais Padrão (cláusulas-modelo) aprovadas pela Comissão Europeia (2010/87/UE), a menos que um mecanismo de transferência diferente, nos termos dos artigos 45, 46 e seguintes do RGPD, venha a estar disponível. Não obstante o acima exposto, seus Dados do Cliente também poderão ser transferidos para países para os quais a Comissão Europeia tenha emitido uma decisão de adequação.

A lista de nossos processadores atuais que podem ter acesso aos seus dados pessoais:

- http://salesforce.comEMEA Ltd. (processamento relacionado a vendas e suporte técnico),
- Microsoft Ireland Operations Limited (colaboração e comunicação, Microsoft Azure – serviços de hospedagem em nuvem),

- TeamViewer GmbH (suporte técnico).

Além dos processadores mencionados acima, também podemos compartilhar seus dados pessoais para gerenciar nossos processos comerciais e cumprir nossas obrigações legais, incluindo serviços logísticos, de faturamento, tributários, jurídicos e técnicos.

Além de fornecedores terceirizados, a MyQ pode compartilhar dados com suas afiliadas localizadas na UE e no Reino Unido para fins de determinados serviços logísticos, de faturamento, tributários, jurídicos e técnicos. A lista atualizada de nossas afiliadas na UE e no Reino Unido está disponível em https://www.myq-solution.com/en/the-list-of-myq-data-processors .

6.6 6. Estatísticas anônimas

Podemos utilizar dados agregados e anônimos derivados dos dados pessoais fornecidos por você ou coletados por análises do programa, tais como comportamento e atividades do usuário, para nossas próprias estatísticas, para auditoria, para fins de pesquisa de produtos e de mercado, para análises (que nos ajudam a otimizar e melhorar nossos Serviços e sua usabilidade, a gama de Serviços e a desenvolver novas tecnologias, produtos e serviços) e para comparações e outras análises.

6.7 7. Comunicações de marketing

Podemos entrar em contato com as pessoas de contato designadas por você ou por seus usuários finais para fornecer informações relacionadas a novos recursos dos Serviços e novas ofertas de produtos, desde que tenhamos a permissão necessária para fazê-lo, seja com base no seu consentimento (quando o tivermos solicitado e você o tiver nos fornecido), seja com base em nossos interesses legítimos de lhe enviar comunicações de marketing, nos casos em que for legalmente permitido, dentro dos limites previstos em lei. Neste último caso, só lhe enviaremos comunicações de marketing se você estiver utilizando ou tiver utilizado recentemente qualquer um de nossos Serviços e não tiver se oposto ao recebimento dessas informações (por qualquer meio mencionado abaixo).

Suas preferências de comunicação de marketing podem ser alteradas a qualquer momento, seguindo as instruções abaixo:

- Caso deseje cancelar a assinatura de um e-mail que lhe foi enviado, siga o link “cancelar assinatura” e/ou as instruções localizadas na parte inferior do e-mail.

- Como alternativa, você pode entrar em contato conosco usando os dados na seção “Fale conosco” abaixo para alterar suas preferências de comunicação de marketing, incluindo a revogação do seu consentimento.

Caso tenha recebido e-mails indesejados e não solicitados enviados por meio de nosso sistema ou que aleguem ter sido enviados por meio de nosso sistema, encaminhe uma cópia desse e-mail com seus comentários para info@myq-solution.com[1] para análise.

Observe que, ocasionalmente, podemos enviar a você informações importantes (inclusive por e-mail) sobre nossos Serviços que você está utilizando ou já utilizou, incluindo alterações nos termos e condições aplicáveis e/ou outras comunicações ou notificações que possam ser necessárias para cumprir nossas obrigações legais e contratuais, conforme descrito na Seção 2.2 acima. Essas comunicações importantes sobre os Serviços não constituem comunicações de marketing e não são afetadas por suas preferências.

6.8 8. Segurança e localização de seus dados

Implementamos e manteremos medidas técnicas e organizacionais adequadas, controles internos e rotinas de segurança da informação, de acordo com as boas práticas do setor, levando em consideração o estado do desenvolvimento tecnológico, a fim de proteger seus dados contra perda acidental, destruição, alteração, divulgação ou acesso não autorizado ou destruição ilegal. Tais medidas podem incluir, sem limitação, a adoção de medidas razoáveis para garantir a confiabilidade dos funcionários que têm acesso aos seus dados e o estabelecimento de direitos de acesso limitados e controles de acesso; autenticação; treinamento de pessoal; backup regular; procedimentos de recuperação de dados e gerenciamento de incidentes; restrições ao armazenamento, impressão e descarte de dados pessoais; proteção por software dos dispositivos nos quais os dados pessoais são armazenados; etc.

6.9 9. Seus direitos

Esta Seção descreve seus direitos nos termos das leis aplicáveis, como o GDPR, e como exercê-los. Caso você exerça qualquer um de seus direitos nos termos desta Seção ou das leis aplicáveis, comunicaremos qualquer retificação ou apagamento de seus dados pessoais, ou restrição ao tratamento, realizada de acordo com sua solicitação a cada destinatário a quem os dados pessoais tenham sido divulgados, nos

1. mailto:info@myq-solution.com

termos da Seção 5 desta Política de Privacidade, a menos que tal comunicação se mostre impossível ou envolva esforço desproporcional.

Caso deseje exercer esses direitos e/ou obter todas as informações relevantes sobre o tratamento de seus dados pessoais, entre em contato conosco pelo e-mail info@myq-solution.com[2]. Será solicitado que você se identifique; isso é necessário para verificar se a solicitação foi enviada por você. Responderemos no prazo de 1 mês após o recebimento de sua solicitação, mas nos reservamos o direito de prorrogar esse prazo para até 2 meses em circunstâncias excepcionais e justificadas. Em qualquer caso, informaremos você no prazo de 1 mês após o recebimento de sua solicitação caso decidamos prorrogar o prazo para nossa resposta.

De acordo com as leis aplicáveis e conforme descrito mais detalhadamente abaixo, você tem o direito de solicitar acesso aos seus dados pessoais e informações sobre seu tratamento, o direito à retificação, ao apagamento ou à portabilidade (por exemplo, transferência de seus dados pessoais para outro prestador de serviços) dos seus dados pessoais que tratamos, bem como o direito de se opor ao tratamento de seus dados pessoais e/ou solicitar a restrição de tal tratamento.

Observe que sua objeção ao tratamento pode significar que não seremos capazes de lhe fornecer nossos Serviços ou de realizar as ações necessárias para atingir as finalidades estabelecidas acima (consulte a Seção 2 “Como usamos os dados”).

É importante que os dados pessoais que mantemos sobre você estejam corretos e atualizados. Por favor, mantenha-nos informados caso seus dados pessoais sejam alterados durante o seu relacionamento conosco, entrando em contato conosco por meio dos dados de contato na Seção 10 “Fale conosco”.

6.9.1 9.1 Informações sobre, acesso a e retificação de seus dados pessoais

De acordo com as leis aplicáveis, você tem o direito de obter confirmação sobre se os dados pessoais a seu respeito estão ou não sendo tratados (conforme o processo descrito acima) e, caso estejam, o direito de acessar e retificar os dados pessoais que você compartilhou conosco. Por meio das configurações dos Serviços, você pode acessar e atualizar as informações da sua conta, bem como alterar as configurações do seu perfil.

2. mailto:info@myq-solution.com

6.9.2 9.2 Exatidão dos seus dados pessoais

Tomamos medidas razoáveis para garantir que você possa manter seus dados pessoais precisos e atualizados. Você pode sempre entrar em contato conosco para obter confirmação sobre se ainda processamos ou não seus dados pessoais.

Caso você constate que seus dados pessoais tratados por nós estão imprecisos ou incompletos e não consiga atualizá-los de acordo com a Seção 9.1 desta Política de Privacidade, você poderá solicitar que atualizemos tais dados. Verificaremos sua identidade e atualizaremos seus dados pessoais em seu nome.

6.9.3 9.3 Exclusão de seus dados pessoais

Você pode nos solicitar o apagamento de seus dados pessoais a qualquer momento. Caso nos encaminhe tal solicitação, excluiremos todos os seus dados pessoais em nosso poder sem demora injustificada, desde que esses dados não sejam mais necessários para a prestação dos Serviços ou para outras finalidades permitidas, em particular no que se refere ao exercício e à defesa de nossos direitos legais, ou ao cumprimento de nossas obrigações legais. Também excluiremos (e garantiremos a exclusão pelos subcontratados que contratamos) todos os seus dados pessoais caso você retire seu consentimento ou nas circunstâncias em que a lei nos obrigue a fazê-lo.

6.9.4 9.4 Restrição do tratamento

Caso você nos solicite a restrição do tratamento de seus dados pessoais, por exemplo, em circunstâncias em que você conteste a exatidão, a legalidade ou a necessidade de tratarmos seus dados pessoais, limitaremos o tratamento de seus dados pessoais ao mínimo necessário (armazenamento) e, se aplicável, os trataremos apenas para o estabelecimento, exercício ou defesa de ações judiciais ou, quando necessário, para a proteção dos direitos de outra pessoa física ou jurídica, ou por outros motivos limitados determinados pela legislação aplicável. Caso a restrição seja suspensa e continuemos a tratar seus dados pessoais, você será informado sobre isso sem demora injustificada.

6.9.5 9.5 Portabilidade dos seus dados pessoais

Você tem o direito de receber os dados pessoais a você relativos e que você nos forneceu. Caso nos apresente tal solicitação, forneceremos seus dados pessoais em formato comumente utilizado e legível por máquina, sem demora indevida a partir do recebimento de sua solicitação. Se você assim o solicitar, enviaremos seus dados

pessoais a um terceiro (outro controlador de dados) que você identificar em sua solicitação, a menos que tal solicitação afete adversamente os direitos ou liberdades de terceiros e desde que seja tecnicamente viável.

6.9.6 9.6 Oposição ao tratamento

Você tem o direito de se opor ao uso de seus dados pessoais com base em nossos interesses legítimos. Nesse caso, não processaremos mais seus dados pessoais, a menos que demonstremos motivos legítimos e imperiosos para o processamento posterior que se sobreponham aos seus interesses, direitos e liberdades, ou para o estabelecimento, exercício ou defesa de nossas reivindicações legais. Se você se opuser ao processamento de seus dados para fins de marketing direto, deixaremos de processar seus dados para esses fins.

6.9.7 9.7 Revogação do consentimento

Caso tenha nos concedido consentimento para o tratamento de dados pessoais, por exemplo, para comunicações de marketing, você pode revogar esse consentimento a qualquer momento, sem necessidade de justificativa. Bloquearemos seus dados pessoais para qualquer tratamento posterior. Observe que a revogação do seu consentimento não afeta a legalidade de qualquer tratamento realizado com base no consentimento antes de sua revogação.

6.9.8 9.8 Reclamação junto a uma autoridade de proteção de dados

Você tem o direito de apresentar uma reclamação relativa às nossas atividades de tratamento de dados ao Úřad pro ochranu osobních údajů, endereço: Pplk. Sochora 2Z, 170 00 Praha 7, República Tcheca.

6.9.9 9.9 Solicitação de exclusão da venda de dados pessoais nos termos da CCPA

A MyQ não vende, conforme definido na CCPA, quaisquer dados pessoais. Portanto, se um consumidor da Califórnia comunicar um pedido de exclusão nos termos desta disposição, tal pedido não terá efeito. Caso necessite de informações adicionais sobre seus direitos nos termos da CCPA para se recusar à venda de seus dados pessoais, entre em contato com: info@myq-solution.com[3].

3. mailto:info@myq-solution.com

6.10 10. Entre em contato conosco

Caso tenha alguma dúvida sobre nossas práticas de coleta e proteção de dados ou sobre seus direitos, não hesite em entrar em contato conosco pelo e-mail info@myq-solution.com.

7 Tempo de atividade do servidor, backup de dados e recuperação de desastres

7.1 Tempo de atividade do servidor

A MyQ Roger se dedica a manter uma meta de tempo de atividade de 99,9%; no entanto, os acordos de nível de serviço (SLAs) são personalizados para cada cliente e não garantem explicitamente essa métrica. Empregamos estratégias avançadas de alta disponibilidade (HA), aproveitando implantações em múltiplas zonas e arquiteturas com múltiplos pods para garantir a continuidade do serviço e minimizar possíveis períodos de inatividade em caso de interrupções operacionais.

7.2 Monitoramento do status do sistema em tempo real

Para aumentar a transparência e fornecer visibilidade em tempo real do desempenho do sistema, mantemos um site dedicado ao status que oferece informações atualizadas sobre a integridade do serviço. Essa plataforma permite que os clientes:

- **Monitorar o status do sistema ao vivo**: visualizar métricas operacionais em tempo real e atualizações sobre incidentes.
- **Receber notificações proativas**: Inscrever-se para receber alertas sobre degradação do serviço ou eventos de manutenção planejada.
- **Acessar relatórios históricos de tempo de atividade**: analisar incidentes passados e tendências de desempenho para avaliar a confiabilidade.

Ao oferecer um site centralizado de status, fornecemos aos clientes informações oportunas e precisas, reforçando a confiança e possibilitando a tomada de decisões proativas em caso de interrupções.

7.3 Estratégias de backup

7.3.1 Estratégia de backup do Azure SQL

Empregamos uma estratégia de backup georedundante para bancos de dados do Azure SQL, garantindo resiliência e capacidade de recuperação dos dados. Os principais aspectos incluem:

- **Armazenamento georedundante**: os backups são replicados em várias regiões para recuperação de desastres.
- **Política de retenção**: os backups são retidos por vários meses, permitindo a recuperação de dados históricos.

- **Backups incrementais**: uma janela de 14 dias para recuperação em um momento específico (PITR) permite a restauração granular de dados perdidos.
- **Personalização com base no SLA**: os períodos de retenção e os objetivos de tempo de recuperação (RTO) variam de acordo com os SLAs específicos do cluster e podem ser adaptados para atender às necessidades do cliente.

7.3.2 Estratégia de backup do Azure Cosmos DB

Para o Azure Cosmos DB, implementamos mecanismos abrangentes de proteção de dados, especialmente para registros contábeis, garantindo a integridade e a rastreabilidade dos dados:

- **Relatórios completos de dados contábeis**: Todas as transações contábeis, incluindo a contabilidade de tarefas para atividades de impressão, digitalização, cópia e fax, são totalmente registradas.
- **Rastreamento de dados históricos**: nosso sistema permite o acompanhamento e o rastreamento de quaisquer registros contábeis relatados para garantir a conformidade e a auditabilidade.
- **Alta disponibilidade e redundância**: a replicação multirregional integrada garante a continuidade e minimiza os riscos de perda de dados.

Ao implementar essas estratégias robustas de backup, protegemos os dados críticos da empresa e, ao mesmo tempo, oferecemos opções flexíveis de recuperação adaptadas aos SLAs específicos de cada cliente.

7.4 Cenários de desastre e plano de resposta

Cenário de desastre	Estratégia de Mitigação	Processo de recuperação
Corrupção de dados	PITR (Recuperação em um Momento Específico)	Restaurar o banco de dados para o último estado válido conhecido
Interrupção na região da nuvem	Backups geo-redundantes e failover	Mudança para a região secundária do Azure
Falha no nó do Kubernetes	Replicação automática de serviços no AKS	Os pods são reescalonados para nós em bom estado
Ataque cibernético (DDoS, ransomware etc.)	WAF, Proteção contra DDoS do Azure e monitoramento de segurança	Isolar sistemas comprometidos e restaurá-los a partir de backups não comprometidos

8 Zero Trust

8.1 Entendendo a Segurança Zero Trust

A confiança é um conceito complexo. Por exemplo, confio que minha mãe prepare um jantar perfeito, mas nunca confiaria nela quando se trata de segurança de rede. Na segurança cibernética, a confiança mal depositada pode levar a vulnerabilidades significativas, e é por isso que existe o modelo Zero Trust.

8.1.1 Exemplo do mundo real: o perigo da confiança implícita

Uma das violações mais conhecidas em que a falta dos princípios do Zero Trust teve um papel importante foi o **ataque à Colonial Pipeline** em 2021. Os invasores obtiveram acesso por meio de uma credencial de VPN comprometida, que não tinha a autenticação multifatorial (MFA) habilitada. Como a rede confiava implicitamente nos usuários autenticados, os invasores conseguiram se mover lateralmente e implantar ransomware, causando escassez generalizada de combustível em todos os EUA. Esse incidente destaca por que “nunca confie, sempre verifique” é fundamental para a cibersegurança moderna.

8.2 O que é Zero Trust?

O Zero Trust é um paradigma de segurança cibernética baseado no princípio de “nunca confie, sempre verifique”. Ele garante que usuários e dispositivos não sejam considerados confiáveis por padrão, mesmo que estejam conectados a uma rede corporativa segura ou tenham sido verificados anteriormente. Em vez disso, a confiança deve ser continuamente avaliada e validada com base em vários sinais de segurança.

8.2.1 Os princípios fundamentais do Zero Trust

O Zero Trust é definido na norma **NIST SP** como**800-207** uma estrutura focada na proteção de recursos por meio da verificação contínua. Esse modelo de segurança se aplica a:

- **Gerenciamento de Identidade e Acesso**: Garantir que usuários e dispositivos sejam autenticados com segurança.
- **Segurança de rede e de terminais**: proteger a comunicação e aplicar controles de acesso rigorosos.
- **Proteção de dados**: garantir que dados confidenciais sejam criptografados e armazenados com segurança.

- **Monitoramento contínuo**: Detectar anomalias e responder a possíveis ameaças em tempo real.

8.3 Como o Zero Trust se aplica ao MyQ Roger

8.3.1 Verificação explícita

- A autenticação é exigida mesmo em dispositivos autorizados (celulares/computadores).
- Utiliza padrões modernos de autenticação.
- A autenticação multifatorial (MFA) é obrigatória para logins em dispositivos móveis e impressoras multifuncionais (MFP).
- O fluxo de dispositivos OAuth2 é implementado para a autorização de dispositivos.
- **Mecanismos de autenticação contínua** monitoram mudanças no comportamento do usuário para detectar anomalias.

8.3.2 Gerenciamento de Acesso

- **O Controle de Acesso Baseado em Função (RBAC)** garante que os usuários tenham apenas o acesso mínimo necessário.
- **O Princípio do Privilégio Mínimo** é aplicado para reduzir riscos de segurança.
- **A microsegmentação** é implementada para limitar a movimentação lateral dentro da rede.
- **Os controles de acesso Just-in-Time (JIT)** ajustam dinamicamente os privilégios do usuário com base no contexto.

8.3.3 Segurança de dispositivos e terminais

- São emitidos tokens de acesso exclusivos para cada tipo de dispositivo.
- A Segurança da Camada de Transporte (TLS) é obrigatória para todas as comunicações.
- **Soluções de Detecção e Resposta em Terminais (EDR)** monitoram e analisam o comportamento dos dispositivos.
- **O Acesso à Rede Zero Trust (ZTNA)** garante que apenas dispositivos autorizados possam acessar recursos específicos.

8.3.4 Proteção de dados

- Todos os dados são armazenados com segurança por meio de soluções de armazenamento criptografado.
- As políticas garantem que os dados sejam acessados apenas por entidades autorizadas.

- **As soluções de Prevenção contra Perda de Dados (DLP)** monitoram e impedem a exfiltração não autorizada de dados.
- **Enclaves seguros** protegem dados altamente confidenciais contra acesso não autorizado.

8.4 Combate às ameaças cibernéticas com o Zero Trust

O modelo Zero Trust ajuda a mitigar as seguintes ameaças:

- **Ameaças internas**: impede que funcionários ou contas comprometidas obtenham acesso não autorizado.
- **Ataques de preenchimento de credenciais e phishing**: reduz o impacto de credenciais comprometidas por meio da autenticação contínua.
- **Ataques de movimentação lateral**: a microsegmentação impede que invasores se movimentem lateralmente pelas redes.
- **Ataques à cadeia de suprimentos**: garante a verificação rigorosa do acesso e das integrações de terceiros.

8.5 Considerações sobre conformidade e regulamentação

O modelo Zero Trust está alinhado com diversas regulamentações e estruturas de segurança cibernética:

- **ISO 27001**: impõe o gerenciamento seguro de acesso e a proteção de dados.
- **GDPR**: Garante o processamento e o armazenamento seguros de dados pessoais.
- **HIPAA**: protege informações confidenciais da área da saúde.
- **Estrutura de Cibersegurança do NIST**: fornece diretrizes para a implementação do Zero Trust.

8.6 Por que o Zero Trust é importante

A adoção do Zero Trust minimiza o risco de violações de segurança, ameaças internas e acesso não autorizado. Em uma era de crescentes ameaças cibernéticas, uma arquitetura Zero Trust oferece proteção robusta, garantindo verificação contínua e controles de acesso rigorosos em todos os recursos.

Ao implementar esses princípios, o MyQ Roger garante uma postura de segurança segura, resiliente e adaptável, alinhada às melhores práticas modernas de cibersegurança. Além disso, o monitoramento contínuo, os controles de acesso e a detecção de ameaças em tempo real aprimoram a capacidade da organização de responder de forma eficaz às ameaças cibernéticas em constante evolução.

9 Login seguro com o MyQ Roger

9.1 Introdução

Usar um PIN como método principal de login nunca foi realmente seguro. Os primeiros celulares dependiam de PINs, mas, à medida que as preocupações com segurança evoluíram, o mesmo ocorreu com os métodos de autenticação. Hoje, a biometria se tornou a norma, oferecendo uma abordagem mais segura e fácil de usar para a autenticação.

O MyQ Roger adota essa mudança ao implementar a mais recente concessão de autorização de dispositivo OAuth 2.0 (anteriormente conhecida como Device Flow). Esse método moderno de autenticação exige que os usuários façam login usando um código QR de uso único, escaneado com seu celular, eliminando a necessidade de senhas estáticas ou PINs inseguros.

Reconhecemos o celular do usuário como um dos meios mais seguros de autenticação. Ao utilizar a autenticação biométrica para desbloquear o celular e, posteriormente, acessar o aplicativo MyQ, garantimos que a pessoa que está fazendo login seja o proprietário legítimo da conta.

9.2 Autenticação segura com o MyQ Roger

- **Autorização de Dispositivo OAuth 2.0**: Em vez de depender de PINs tradicionais, os usuários se autenticam usando um código QR gerado dinamicamente. Esse método reduz significativamente o risco de roubo de credenciais ou ataques de reutilização.
- **Verificação biométrica**: como os smartphones modernos exigem verificação biométrica (por exemplo, impressão digital ou reconhecimento facial) para serem desbloqueados, isso adiciona uma camada extra de segurança antes do acesso ao MyQ Roger.

9.3 Autenticação por PIN tradicional

Embora o MyQ Roger ainda ofereça o login por PIN como opção, esse método é considerado inseguro e não é recomendado por padrão. Os usuários que optarem por ativar a autenticação por PIN devem marcá-la explicitamente como segura, reconhecendo os riscos de segurança associados. Além disso, ativar o login por PIN desativará alguns recursos avançados de segurança para mitigar possíveis vulnerabilidades.

9.4 Responsabilidade pela segurança

Se uma organização optar por permitir o login por PIN, a responsabilidade pela manutenção de um ambiente seguro recai sobre o cliente. Práticas recomendadas, como a aplicação de políticas rigorosas de PIN, a implementação de medidas de segurança física e o monitoramento de registros de acesso, devem ser seguidas para minimizar os riscos.

9.5 Conclusão

Com o MyQ Roger, priorizamos a segurança ao adotar padrões modernos de autenticação. A adoção da autenticação biométrica por dispositivos móveis garante uma experiência do usuário integrada e segura. Embora o login tradicional por PIN continue disponível, ele não é o método recomendado, e os clientes devem tomar precauções adicionais caso optem por usá-lo. Ao adotar mecanismos de login seguros, as organizações podem aprimorar tanto a segurança quanto a usabilidade para seus usuários.

10 Impressão segura com o MyQ Roger

10.1 O desafio da impressão segura

Os métodos tradicionais de impressão segura dependem de conexões fisicamente ligadas, como cabos LPT, nos quais uma impressora dedicada é atribuída a um único laptop. Embora esse método garanta o mais alto nível de segurança, ele é impraticável em ambientes modernos que exigem flexibilidade, mobilidade e recursos compartilhados.

O AirPrint e o Mopria oferecem recursos de impressão segura, mas são insuficientes em cenários em que os usuários podem iniciar trabalhos de impressão remotos sem estar fisicamente presentes perto da impressora. Isso cria vulnerabilidades de segurança, nas quais documentos confidenciais podem ser deixados sem supervisão.

10.2 MyQ Roger: uma solução abrangente de impressão segura

O MyQ Roger integra múltiplos fluxos de trabalho de impressão ao mesmo tempo em que aplica protocolos de segurança para garantir que os usuários estejam fisicamente presentes para autenticar e liberar trabalhos de impressão. O sistema garante que os trabalhos de impressão sejam armazenados e transmitidos com segurança, minimizando a exposição de dados.

10.3 Métodos de impressão segura no MyQ Roger

10.3.1 Impressão direta do PC para a impressora

- Utiliza **o IPP/s (Internet Printing Protocol Secure)** para transferir trabalhos de impressão com segurança.
- Marcas de impressoras compatíveis: **Ricoh, Kyocera**.
- Os trabalhos de impressão permanecem armazenados diretamente na impressora até que o usuário se autentique e libere o trabalho.

10.3.2 MyQ Roger Client (MRC)

- Os trabalhos de impressão são **criptografados e armazenados localmente** no PC do usuário.
- A impressora recupera o arquivo criptografado **somente após a autenticação do usuário**.
- A impressão segura é executada via **IPP/s**.

10.3.3 Impressão na nuvem

- Os arquivos de impressão são armazenados com segurança no armazenamento em nuvem do usuário (por exemplo, **OneDrive, Google Drive, Dropbox**).
- A impressora baixa o documento diretamente do armazenamento em nuvem usando um **link de acesso de curta duração**.
- **Não há retenção de documentos** na impressora após a impressão, garantindo a confidencialidade dos dados.

10.3.4 Integração com o Microsoft Universal Print

- O MyQ Roger implementa um **Universal Print Connector** que permite que as impressoras se comuniquem diretamente com **os servidores do Universal Print da Microsoft**.
- Os trabalhos de impressão são armazenados com segurança nos **servidores da Microsoft** e recuperados sob demanda após a autenticação do usuário.
- A impressão é realizada por meio de **drivers do Universal Print**, garantindo um processamento de tarefas contínuo e seguro.

10.4 Conclusão

O MyQ Roger oferece um **ambiente de impressão abrangente e seguro**, combinando fluxos de trabalho de impressão diretos, locais e baseados na nuvem com medidas de segurança robustas. Ao exigir que os usuários se autentiquem pessoalmente antes da execução do trabalho, o MyQ Roger elimina os riscos associados a trabalhos de impressão sem supervisão, garantindo proteção máxima dos dados em ambientes de trabalho modernos.

11 Contatos comerciais

Fabricante do MyQ®	**MyQ® spol. s r.o.** Harfa Business Center, Ceskomoravska 2532/19b, 190 00 Praga 9, República Tcheca N.º de identificação 615 06 133 A MyQ® spol. s r.o. está registrada no Registro Comercial do Tribunal Municipal de Praga, sob o n.º de processo C 29842 (doravante denominada “MyQ®”)
Informações comerciais	http://www.myq-solution.com info@myq-solution.com[4]
Suporte técnico	support@myq-solution.com[5]
Aviso	O FABRICANTE NÃO SE RESPONSABILIZA POR QUALQUER PERDA OU DANO CAUSADO PELA INSTALAÇÃO OU OPERAÇÃO DO SOFTWARE E DAS PEÇAS DE HARDWARE DA SOLUÇÃO DE IMPRESSÃO MyQ®. Este manual, seu conteúdo, design e estrutura são protegidos por direitos autorais. É proibida e pode ser punível a cópia ou qualquer outra forma de reprodução total ou parcial deste guia, ou de qualquer material protegido por direitos autorais, sem o consentimento prévio por escrito da MyQ®. A MyQ® não se responsabiliza pelo conteúdo deste manual, especialmente no que diz respeito à sua integridade, atualidade e adequação comercial. Todo o material aqui publicado tem caráter exclusivamente informativo. Este manual está sujeito a alterações sem aviso prévio. A MyQ® não é obrigada a realizar essas alterações periodicamente nem a anunciá-las, e não se responsabiliza pela compatibilidade das informações atualmente publicadas com a versão mais recente da solução de impressão MyQ®.

4. mailto:info@myq-solution.com
5. mailto:support@myq-solution.com

Marcas registradas	“MyQ®”, incluindo seus logotipos, é uma marca registrada da MyQ®. É proibido qualquer uso das marcas registradas da MyQ®, incluindo seus logotipos, sem o consentimento prévio por escrito da empresa MyQ®. A marca registrada e o nome do produto são protegidos pela MyQ® e/ou suas afiliadas locais.

myQ roger

POUPE TEMPO COM SOLUÇÕES DE IMPRESSÃO PERSONALIZADAS

MyQ Roger é uma solução cloud-native criada para escritórios modernos cloud-first, simplificando os fluxos de trabalho documentais e permitindo navegação, impressão e digitalização seguras, onde quer que os utilizadores estejam.

info@myq-solution.com

myq-solution.com

50+ milhões
Utilizadores que confiam na MyQ

1+ milhão
Dispositivos ativos

26+
Marcas suportadas

1000+
Parceiros certificados

Presente em 140+ países

Prémios e certificações

BuyersLab PLATINUM TESTED SOLUTION 2023

BuyersLab PLATINUM TESTED SOLUTION 2022

BuyersLab PLATINUM TESTED SOLUTION 2021

ISO 9001 TÜV SÜD ISO 14001 ISO/IEC 27001