
# Informe sobre la seguridad de los datos de MyQ Roger 2.x

Generado a partir de docs.myq-solution.com
agosto/2026


ESPAÑOL

**Aviso sobre la traducción**

Esta traducción se creó con la ayuda de inteligencia artificial. En caso de discrepancia o ambigüedad, prevalecerá el documento original en inglés.

# Tabla de contenido

# 1 Introducción

El objetivo de este documento es informar a los clientes de MyQ Roger sobre los procesos que implican el establecimiento de conexiones en el sistema y sobre las medidas de seguridad adoptadas para proteger la consiguiente transferencia de datos.

Se tratan los siguientes temas:

- Glosario: resumen de la terminología utilizada.
- Seguridad de las operaciones: analiza detenidamente los sistemas de supervisión, la infraestructura y los flujos de trabajo de desarrollo en la página para mantener la seguridad de MyQ Roger.
- Seguridad de las aplicaciones: describe el enfoque de seguridad de MyQ Roger, detallando las responsabilidades de las distintas partes, la automatización y la gestión.
- Protección de datos: resume los estándares de MyQ Roger para la seguridad de la nube multitenant, el cifrado y la comunicación segura, y el cumplimiento normativo y la gestión de identidades. También incluye disposiciones sobre el cumplimiento del RGPD y la copia de seguridad de datos.
- Tiempo de actividad del servidor, copia de seguridad de datos y recuperación ante desastres: detalla la supervisión del estado que proporciona MyQ Roger y las estrategias de copia de seguridad y los planes de respuesta disponibles.
- Confianza cero: examina el significado y la importancia de la seguridad de confianza cero y describe cómo MyQ Roger cumple con estos principios.
- Inicio de sesión seguro con MyQ Roger: detalla las medidas adoptadas por MyQ Roger para garantizar la seguridad del inicio de sesión.
- Impresión segura con MyQ Roger: proporciona detalles sobre los distintos métodos de impresión empleados por MyQ Roger y las medidas de seguridad que acompañan a cada uno de ellos.

# 2 Guía en PDF

Esta guía también está disponible en formato PDF.

| File | Size |
| --- | --- |
| MyQ Roger Data Security Whitepaper.pdf | 3.2 MB |

# 3 Glosario

- **IPP/s (Protocolo de impresión por Internet sobre TLS seguro)**:
  - MyQ Roger garantiza una impresión segura utilizando el Protocolo de impresión por Internet (IPP) a través de un canal cifrado TLS, lo que impide el acceso no autorizado y garantiza la integridad de los datos en tránsito.
  - MyQ Roger optimiza el tráfico de red mediante un manejo eficiente de los paquetes, lo que reduce la transmisión innecesaria de datos y garantiza una comunicación segura entre los puntos finales.
- **TLS (Seguridad de la capa de transporte)**:
  MyQ Roger aplica TLS 1.2/1.3 para el cifrado seguro de los datos en todas las comunicaciones, lo que garantiza la protección contra la interceptación y los ataques de tipo «man-in-the-middle» (MITM).
- **Datos en reposo, datos en tránsito**:
  - **Datos en reposo**: MyQ Roger cifra los datos almacenados utilizando AES-256, lo que garantiza que la información confidencial permanezca segura frente a accesos no autorizados.
  - **Datos en tránsito**: Todos los datos transferidos entre clientes, servidores y servicios en la nube se cifran mediante TLS para mantener la integridad y la confidencialidad.
- **Infraestructura de confianza cero**:
  MyQ Roger sigue un modelo de seguridad **de confianza cero** mediante la implementación de autenticación continua, verificación de dispositivos y acceso con privilegios mínimos para usuarios y servicios.
- **IAM (gestión de identidades y accesos)**:
  MyQ Roger integra las mejores prácticas de IAM mediante la aplicación de una autenticación segura de los usuarios, la autenticación multifactorial (MFA) y los controles de acceso basados en la identidad.
- **RBAC (control de acceso basado en roles)**:
  MyQ Roger implementa RBAC para restringir los permisos en función de los roles de los usuarios, lo que garantiza que solo el personal autorizado pueda acceder a funciones críticas y datos confidenciales.
- **SSO (inicio de sesión único)**:
  MyQ Roger admite **SSO** a través de la integración OAuth2, lo que permite una autenticación fluida en todas las aplicaciones empresariales, al tiempo que se mantiene la seguridad y el cumplimiento normativo.

# 4 Seguridad de las operaciones

## 4.1 Introducción

La seguridad es una prioridad máxima en MyQ Roger. Aplicamos un enfoque **que da prioridad a la seguridad** en todas las etapas del desarrollo, la implementación y las operaciones. Dada la naturaleza crítica de los entornos en la nube, la seguridad debe ser **proactiva, automatizada y supervisada continuamente** para evitar infracciones y accesos no autorizados.

Nuestra **estrategia de operaciones seguras** integra **la supervisión continua, la gestión de vulnerabilidades, la seguridad de la infraestructura y el cumplimiento** normativo para garantizar la integridad de las aplicaciones y la infraestructura.

## 4.2 Supervisión

La supervisión continua es esencial para detectar y responder a las amenazas en tiempo real. MyQ implementa un **enfoque de supervisión en varias capas:**

### 4.2.1 Detección y respuesta en los puntos finales (EDR)

- Supervisa todos los puntos finales (servidores, máquinas virtuales y contenedores) en busca de actividades sospechosas.
- Utiliza **análisis de comportamiento e inteligencia sobre amenazas** para detectar amenazas avanzadas.
- Aísla automáticamente los puntos finales comprometidos para evitar el movimiento lateral.

### 4.2.2 Azure Defender (ahora Defender para la nube)

- Protege **Azure AKS, SQL Server, máquinas virtuales y almacenamiento**.
- Proporciona **detección de amenazas en tiempo real** y recomendaciones de configuración de seguridad.
- Se integra con **Microsoft Sentinel (SIEM)** para la centralización de alertas.

### 4.2.3 Escaneo de hosts

- Analiza **máquinas virtuales, instancias en la nube y servidores locales** en busca de configuraciones incorrectas y software obsoleto.
- Detecta **riesgos de escalada de privilegios, puntos de acceso no autorizados y dependencias obsoletas**.

### 4.2.4 Recopilación y análisis de registros

- **Registro centralizado** en un clúster independiente para mayor escalabilidad y aislamiento.
- **Los registros de Kubernetes, las aplicaciones y la infraestructura** se etiquetan para facilitar su recuperación.
- **Las políticas de retención a largo plazo** garantizan el cumplimiento normativo y el análisis de seguridad.
- **Los mecanismos de alerta** detectan anomalías e incidentes de seguridad, integrándose con SIEM.
- **Correlación de registros en tiempo real** para solicitudes de API, eventos de autenticación, consultas de bases de datos y tráfico de firewall.

### 4.2.5 Escaneo de puertos

- Detecta **puertos abiertos** no autorizados que exponen los servicios a amenazas.
- Utiliza **herramientas automatizadas como Nmap y ZMap** para escanear **cambios inesperados** en **los puertos**.

### 4.2.6 Escaneo de contenedores

- **Escaneo estático y dinámico** de contenedores Docker antes de la implementación.
- Identifica vulnerabilidades en **imágenes base, capas de aplicaciones y permisos de tiempo de ejecución**.
- Integrado con **Trivy** para **el escaneo de seguridad de imágenes**.

### 4.2.7 Supervisión de Kubernetes

- Utiliza **la supervisión integrada de Azure Kubernetes Service (AKS)** con **Prometheus y Grafana**.
- Supervisa **las llamadas a la API de Kubernetes, las políticas RBAC y la seguridad de los pods**.
- Alertas sobre **escaladas de privilegios de contenedores, uso excesivo de recursos e intentos de movimiento lateral.**

### 4.2.8 Escaneos TLS regulares

- MyQ realiza **análisis de seguridad TLS utilizando Qualys SSL Labs** para garantizar las mejores prácticas.
- Se evalúan las configuraciones TLS para mantener una **calificación de seguridad A+**, mitigando los riesgos derivados de protocolos débiles.
- Las herramientas automatizadas verifican **la validez de los certificados, el seguimiento de su caducidad y la solidez de los protocolos**.

## 4.3 Gestión de vulnerabilidades

### 4.3.1 Análisis de vulnerabilidades

- **Los análisis periódicos** detectan fallos de seguridad en las aplicaciones y la infraestructura.
- Incluye **análisis CVE automatizados** para componentes implementados en la nube.
- Se integra con **DefectDojo, SonarQube y Trivy** para la evaluación de riesgos.

### 4.3.2 Pruebas de penetración

- Se realizan periódicamente para identificar las debilidades de seguridad antes de que sean explotadas.
- Combina **metodologías de pruebas automatizadas y manuales** para una evaluación exhaustiva.
- Los resultados se **documentan, priorizan y corrigen** según corresponda.

## 4.4 Seguridad de la infraestructura

Una **infraestructura reforzada** garantiza la seguridad más allá de la simple supervisión. MyQ emplea:

### 4.4.1 SIEM (gestión de información y eventos de seguridad)

- **Microsoft Sentinel SIEM** recopila eventos de seguridad para su detección en tiempo real.
- Analiza los registros de **los cortafuegos, los sistemas de identidad, los registros de aplicaciones, los registros de auditoría y las fuentes de amenazas**.
- Permite **respuestas automatizadas a las amenazas detectadas**.

### 4.4.2 Seguimiento y gestión de la seguridad

- **La base de datos de errores Jira** realiza un seguimiento, clasifica y prioriza las vulnerabilidades de seguridad.
- **DefectDojo** consolida los resultados de las pruebas, lo que garantiza un seguimiento estructurado de las actividades de seguridad.
- **La aplicación** regular **de parches y la corrección de errores** mantienen una sólida postura de seguridad.

### 4.4.3 Gestión de identidades y accesos (IAM)

- Aplica **el modelo Zero Trust** con **control de acceso basado en roles (RBAC) y autenticación multifactor (MFA)**.

- Utiliza **Azure AD** para la gobernanza de identidades.
- **Las alertas de escalada de privilegios** detectan el acceso administrativo no autorizado.

## 4.5 Flujo de trabajo de desarrollo

El desarrollo seguro de software es un aspecto fundamental de la estrategia de seguridad de MyQ. Las siguientes medidas garantizan la integridad del código, los procesos y los entornos en la nube:

### 4.5.1 Entorno de desarrollo seguro

- Los desarrolladores de MyQ utilizan **entornos** con **seguridad reforzada** y protección de puntos finales.
- Los desarrolladores deben seguir **prácticas de codificación seguras y recibir formación periódica en materia de seguridad**.

### 4.5.2 Canales seguros de GitLab

- Los procesos de GitLab CI/CD incluyen **comprobaciones de seguridad automatizadas, revisiones de código y pruebas**.
- **Las pruebas de seguridad estáticas de aplicaciones (SAST)** y **las pruebas de seguridad dinámicas de aplicaciones (DAST)** detectan vulnerabilidades.
- **La firma de imágenes de contenedores** garantiza que solo se implementen imágenes de confianza.

### 4.5.3 IAM y control de acceso

- Solo **el personal seleccionado de DevOps y SecOps** tiene acceso a los entornos de nube de Azure.
- Se aplica **el control de acceso basado en roles (RBAC) con elevación de privilegios mínimos Just-In-Time (JIT)**.

### 4.5.4 Azure Kubernetes y seguridad de contenedores

- **Los clústeres AKS** de MyQ **extraen imágenes únicamente del Registro de contenedores de Azure (ACR)**.
- Los entornos AKS aplican **políticas de red y Pod Security Standards (PSS)** para aislar las cargas de trabajo.

### 4.5.5 Gestión de secretos

- **Todos los secretos y claves API se almacenan en Azure Key Vault**, al que solo puede acceder el personal autorizado por IAM.

- Se realizan **análisis del sistema de archivos Trivy** antes de realizar el commit en Git para detectar y prevenir secretos confidenciales.

## 4.6 Conclusión

**La estrategia de operaciones seguras** de MyQ se basa en la **supervisión continua, la gestión proactiva de amenazas y una sólida seguridad de la infraestructura**. Al aprovechar **herramientas de seguridad avanzadas, controles de acceso estrictos y pruebas automatizadas**, MyQ garantiza un **entorno de nube seguro y resistente**.

Con la **integración de análisis de seguridad TLS, pruebas de penetración y registro centralizado**, MyQ mejora su capacidad para **detectar, responder y mitigar los riesgos de seguridad** de forma eficaz.

La seguridad es un **reto en constante evolución**, y MyQ mantiene su compromiso de **mejorar las medidas de seguridad mediante actualizaciones periódicas, auditorías de cumplimiento y mejores prácticas de seguridad**. Al mantener una **mentalidad que da prioridad a la seguridad**, MyQ defiende la **integridad y la confidencialidad** de sus servicios, garantizando **la confianza y la fiabilidad** para todas las partes interesadas.

# 5 Seguridad de las aplicaciones

## 5.1 La evolución de las amenazas a la seguridad

En los primeros tiempos, antes de que se generalizara el uso de Internet, las impresoras se conectaban directamente mediante cables LPT y las preocupaciones en materia de seguridad eran mínimas. El mayor riesgo era físico: que alguien mirara por encima del hombro del usuario para ver los documentos impresos. El panorama de la seguridad era sencillo y las amenazas cibernéticas eran prácticamente inexistentes.

Sin embargo, a medida que las impresoras y los dispositivos se conectaron a la red, el panorama de las amenazas cambió drásticamente. Ahora que se puede acceder a las impresoras a través de redes de área local (LAN) e incluso de Internet, los atacantes ya no necesitan acceso físico. Amenazas como los ataques de tipo «man-in-the-middle» (MITM), la interceptación no autorizada de datos y los exploits remotos se han vuelto frecuentes. Los ciberdelincuentes han pasado de mirar por encima del hombro a espiar el tráfico de la red y explotar las vulnerabilidades.

Mitigar estos riesgos es un reto continuo, ya que surgen nuevas amenazas con frecuencia. Para hacer frente a estos retos de seguridad en constante evolución, MyQ Roger implementa prácticas de seguridad continuas, supervisión proactiva y sólidos mecanismos de defensa.

## 5.2 El enfoque de seguridad de MyQ Roger

MyQ Roger se ha creado con un enfoque que da prioridad a la seguridad, lo que garantiza que la innovación y la experiencia del usuario estén siempre en consonancia con los más altos estándares de seguridad. Nuestro compromiso con la seguridad se refleja en nuestros continuos esfuerzos por integrar medidas de seguridad robustas en cada etapa del desarrollo. Adoptamos una filosofía de «seguridad por defecto», incorporando la seguridad en nuestros productos y servicios desde el principio.

Para lograrlo, MyQ Roger aprovecha la automatización, las evaluaciones de riesgos basadas en datos y las mejores prácticas de seguridad para identificar y mitigar de forma proactiva las amenazas. Al implementar controles de seguridad en las primeras fases del ciclo de desarrollo, siguiendo un **enfoque de «desplazamiento a la izquierda»**, nos aseguramos de que las vulnerabilidades se detecten y se corrijan antes de que lleguen a la fase de producción. Esta integración proactiva nos permite escalar de forma eficiente, reducir los riesgos y minimizar las amenazas de seguridad.

Nuestro enfoque refuerza nuestro compromiso con la protección de los datos de los clientes, los flujos de trabajo y la postura de seguridad general.

## 5.3 Desplazamiento hacia la izquierda en materia de seguridad

El desplazamiento hacia la izquierda en materia de seguridad significa integrar la seguridad en una fase temprana del ciclo de vida del desarrollo de software (SDLC), en lugar de abordar las vulnerabilidades más adelante. Al detectar los problemas de seguridad en las etapas iniciales de desarrollo, evitamos costosas correcciones y mitigamos posibles infracciones. Esta estrategia proactiva garantiza que cada línea de código cumpla con los más altos estándares de seguridad antes de llegar a la fase de producción, lo que reduce los riesgos y refuerza nuestra postura de seguridad general.

## 5.4 Responsabilidades de seguridad de MyQ

MyQ Roger se compromete a proteger los datos de los clientes y a garantizar un entorno operativo seguro. Nuestras principales responsabilidades en materia de seguridad incluyen:

- **Protección de datos**: MyQ garantiza que los datos de los clientes se almacenen y cifren de forma segura, evitando el acceso no autorizado y garantizando la confidencialidad de los datos.
- **Aplicación periódica de parches de seguridad**: aplicamos de forma proactiva parches y actualizaciones de seguridad a todos los sistemas para eliminar las vulnerabilidades antes de que puedan ser explotadas.
- **Gestión del control de acceso**: aplicamos políticas de acceso estrictas siguiendo el principio del mínimo privilegio, lo que garantiza que solo el personal autorizado pueda acceder a los recursos confidenciales.

Al defender estos principios de seguridad, MyQ Roger fomenta una cultura de seguridad, protegiendo a los usuarios de posibles amenazas y garantizando el cumplimiento de los estándares del sector.

## 5.5 Control/gestión de la seguridad de MyQ Roger

Aunque confiamos en una infraestructura de nube segura, MyQ Roger asume la responsabilidad directa de implementar capas de seguridad adicionales y cumplir con las mejores prácticas del sector. Nuestro enfoque incluye:

- **Gestión de claves con Azure Key Vault**: utilizamos Azure Key Vault para almacenar y gestionar de forma segura todos los secretos, claves privadas y certificados, garantizando controles de acceso y cifrado estrictos.
- **Certificación ISO 27001**: cumplimos con las normas ISO 27001 para mantener un enfoque estructurado y coherente de la seguridad de la información.
- **Detección y respuesta en los puntos finales (EDR)**: aprovechamos soluciones EDR avanzadas para detectar, analizar y mitigar las amenazas de seguridad en tiempo real, lo que reduce el tiempo de respuesta y minimiza los riesgos.
- **Prácticas de desarrollo seguro**: nuestro ciclo de vida de desarrollo de software seguro incluye evaluaciones de vulnerabilidad, supervisión continua y análisis de seguridad automatizados para detectar y corregir fallos de seguridad.
- **Auditorías de seguridad periódicas**: realizamos auditorías internas y externas para garantizar el cumplimiento y abordar de forma proactiva los riesgos de seguridad.
- **SIEM con Azure Sentinel**: utilizamos Azure Sentinel para la detección de amenazas en tiempo real, la respuesta automatizada y la supervisión continua de la seguridad en todos los entornos de nube y red.

Al implementar estas medidas de seguridad, MyQ Roger refuerza su marco de seguridad general, garantizando que los datos de los clientes permanezcan protegidos en todo momento.

## 5.6 Microsoft Azure y el cumplimiento normativo

MyQ Roger se ejecuta en Microsoft Azure, aprovechando Azure Kubernetes Service (AKS), Azure SQL Servers y Azure Cosmos DB para MongoDB. Al operar dentro de la infraestructura de Azure, nos beneficiamos de los estándares de seguridad, cumplimiento normativo y fiabilidad líderes en el sector de Microsoft.

### 5.6.1 Responsabilidades de Microsoft en materia de seguridad y cumplimiento normativo

- Azure se adhiere a marcos de cumplimiento globales como ISO 27001, SOC 2 y GDPR en la UE, lo que garantiza el cumplimiento de estrictas normas reglamentarias.
- Microsoft proporciona características de seguridad integradas, como aislamiento de red, protección de identidad y detección continua de amenazas, lo que reduce las superficies de ataque.
- Los servicios de Azure se someten a rigurosas evaluaciones de seguridad y pruebas de penetración para identificar y corregir de forma proactiva las vulnerabilidades.

Aprovechando la infraestructura segura de Azure, MyQ Roger añade sus propias capas de seguridad para crear un modelo de seguridad robusto y resistente que protege las aplicaciones y los datos de los clientes.

## 5.7 Responsabilidades de seguridad del cliente

Aunque MyQ Roger proporciona una infraestructura segura y las mejores medidas de seguridad de su clase, los clientes también tienen responsabilidades clave para garantizar la seguridad de su entorno. Entre ellas se incluyen:

- **Mantener una lista de usuarios activos**: los clientes deben gestionar continuamente el acceso de los usuarios aprovechando la sincronización automática de usuarios o desactivando manualmente las cuentas inactivas para minimizar el riesgo.
- **Aplicación del control de acceso basado en roles (RBAC)**: los clientes deben aplicar los principios del RBAC para restringir el acceso de los usuarios solo a los permisos necesarios, lo que garantiza una mayor seguridad y eficiencia operativa.
- **Proteger la red local**: aunque MyQ Roger funciona con un modelo de confianza cero, los clientes deben asegurarse de que su red local cumpla con las mejores prácticas de seguridad, como configuraciones de cortafuegos, segmentación de la red y protección de los puntos finales.
- **Mantenimiento adecuado de los recursos**: Todos los dispositivos conectados, incluidas las impresoras y los dispositivos multifunción (MFP), deben actualizarse periódicamente con el firmware y los parches de seguridad más recientes para evitar vulnerabilidades.

Al cumplir con estas responsabilidades, los clientes refuerzan su postura de seguridad y se benefician del completo marco de seguridad de MyQ Roger.

## 5.8 Automatización de la seguridad

Para mejorar aún más la seguridad a lo largo del ciclo de vida del desarrollo, MyQ Roger integra pruebas de seguridad automatizadas y evaluaciones de seguridad externas:

- **SAST (pruebas estáticas de seguridad de aplicaciones)**: se realizan en cada compromiso para detectar vulnerabilidades de seguridad en una fase temprana del ciclo de desarrollo, lo que reduce la probabilidad de que el código inseguro llegue a la producción.
- **DAST (pruebas dinámicas de seguridad de aplicaciones)**: se realizan en entornos sandbox para identificar y mitigar los riesgos de seguridad en tiempo de ejecución antes de la implementación.

- **Pruebas de penetración externas**: Contratamos a expertos en seguridad independientes para que realicen pruebas de penetración, lo que garantiza que nuestras defensas de seguridad puedan resistir escenarios de ataque reales.

Al automatizar las pruebas de seguridad y realizar evaluaciones externas periódicas, MyQ Roger mantiene una postura de seguridad proactiva y resistente.

## 5.9 Conclusión

En MyQ Roger, la seguridad no es una cuestión secundaria, sino que forma parte integral de nuestro producto y del ciclo de vida del desarrollo. Al combinar principios de seguridad desde el diseño, las mejores prácticas del sector y un sólido marco de cumplimiento, ofrecemos una postura de seguridad robusta que protege los datos y las operaciones de nuestros clientes. Nuestro compromiso con la mejora continua de la seguridad garantiza que MyQ Roger siga siendo resistente frente a las amenazas en constante evolución, al tiempo que mantiene los más altos estándares de fiabilidad y confianza. Seguiremos evolucionando nuestra estrategia de seguridad, adaptándonos a los nuevos retos y aprovechando las últimas tecnologías para mantener nuestra misión de proporcionar una experiencia de usuario segura y fluida.

# 6 Protección de datos

## 6.1 Resumen

La protección de datos es el núcleo del enfoque de seguridad **de MyQ Roger**, que garantiza que todos los aspectos de su solución de impresión y escaneo basada en la nube cumplan con los más altos estándares de la industria. Un principio fundamental de MyQ Roger es que **ningún dato de trabajos de impresión o escaneo se transfiere a través de sus servidores**. En cambio, MyQ Roger limita estrictamente su recopilación de datos a **metadatos** esenciales, como **nombres de archivos de trabajos, tamaños de archivos e información sobre el número de páginas**. Esto garantiza la eficiencia operativa al tiempo que protege la privacidad de los usuarios.

## 6.2 Seguridad en la nube multitenant

Como **producto en la nube multitenant**, MyQ Roger ofrece a los clientes un entorno **lógicamente aislado** para evitar la exposición de datos entre tenants.

Para proporcionar resiliencia, MyQ Roger se basa en **Azure SQL** y **Azure Cosmos DB**, que ofrecen funciones de seguridad integradas**,** como **el cifrado de datos en reposo y en tránsito, la detección automatizada de amenazas y la supervisión del acceso**. La infraestructura en la nube se somete a evaluaciones de seguridad continuas para mitigar los riesgos asociados a los entornos multitenant.

## 6.3 Cifrado y comunicación segura

La seguridad está integrada en todos los niveles de las operaciones de MyQ Roger. Todas las comunicaciones entre los clientes, los servicios en la nube y las impresoras se **cifran mediante TLS (Transport Layer Security)** para evitar el acceso no autorizado o la manipulación.

Para reforzar aún más la seguridad, **las autoridades de certificación (CA) de confianza pública** firman todos los certificados utilizados en MyQ Roger, lo que garantiza el máximo nivel de confianza. Además, los certificados se **renuevan cada tres meses**, lo que reduce el riesgo de posibles compromisos y mantiene el cumplimiento de las mejores prácticas de seguridad.

## 6.4 Cumplimiento normativo y gestión de identidades

MyQ Roger se ajusta a las normas de seguridad reconocidas internacionalmente y cuenta con **la certificación ISO 27001**, lo que demuestra su compromiso con la implementación de prácticas sólidas de gestión de la seguridad de la información.

Para aplicar controles de acceso estrictos, se implementa **el control de acceso basado en roles (RBAC)**, lo que garantiza que a los usuarios **solo** se les concedan **los permisos necesarios para su función**. Esto minimiza la exposición a datos confidenciales y reduce el riesgo de uso indebido accidental o intencionado.

## 6.5 Cumplimiento del RGPD

Garantizar el cumplimiento del **Reglamento General de Protección de Datos (RGPD)** es una prioridad máxima para MyQ Roger. De acuerdo con los principios del RGPD, MyQ Roger sigue estrictas medidas de protección de datos para salvaguardar la privacidad de los usuarios:

- **Minimización de datos**: solo se recopilan los metadatos esenciales, lo que elimina el riesgo de almacenar documentos confidenciales de los usuarios.
- **Derechos y control de los usuarios**: los usuarios tienen la posibilidad de solicitar **el acceso, la corrección, la eliminación o la anonimización** de sus datos personales, tal y como exige el RGPD.
- **Transparencia en el tratamiento de datos**: las políticas de privacidad, claras y concisas, describen cómo se gestionan, almacenan y protegen los metadatos.
- **Almacenamiento seguro de datos**: todos los datos se **cifran en reposo y en tránsito**, lo que garantiza el pleno cumplimiento de los estrictos requisitos de seguridad del RGPD.
- **Medidas de anonimización**: cuando es necesario, MyQ Roger implementa **técnicas de anonimización de datos** para garantizar que los datos personales ya no puedan atribuirse a un usuario específico, lo que refuerza la protección de la privacidad.

Estas medidas garantizan que MyQ Roger se ajusta plenamente a los requisitos fundamentales del RGPD, lo que permite a los usuarios controlar sus datos personales y mantiene un entorno seguro y conforme a la normativa.

## 6.6 Copias de seguridad de datos

Para proteger contra la pérdida de datos y garantizar la fiabilidad del servicio, MyQ Roger implementa una **estrategia integral de copias de seguridad de datos**. Esto incluye:

- **Copias de seguridad automatizadas**: **las copias de seguridad incrementales y completas** programadas periódicamente garantizan que los datos sigan siendo recuperables en caso de incidente.
- **Almacenamiento seguro**: las copias de seguridad se cifran mediante **el cifrado AES-256**, lo que garantiza que, incluso en el improbable caso de que se produzca un acceso no autorizado, los datos sigan siendo ilegibles.
- **Políticas de retención**: las copias de seguridad se **almacenan durante un periodo definido** de acuerdo con los requisitos de cumplimiento, lo que permite una recuperación eficiente en caso de fallo del sistema o situaciones de recuperación ante desastres.
- **Pruebas y verificación de integridad**: se realizan **pruebas** periódicas **de integridad de las copias de seguridad** para confirmar que las copias almacenadas son funcionales y fiables, lo que garantiza una restauración de datos sin problemas cuando sea necesario.

Al implementar estas sólidas medidas de seguridad, cumplimiento normativo y copia de seguridad, **MyQ Roger ofrece una solución de impresión y escaneo basada en la nube segura, privada y altamente eficiente** que cumple con los más altos estándares de protección de datos del sector.

# 7 Política de privacidad

Su privacidad es nuestra preocupación, y nos la tomamos muy en serio. La presente Política de privacidad de MyQ Roger Solution (la «Política de privacidad») explica qué tipo de información puede recopilar, conservar y procesar MyQ en relación con el suministro de cualquier producto, servicio, contenido, aplicación u otros componentes que formen parte de MyQ Roger Solution (los «Servicios»), y cómo se utiliza y protege dicha información. También establece cómo puede ponerse en contacto con nosotros si tiene alguna pregunta o duda sobre sus datos personales.

Esta Política de privacidad ha sido emitida por MyQ, spol. s.r.o., con domicilio social en Českomoravská 2420/15, Libeň, 190 00 Praga 9, República Checa, con número de identificación fiscal 615 06 133, inscrita en el Registro Mercantil del Tribunal Municipal de Praga, sección C, inserto 29842 («MyQ» o «nosotros»).

Nos reservamos el derecho a realizar cambios en esta Política de privacidad en cualquier momento. Le rogamos que consulte periódicamente la Política de privacidad para conocer los cambios, aunque, si es usted cliente nuestro, también podremos notificarle por correo electrónico cualquier cambio que, a nuestro exclusivo criterio, afecte de manera significativa a su uso de los Servicios o a la forma en que tratamos sus datos personales. El uso continuado de nuestros Servicios cubiertos por esta Política de privacidad significará su aceptación de todos y cada uno de los cambios que realicemos en esta Política de privacidad de vez en cuando.

## 7.1 1. Datos que recopilamos o recibimos

Recopilamos datos personales de nuestros clientes, como usuarios de los Servicios, y de sus usuarios finales (lo que incluye a los empleados de nuestros clientes) con el fin de configurar y gestionar cuentas de usuario y proporcionar y administrar los Servicios. También recopilamos datos y métricas de uso. Somos los responsables del tratamiento de estos datos personales.

Con respecto a los datos personales que puedan estar incluidos en los metadatos del Contenido, tal y como se define en los Términos de servicio https://www.myq-solution.com/en/myq-legal-documents , que los usuarios o usuarios finales gestionan utilizando los Servicios, o con respecto a los datos personales a los que podamos tener acceso mientras prestamos servicios de asistencia remota o local (los «Datos del cliente»), tratamos dichos datos personales en nombre de nuestros clientes como encargados del tratamiento. Cuando tratamos los Datos del cliente para prestar los Servicios a nuestros clientes, actuamos de acuerdo con las instrucciones de nuestros

clientes como encargados del tratamiento de sus datos. Siempre mantenemos los Datos del cliente que tratamos en nombre de nuestros clientes y de conformidad con sus instrucciones separados de los datos de nuestros otros clientes y los mantenemos estrictamente confidenciales.

### 7.1.1 1.1 Datos de los usuarios y usuarios finales de nuestros Servicios

Recopilamos sus datos personales cuando:

- Crea una cuenta en nuestros Servicios;
- Inicia sesión en nuestro Servicio, introduciendo su nombre de usuario (correo electrónico) y contraseña;
- Utiliza nuestros Servicios o interactúa de otro modo con MyQ, por ejemplo, cuando nos envía alguna consulta;
- Proporciona voluntariamente dichos datos a MyQ.

Cuando crea una cuenta en MyQ, le pedimos que rellene un formulario de registro indicando su nombre, apellidos, correo electrónico, empresa y cargo. También puede optar por añadir un número de teléfono a su cuenta.

También recopilamos y procesamos su nombre de usuario (correo electrónico) y contraseña.

Con fines de análisis y mejora de nuestros Servicios, nuestros servidores pueden registrar automáticamente información cuando visita nuestro sitio web o utiliza algunos de nuestros Servicios («datos de uso»), incluyendo:

- Información sobre servicios de terceros que el usuario y sus usuarios finales conectan a los Servicios con fines de autenticación y conexión al almacenamiento en la nube del usuario;
- Información sobre los dispositivos del usuario, por ejemplo, el tipo y la marca de las impresoras y su número de serie;
- Información sobre el uso de nuestros Servicios, por ejemplo, la cantidad de documentos impresos o escaneados.

Los Servicios le permiten conectarse a aplicaciones de terceros u otros servicios, por ejemplo, One Drive o Google Disk, con el fin de compartir documentos y otros Contenidos con los Servicios. Si decide conectarse a servicios de terceros, le pediremos su permiso para que los Servicios puedan acceder a dichos servicios de terceros; sin embargo, MyQ no procesará ningún dato personal almacenado allí, excepto los Datos del cliente, tal y como se definen anteriormente.

Si nuestros Servicios son adquiridos por una entidad, son los usuarios individuales dentro de la organización de dicha entidad los que inician sesión en nuestra plataforma de Servicios y cuyos datos personales se recopilan, tal y como se ha

descrito anteriormente. Cuando dicha entidad nos proporcione directamente cualquier dato personal de sus empleados u otros usuarios individuales a los que haya autorizado a acceder a los Servicios, deberá contar con todos los consentimientos, permisos o registros necesarios para procesar y proporcionarnos los datos personales de sus empleados o usuarios.

### 7.1.2 1.2 Datos del cliente

Para prestar nuestros Servicios a nuestros usuarios y usuarios finales, también podemos tratar Datos del cliente, tal y como se definen anteriormente. El tratamiento de los Datos del cliente está sujeto a la política de privacidad de los usuarios, y estos están obligados a garantizar que el tratamiento de dichos datos sea lícito y cumpla con la legislación aplicable. El tratamiento de datos con respecto a los Datos del cliente realizado por MyQ se rige por los acuerdos de tratamiento de datos aplicables celebrados con los usuarios.

## 7.2 2. Cómo utilizamos los datos

Utilizamos sus datos personales para los siguientes fines:

### 7.2.1 2.1 Para prestar los Servicios

Podemos tratar sus datos personales para identificarle cuando inicia sesión en su cuenta y utiliza nuestros Servicios, con el fin de poder operar los Servicios y prestárselos. Esto puede incluir la verificación de sus pagos, órdenes de compra e información de facturación.

### 7.2.2 2.2 Para comunicarnos con usted

Podemos procesar los datos de nuestros clientes o de sus usuarios finales individuales, en particular el correo electrónico u otros datos de contacto, para comunicarnos con nuestros usuarios y usuarios finales, por ejemplo, cuando les ayudamos a configurar o administrar su cuenta, cuando les proporcionamos atención al cliente y asistencia, les enviamos avisos técnicos, actualizaciones de próximos cambios o mejoras en los Servicios, recordatorios, alertas de seguridad y otros mensajes de asistencia y administrativos.

### 7.2.3 2.3 Para proporcionar una mejor experiencia de usuario

Podemos procesar sus datos personales para conocer cómo utiliza nuestros Servicios y, de este modo, mejorar continuamente la experiencia del usuario, así como

proporcionar una atención al cliente fluida. También podemos procesar dichos datos personales para mejorar y optimizar nuestros Servicios existentes y desarrollar nuevas ofertas. Esto incluye estadísticas de productos y mercados, investigaciones y análisis, comparativas y otros análisis para comprender mejor sus necesidades y las necesidades de los usuarios en su conjunto, diagnosticar problemas y analizar tendencias.

### 7.2.4 2.4 Para proteger nuestros Servicios y defender nuestros derechos o los de terceros

Procesamos sus datos personales para mantener el Servicio seguro, protegido y fiable. Esto incluye detectar, prevenir y responder a fraudes, abusos, riesgos de seguridad y problemas técnicos que podrían perjudicar a MyQ, a nuestros clientes y a los usuarios finales.

Podemos tratar algunos de los datos especificados en la sección 1.1 cuando lo exija la ley o para establecer, ejercer o defender nuestras reclamaciones legales o, cuando sea necesario, proteger los derechos e intereses de MyQ.

### 7.2.5 2.5 Con fines de marketing y ventas

Podemos tratar los datos de contacto de las personas de contacto designadas por usted o sus usuarios finales con el fin de proporcionarle información relacionada con las nuevas funciones de los Servicios y las nuevas ofertas de productos. Para obtener más detalles, consulte la sección 7 más abajo.

## 7.3 3. Base legal

Para los fines especificados en las secciones 2.1 y 2.2, procesamos sus datos personales basándonos en nuestro contrato con usted (si es nuestro cliente directo y una persona física) o basándonos en nuestro interés legítimo de proporcionar nuestros Servicios a nuestros clientes (cuando nuestro cliente es su empresa u organización y usted es un usuario final autorizado designado por su empresa u organización).

Para los fines especificados en la sección 2.3, tratamos sus datos personales basándonos en nuestro interés legítimo de desarrollar y mejorar nuestros Servicios.

Para los fines especificados en la sección 2.4, tratamos sus datos personales basándonos en nuestro interés legítimo de proteger y garantizar nuestros derechos o reclamaciones o los derechos de nuestros clientes o usuarios.

Para los fines especificados en la sección 2.5, tratamos sus datos personales basándonos en su consentimiento voluntario, siempre que nos lo haya dado. En un ámbito limitado permitido por la legislación aplicable, también podemos utilizar sus datos de contacto electrónicos para informarle sobre nuestros Servicios sin su consentimiento explícito, basándonos en nuestro interés legítimo, tal y como se describe con más detalle en la sección 7 más adelante.

Cuando utilizamos sus datos personales para nuestros intereses legítimos, nos aseguramos de tener en cuenta cualquier impacto potencial que dicho uso pueda tener sobre usted. Nuestros intereses legítimos no prevalecen automáticamente sobre los suyos y no utilizaremos su información si creemos que sus intereses deben prevalecer sobre los nuestros, a menos que tengamos otros motivos para hacerlo (como el cumplimiento de un contrato, su consentimiento o una obligación legal). Si tiene alguna duda sobre nuestro tratamiento, consulte los detalles de «Sus derechos» en la sección 9 más abajo.

## 7.4 4. Plazos de conservación

Cuando tratamos datos personales como responsables del tratamiento, conservamos sus datos personales durante el periodo necesario para cumplir los fines descritos en la presente Política de privacidad y/o en cualquier acuerdo de servicios, a menos que la ley exija una conservación más prolongada (por ejemplo, con fines fiscales o contables o debido a otros requisitos legales) o que sea necesario almacenar los datos para el establecimiento, el ejercicio o la defensa de las reclamaciones legales de MyQ; en tal caso, solo almacenaremos los datos necesarios para la ejecución de nuestras reclamaciones o nuestra defensa durante el periodo necesario en cada caso y sin exceder los plazos de prescripción legales.

Cuando tratamos datos personales en nombre de nuestros clientes como encargados del tratamiento, conservamos dichos datos durante la vigencia de nuestro acuerdo con dichos clientes y los eliminamos de acuerdo con nuestros procesos de conservación y copia de seguridad automáticamente en un plazo de 90 días tras la rescisión del acuerdo, a menos que los clientes nos pidan que los borremos antes.

## 7.5 5. Compartir sus datos personales con fines legales y comerciales

Podemos utilizar y/o divulgar a terceros (incluidos organismos gubernamentales y autoridades policiales, nuestras filiales, asesores profesionales y nuestros proveedores o subcontratistas) información sobre usted cuando:

- Cumplimos con un proceso legal;
- Hacemos valer o defendemos los derechos legales de MyQ, y en relación con una reestructuración corporativa, como una fusión, adquisición de negocios o situaciones de insolvencia;
- Prevenir el fraude o daños inminentes; y
- Garantizamos la seguridad y la operatividad de nuestra red y nuestros servicios.

Esta información se compartirá siempre que, en todas estas circunstancias, solo compartamos la información personal limitada que sea necesaria compartir en esa situación concreta.

Compartimos sus datos con nuestros socios comerciales de confianza o con personas que procesan sus datos como nuestros procesadores de datos en nuestro nombre y de conformidad con nuestras instrucciones, de acuerdo con esta Política de privacidad. Seleccionamos a nuestros proveedores con mucho cuidado y siempre nos aseguramos de que proporcionen una protección de datos y unas garantías de seguridad adecuadas. A tal efecto, hemos vinculado a nuestros procesadores de datos con acuerdos de procesamiento de datos celebrados de conformidad con el artículo 28 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) («RGPD»).

Si selecciona que su inquilino de Servicios en la interfaz de administración de MyQ se encuentre en la UE, sus Datos de cliente se tratarán en la UE, de conformidad con los compromisos contractuales de Microsoft en materia de límites de datos de la UE. Si selecciona que su inquilino de Servicios en la interfaz de administración de MyQ se ubique fuera de la UE, dicha transferencia se realizará sobre la base de las cláusulas contractuales tipo (cláusulas modelo) aprobadas por la Comisión Europea (2010/87/UE), a menos que se disponga de un mecanismo de transferencia diferente en virtud de los artículos 45, 46 y siguientes del RGPD. No obstante lo anterior, sus datos de cliente también pueden transferirse a países para los que la Comisión Europea haya emitido una decisión de adecuación.

La lista de nuestros procesadores actuales que pueden tener acceso a sus datos personales:

- http://salesforce.comEMEA Ltd. (procesamiento relacionado con las ventas y asistencia técnica),
- Microsoft Ireland Operations Limited (colaboración y comunicación, Microsoft Azure: servicios de alojamiento en la nube),

- TeamViewer GmbH (asistencia técnica).

Además de los procesadores mencionados anteriormente, también podemos compartir sus datos personales para gestionar nuestros procesos comerciales y cumplir con nuestras obligaciones legales, incluidos los servicios logísticos, de facturación, fiscales, legales y técnicos.

Además de los proveedores externos, MyQ puede compartir datos con sus filiales ubicadas en la UE y el Reino Unido con el fin de prestar determinados servicios logísticos, de facturación, fiscales, jurídicos y técnicos. La lista actualizada de nuestras filiales en la UE y el Reino Unido está disponible en https://www.myq-solution.com/en/the-list-of-myq-data-processors .

## 7.6 6. Estadísticas anónimas

Podemos utilizar datos agregados y anonimizados derivados de los datos personales que usted nos ha facilitado o recopilados por el programa de análisis, como el comportamiento y las actividades de los usuarios, para nuestras propias estadísticas, para auditorías, con fines de investigación de productos y mercados, para análisis (que nos ayudan a optimizar y mejorar nuestros Servicios y su usabilidad, la gama de Servicios y a desarrollar nuevas tecnologías, productos y servicios), y para comparativas y otros análisis.

## 7.7 7. Comunicaciones de marketing

Podemos ponernos en contacto con las personas de contacto designadas por usted o sus usuarios finales para proporcionarles información relacionada con las nuevas funciones de los Servicios y las nuevas ofertas de productos, siempre que tengamos el permiso necesario para hacerlo, ya sea sobre la base de su consentimiento (cuando lo hayamos solicitado y usted nos lo haya proporcionado) o de nuestros intereses legítimos para proporcionarle comunicaciones de marketing cuando podamos hacerlo legalmente, dentro de los límites establecidos por la ley. En este último caso, solo le enviaremos comunicaciones de marketing si está utilizando o ha utilizado recientemente cualquiera de nuestros Servicios y no se ha opuesto a recibir dicha información (por cualquiera de los medios que se mencionan a continuación).

Puede cambiar sus preferencias de comunicación de marketing en cualquier momento siguiendo las instrucciones que se indican a continuación:

- Si desea darse de baja de un correo electrónico que se le ha enviado, siga el enlace «darse de baja» y/o las instrucciones que figuran en la parte inferior del correo electrónico.

- También puede ponerse en contacto con nosotros utilizando los datos que figuran en la sección «Contacto» más abajo para cambiar sus preferencias de comunicación comercial, incluida la retirada de su consentimiento.

Si ha recibido correos electrónicos no deseados y no solicitados enviados a través de nuestro sistema o que pretenden haber sido enviados a través de nuestro sistema, reenvíe una copia de dicho correo electrónico con sus comentarios a info@myq-solution.com[1] para su revisión.

Tenga en cuenta que ocasionalmente podemos enviarle información importante (incluso por correo electrónico) sobre los Servicios que utiliza o ha utilizado, incluidos los cambios en los términos y condiciones aplicables y/u otras comunicaciones o notificaciones que puedan ser necesarias para cumplir con nuestras obligaciones legales y contractuales, tal y como se describe en la sección 2.2 anterior. Estas comunicaciones importantes sobre los Servicios no constituyen comunicaciones de marketing y no se ven afectadas por sus preferencias.

## 7.8 8. Seguridad y ubicación de sus datos

Hemos implementado y mantendremos las medidas técnicas y organizativas adecuadas, los controles internos y las rutinas de seguridad de la información de acuerdo con las buenas prácticas del sector, teniendo en cuenta el estado del desarrollo tecnológico, con el fin de proteger sus datos contra la pérdida accidental, la destrucción, la alteración, la divulgación o el acceso no autorizados o la destrucción ilegal. Dichas medidas pueden incluir, entre otras, la adopción de medidas razonables para garantizar la fiabilidad de los empleados que tienen acceso a sus datos y el establecimiento de derechos de acceso limitados y controles de acceso; la autenticación; la formación del personal; copias de seguridad periódicas; procedimientos de recuperación de datos y gestión de incidentes; restricciones al almacenamiento, la impresión y la eliminación de datos personales; protección mediante software de los dispositivos en los que se almacenan datos personales; etc.

## 7.9 9. Sus derechos

En esta sección se describen sus derechos en virtud de las leyes aplicables, como el RGPD, y cómo ejercerlos. Si ejerce alguno de sus derechos de conformidad con esta sección o con las leyes aplicables, comunicaremos cualquier rectificación o supresión de sus datos personales o restricción del tratamiento realizada de acuerdo con su solicitud a cada destinatario al que se hayan revelado los datos personales de

1. mailto:info@myq-solution.com

conformidad con la sección 5 de esta Política de privacidad, a menos que dicha comunicación resulte imposible o suponga un esfuerzo desproporcionado.

Si desea ejercer estos derechos y/u obtener toda la información relevante sobre el tratamiento de sus datos personales, póngase en contacto con nosotros en info@myq-solution.com[2]. Se le pedirá que se identifique; esto es necesario para verificar que la solicitud ha sido enviada por usted. Le responderemos en el plazo de un mes a partir de la recepción de su solicitud, pero nos reservamos el derecho de ampliar este plazo hasta dos meses en circunstancias excepcionales justificadas. En cualquier caso, le informaremos en el plazo de un mes a partir de la recepción de su solicitud si decidimos ampliar el plazo de nuestra respuesta.

De conformidad con la legislación aplicable y tal y como se describe más adelante, usted tiene derecho a solicitar el acceso a sus datos personales y a la información sobre su tratamiento, el derecho a la rectificación, supresión o portabilidad (por ejemplo, la transferencia de sus datos personales a otro proveedor de servicios) de los datos personales que tratamos, así como el derecho a oponerse al tratamiento de sus datos personales y/o solicitar la restricción de dicho tratamiento.

Tenga en cuenta que su oposición al tratamiento podría significar que no podamos prestarle nuestros Servicios o realizar las acciones necesarias para alcanzar los fines establecidos anteriormente (véase la sección 2 «Cómo utilizamos los datos»).

Es importante que los datos personales que tenemos sobre usted sean precisos y estén actualizados. Manténganos informados si sus datos personales cambian durante su relación con nosotros poniéndose en contacto con nosotros a través de los datos de contacto que figuran en la sección 10 «Contacte con nosotros».

### 7.9.1 9.1 Información sobre sus datos personales, acceso a ellos y rectificación de los mismos

De acuerdo con la legislación aplicable, tiene derecho a obtener confirmación sobre si se están tratando datos personales que le conciernen (de acuerdo con el proceso descrito anteriormente) y, en tal caso, tiene derecho a acceder y rectificar los datos personales que ha compartido con nosotros. A través de la configuración de los Servicios, puede acceder y actualizar la información de su cuenta y cambiar la configuración de su perfil.

2. mailto:info@myq-solution.com

### 7.9.2 9.2 Exactitud de sus datos personales

Tomamos medidas razonables para garantizar que pueda mantener sus datos personales exactos y actualizados. Siempre puede ponerse en contacto con nosotros para obtener confirmación de si seguimos tratando sus datos personales.

Si descubre que sus datos personales tratados por nosotros son inexactos o incompletos y no puede actualizarlos de acuerdo con la sección 9.1 de esta Política de privacidad, puede solicitarnos que los actualicemos. Verificaremos su identidad y actualizaremos sus datos personales en su nombre.

### 7.9.3 9.3 Eliminación de sus datos personales

Puede solicitarnos que eliminemos sus datos personales en cualquier momento. Si nos envía dicha solicitud, eliminaremos todos sus datos personales que tengamos sin demora injustificada, siempre que sus datos personales ya no sean necesarios para la prestación de los Servicios u otros fines permitidos, en particular en relación con el ejercicio y la defensa de nuestros derechos legales, o el cumplimiento de nuestras obligaciones legales. También eliminaremos (y nos aseguraremos de que los encargados del tratamiento con los que trabajamos también lo hagan) todos sus datos personales en caso de que retire su consentimiento o en las circunstancias en que la ley nos obligue a hacerlo.

### 7.9.4 9.4 Restricción del tratamiento

Si nos solicita que restrinjamos el tratamiento de sus datos personales, por ejemplo, en circunstancias en las que impugne la exactitud, la legalidad o nuestra necesidad de tratar sus datos personales, limitaremos el tratamiento de sus datos personales al mínimo necesario (almacenamiento) y, si procede, los trataremos únicamente para el establecimiento, el ejercicio o la defensa de reclamaciones legales o, cuando sea necesario, para la protección de los derechos de otra persona física o jurídica, u otras razones limitadas dictadas por la legislación aplicable. En caso de que se levante la restricción y continuemos tratando sus datos personales, se le informará de ello sin demora injustificada.

### 7.9.5 9.5 Portabilidad de sus datos personales

Tiene derecho a recibir los datos personales que le conciernen y que nos ha facilitado. Si nos lo solicita, le proporcionaremos sus datos personales en un formato de uso común y legible por máquina sin demora injustificada desde la recepción de su solicitud. Si lo solicita, enviaremos sus datos personales a un tercero (otro

responsable del tratamiento) que usted identifique en su solicitud, a menos que dicha solicitud afecte negativamente a los derechos o libertades de otras personas y siempre que sea técnicamente posible.

### 7.9.6 9.6 Oposición al tratamiento

Tiene derecho a oponerse a que utilicemos sus datos personales sobre la base de nuestros intereses legítimos. En tal caso, dejaremos de tratar sus datos personales, salvo que demostremos motivos legítimos imperiosos para su tratamiento posterior que prevalezcan sobre sus intereses, derechos y libertades, o para el establecimiento, el ejercicio o la defensa de nuestras reclamaciones legales. Si se opone al tratamiento de sus datos con fines de marketing directo, dejaremos de tratar sus datos para estos fines.

### 7.9.7 9.7 Retirada de su consentimiento

Si nos ha dado su consentimiento para el tratamiento de datos personales, por ejemplo, para comunicaciones de marketing, puede retirar su consentimiento en cualquier momento sin indicar ningún motivo. Bloquearemos sus datos personales para cualquier tratamiento posterior. Tenga en cuenta que la retirada de su consentimiento no afecta a la legalidad de cualquier tratamiento basado en el consentimiento antes de su retirada.

### 7.9.8 9.8 Reclamación ante una autoridad de protección de datos

Tiene derecho a presentar una reclamación sobre nuestras actividades de tratamiento de datos ante Úřad pro ochranu osobních údajů, en Pplk. Sochora 2Z, 170 00 Praha 7, República Checa.

### 7.9.9 9.9 Solicitud de exclusión de la venta de datos personales en virtud de la CCPA

MyQ no vende, tal y como se define en la CCPA, ningún dato personal. Por lo tanto, si un consumidor de California comunica una solicitud de exclusión en virtud de esta disposición, no tendrá ningún efecto. Si necesita información adicional sobre sus derechos en virtud de la CCPA para excluirse de la venta de sus datos personales, póngase en contacto con: info@myq-solution.com[3].

3. mailto:info@myq-solution.com

## 7.10 10. Contacte con nosotros

Si tiene alguna pregunta sobre nuestras prácticas de recopilación y protección de datos o sobre sus derechos, no dude en ponerse en contacto con nosotros en info@myq-solution.com[4].

4. mailto:info@myq-solution.com

# 8 Tiempo de actividad del servidor, copia de seguridad de datos y recuperación en caso de desastre

## 8.1 Tiempo de actividad del servidor

MyQ Roger se compromete a mantener un objetivo de tiempo de actividad del 99,9 %; sin embargo, los acuerdos de nivel de servicio (SLA) se adaptan a cada cliente y no garantizan explícitamente esta métrica. Empleamos estrategias avanzadas de alta disponibilidad (HA), aprovechando las implementaciones multizona y las arquitecturas multipod para garantizar la continuidad del servicio y minimizar el tiempo de inactividad potencial en caso de interrupciones operativas.

## 8.2 Supervisión del estado del sistema en tiempo real

Para mejorar la transparencia y proporcionar visibilidad en tiempo real del rendimiento del sistema, mantenemos un sitio web dedicado que ofrece información actualizada sobre el estado del servicio. Esta plataforma permite a los clientes:

- **Supervisar el estado del sistema en tiempo real**: ver métricas operativas y actualizaciones de incidentes en tiempo real.
- **Recibir notificaciones proactivas**: suscribirse a alertas sobre la degradación del servicio o eventos de mantenimiento planificados.
- **Acceder a informes históricos de tiempo de actividad**: revisar incidentes pasados y tendencias de rendimiento para evaluar la fiabilidad.

Al ofrecer un sitio web centralizado sobre el estado del sistema, proporcionamos a los clientes información oportuna y precisa, lo que refuerza la confianza y permite una toma de decisiones proactiva en caso de interrupciones.

## 8.3 Estrategias de copia de seguridad

### 8.3.1 Estrategia de copia de seguridad de Azure SQL

Empleamos una estrategia de copia de seguridad georedundante para las bases de datos de Azure SQL, lo que garantiza la resiliencia y la recuperabilidad de los datos. Los aspectos clave incluyen:

- **Almacenamiento georedundante**: las copias de seguridad se replican en varias regiones para la recuperación ante desastres.
- **Política de retención**: las copias de seguridad se conservan durante varios meses, lo que permite la recuperación de datos históricos.

- **Copias de seguridad incrementales**: una ventana de recuperación en un momento dado (PITR) de 14 días permite la restauración granular de los datos perdidos.
- **Personalización basada en SLA**: los períodos de retención y los objetivos de tiempo de recuperación (RTO) varían en función de los SLA específicos del clúster y se pueden adaptar para satisfacer las necesidades del cliente.

### 8.3.2 Estrategia de copia de seguridad de Azure Cosmos DB

Para Azure Cosmos DB, implementamos mecanismos integrales de protección de datos, en particular para los registros contables, lo que garantiza la integridad y la trazabilidad de los datos:

- **Informes completos de datos contables**: todas las transacciones contables, incluida la contabilidad de trabajos de impresión, escaneo, copia y fax, se registran íntegramente.
- **Rastreo de datos históricos**: nuestro sistema permite el seguimiento y el rastreo de cualquier registro contable notificado para garantizar el cumplimiento y la auditabilidad.
- **Alta disponibilidad y redundancia**: la replicación multirregional integrada garantiza la continuidad y minimiza los riesgos de pérdida de datos.

Mediante la implementación de estas sólidas estrategias de copia de seguridad, protegemos los datos empresariales críticos y ofrecemos opciones de recuperación flexibles adaptadas a los acuerdos de nivel de servicio específicos de cada cliente.

## 8.4 Escenarios de desastre y plan de respuesta

| Escenario de desastre | Estrategia de mitigación | Proceso de recuperación |
|---|---|---|
| Corrupción de datos | PITR (recuperación a un punto en el tiempo) | Restaurar la base de datos al último estado válido conocido |
| Interrupción del servicio en la región de la nube | Copias de seguridad y conmutación por error georedundantes | Cambiar a la región secundaria de Azure |
| Fallo del nodo de Kubernetes | Réplica automática de servicios en AKS | Los pods se reprograman en nodos en buen estado |

| Escenario de desastre | Estrategia de mitigación | Proceso de recuperación |
| --- | --- | --- |
| Ciberataque (DDoS, ransomware, etc.) | WAF, protección contra DDoS de Azure y supervisión de la seguridad | Aislamiento de los sistemas comprometidos y restauración a partir de copias de seguridad limpias |

# 9 Confianza cero

## 9.1 Comprender la seguridad de confianza cero

La confianza es un concepto complejo. Por ejemplo, confío en que mi madre prepare una cena perfecta, pero nunca le confiaría la seguridad de la red. En ciberseguridad, la confianza mal depositada puede dar lugar a vulnerabilidades importantes, por lo que existe el modelo Zero Trust.

### 9.1.1 Ejemplo real: el peligro de la confianza implícita

Una de las violaciones más conocidas en las que influyó la falta de principios de confianza cero fue el **ataque a Colonial Pipeline** en 2021. Los atacantes obtuvieron acceso a través de una credencial VPN comprometida, que no tenía habilitada la autenticación multifactorial (MFA). Dado que la red confiaba implícitamente en los usuarios autenticados, los atacantes pudieron moverse lateralmente y desplegar ransomware, lo que provocó una escasez generalizada de combustible en todo Estados Unidos. Este incidente pone de relieve por qué «nunca confiar, siempre verificar» es fundamental para la ciberseguridad moderna.

## 9.2 ¿Qué es Zero Trust?

Zero Trust es un paradigma de ciberseguridad basado en el principio de «nunca confiar, siempre verificar». Garantiza que no se confíe de forma predeterminada en los usuarios y dispositivos, incluso si están conectados a una red corporativa segura o han sido verificados previamente. En su lugar, la confianza debe evaluarse y validarse continuamente basándose en diversas señales de seguridad.

### 9.2.1 Los principios básicos de Zero Trust

El «Zero Trust» se define en **la norma NIST SP 800-207** como un marco centrado en la protección de los recursos mediante la verificación continua. Este modelo de seguridad se aplica a:

- **Gestión de identidades y accesos**: garantizar que los usuarios y los dispositivos se autentiquen de forma segura.
- **Seguridad de la red y de los puntos finales**: proteger las comunicaciones y aplicar controles de acceso estrictos.
- **Protección de datos**: garantizar que los datos confidenciales se cifren y se almacenen de forma segura.

- **Supervisión continua**: detectar anomalías y responder a posibles amenazas en tiempo real.

## 9.3 Cómo se aplica Zero Trust a MyQ Roger

### 9.3.1 Verificación explícita

- Se requiere autenticación incluso en dispositivos autorizados (teléfonos/ordenadores de sobremesa).
- Utiliza estándares de autenticación modernos.
- Se aplica la autenticación multifactorial (MFA) para los inicios de sesión en dispositivos móviles e impresoras multifunción (MFP).
- Se implementa OAuth2 Device Flow para la autorización de dispositivos.
- **Los mecanismos de autenticación continua** rastrean los cambios en el comportamiento de los usuarios para detectar anomalías.

### 9.3.2 Gestión de accesos

- **El control de acceso basado en roles (RBAC)** garantiza que los usuarios solo tengan el acceso mínimo necesario.
- Se aplica **el principio del privilegio mínimo** para reducir los riesgos de seguridad.
- Se implementa **la microsegmentación** para limitar el movimiento lateral dentro de la red.
- **Los controles de acceso justo a tiempo (JIT)** ajustan dinámicamente los privilegios de los usuarios en función del contexto.

### 9.3.3 Seguridad de dispositivos y terminales

- Se emiten tokens de acceso únicos para cada tipo de dispositivo.
- La seguridad de la capa de transporte (TLS) es obligatoria para todas las comunicaciones.
- **Las soluciones de detección y respuesta en los terminales (EDR)** supervisan y analizan el comportamiento de los dispositivos.
- **El acceso a la red de confianza cero (ZTNA)** garantiza que solo los dispositivos autorizados puedan acceder a recursos específicos.

### 9.3.4 Protección de datos

- Todos los datos se almacenan de forma segura utilizando soluciones de almacenamiento cifrado.
- Las políticas garantizan que solo las entidades autorizadas puedan acceder a los datos.

- **Las soluciones de prevención de pérdida de datos (DLP)** supervisan y evitan la filtración no autorizada de datos.
- **Los enclaves seguros** protegen los datos altamente confidenciales del acceso no autorizado.

## 9.4 Abordar las amenazas cibernéticas con Zero Trust

Zero Trust ayuda a mitigar las siguientes amenazas:

- **Amenazas internas**: evita que los empleados o las cuentas comprometidas obtengan acceso no autorizado.
- **Ataques de relleno de credenciales y phishing**: reduce el impacto de las credenciales comprometidas mediante la autenticación continua.
- **Ataques de movimiento lateral**: la microsegmentación restringe el movimiento lateral de los atacantes a través de las redes.
- **Ataques a la cadena de suministro**: garantiza una verificación estricta del acceso y las integraciones de terceros.

## 9.5 Consideraciones normativas y de cumplimiento

Zero Trust se ajusta a diversas normativas y marcos de ciberseguridad:

- **ISO 27001**: impone una gestión segura del acceso y la protección de los datos.
- **RGPD**: garantiza el procesamiento y almacenamiento seguros de los datos personales.
- **HIPAA**: protege la información sanitaria confidencial.
- **Marco de ciberseguridad del NIST**: proporciona directrices para la implementación de Zero Trust.

## 9.6 Por qué es importante Zero Trust

La adopción del modelo Zero Trust minimiza el riesgo de violaciones de seguridad, amenazas internas y accesos no autorizados. En una era de crecientes amenazas cibernéticas, una arquitectura Zero Trust proporciona una protección sólida al garantizar una verificación continua y controles de acceso estrictos en todos los recursos.

Al implementar estos principios, MyQ Roger garantiza una postura de seguridad segura, resistente y adaptable que se ajusta a las mejores prácticas modernas de ciberseguridad. Además, la supervisión continua, los controles de acceso y la detección de amenazas en tiempo real mejoran la capacidad de la organización para responder de forma eficaz a las amenazas cibernéticas en constante evolución.

# 10 Inicio de sesión seguro con MyQ Roger

## 10.1 Introducción

El uso de un PIN como método principal de inicio de sesión nunca fue realmente seguro. Los primeros teléfonos móviles dependían de los PIN, pero a medida que evolucionaron las preocupaciones en materia de seguridad, también lo hicieron los métodos de autenticación. Hoy en día, la biometría se ha convertido en la norma, ya que ofrece un enfoque más seguro y fácil de usar para la autenticación.

MyQ Roger se suma a este cambio implementando la última versión de OAuth 2.0 Device Authorization Grant (antes conocida como Device Flow). Este moderno método de autenticación requiere que los usuarios inicien sesión utilizando un código QR de un solo uso escaneado con su teléfono móvil, lo que elimina la necesidad de contraseñas estáticas o PIN inseguros.

Reconocemos el teléfono móvil del usuario como uno de los medios de autenticación más seguros. Al aprovechar la autenticación biométrica para desbloquear el teléfono y, posteriormente, acceder a la aplicación MyQ, nos aseguramos de que la persona que inicia sesión es el propietario legítimo de la cuenta.

## 10.2 Autenticación segura con MyQ Roger

- **OAuth 2.0 Device Authorization Grant**: en lugar de depender de los PIN tradicionales, los usuarios se autentican utilizando un código QR generado dinámicamente. Este método reduce significativamente el riesgo de robo de credenciales o ataques de reutilización.
- **Verificación biométrica**: dado que los teléfonos inteligentes modernos requieren una verificación biométrica (por ejemplo, huella dactilar o reconocimiento facial) para desbloquearse, esto añade una capa adicional de seguridad antes de acceder a MyQ Roger.

## 10.3 Autenticación con PIN heredado

Aunque MyQ Roger sigue ofreciendo el inicio de sesión con PIN como opción, se considera un método inseguro y se desaconseja por defecto. Los usuarios que decidan habilitar la autenticación con PIN deben marcarla explícitamente como segura, reconociendo los riesgos de seguridad asociados. Además, al habilitar el inicio de sesión con PIN se desactivarán algunas funciones de seguridad avanzadas para mitigar posibles vulnerabilidades.

## 10.4 Responsabilidad en materia de seguridad

Si una organización opta por permitir el inicio de sesión basado en PIN, la responsabilidad de mantener un entorno seguro recae en el cliente. Se deben seguir las mejores prácticas, como aplicar políticas de PIN sólidas, implementar medidas de seguridad física y supervisar los registros de acceso, para minimizar los riesgos.

## 10.5 Conclusión

Con MyQ Roger, damos prioridad a la seguridad aprovechando los estándares de autenticación modernos. La adopción de la autenticación biométrica basada en dispositivos móviles garantiza una experiencia de usuario fluida y segura. Aunque el inicio de sesión basado en PIN heredado sigue estando disponible, no es el método recomendado, y los clientes deben tomar precauciones adicionales si deciden utilizarlo. Al adoptar mecanismos de inicio de sesión seguros, las organizaciones pueden mejorar tanto la seguridad como la usabilidad para sus usuarios.

# 11 Impresión segura con MyQ Roger

## 11.1 El reto de la impresión segura

Los métodos tradicionales de impresión segura se basan en conexiones físicas, como los cables LPT, en los que se asigna una impresora dedicada a un único ordenador portátil. Aunque este método garantiza el máximo nivel de seguridad, resulta poco práctico en entornos modernos que exigen flexibilidad, movilidad y recursos compartidos.

AirPrint y Mopria ofrecen funciones de impresión segura, pero son insuficientes en situaciones en las que los usuarios pueden iniciar trabajos de impresión remotos sin estar físicamente cerca de la impresora. Esto crea vulnerabilidades de seguridad, ya que los documentos confidenciales pueden quedar desatendidos.

## 11.2 MyQ Roger: una solución integral de impresión segura

MyQ Roger integra múltiples flujos de trabajo de impresión al tiempo que aplica protocolos de seguridad para garantizar que los usuarios deben estar físicamente presentes para autenticar y liberar los trabajos de impresión. El sistema garantiza que los trabajos de impresión se almacenen y transmitan de forma segura, minimizando la exposición de los datos.

## 11.3 Métodos de impresión segura en MyQ Roger

### 11.3.1 1) Impresión directa desde el PC a la impresora

- Utiliza **IPP/s (Internet Printing Protocol Secure)** para transferir los trabajos de impresión de forma segura.
- Marcas de impresoras compatibles: **Ricoh, Kyocera**.
- Los trabajos de impresión permanecen almacenados directamente en la impresora hasta que el usuario se autentica y libera el trabajo.

### 11.3.2 2) MyQ Roger Client (MRC)

- Los trabajos de impresión se **cifran y se almacenan localmente** en el PC del usuario.
- La impresora recupera el archivo cifrado **solo después de la autenticación del usuario**.
- La impresión segura se ejecuta a través de **IPP/s**.

### 11.3.3 3) Impresión en la nube

- Los archivos de impresión se almacenan de forma segura en el almacenamiento en la nube del usuario (por ejemplo, **OneDrive, Google Drive, Dropbox**).
- La impresora descarga el documento directamente desde el almacenamiento en la nube utilizando un **enlace de acceso de corta duración**.
- **No se retienen documentos** en la impresora después de la impresión, lo que garantiza la confidencialidad de los datos.

### 11.3.4 4) Integración con Microsoft Universal Print

- MyQ Roger implementa un **conector de impresión universal** que permite a las impresoras comunicarse directamente con **los servidores de impresión universal de Microsoft**.
- Los trabajos de impresión se almacenan de forma segura en **los servidores de Microsoft** y se recuperan bajo demanda tras la autenticación del usuario.
- La impresión se realiza a través de **controladores Universal Print**, lo que garantiza un manejo fluido y seguro de los trabajos.

## 11.4 Conclusión

MyQ Roger ofrece un **entorno de impresión holístico y seguro** al combinar flujos de trabajo de impresión directos, locales y basados en la nube con sólidas medidas de seguridad. Al exigir a los usuarios que se autentiquen en persona antes de la ejecución del trabajo, MyQ Roger elimina los riesgos asociados a los trabajos de impresión desatendidos, lo que garantiza la máxima protección de los datos en los lugares de trabajo modernos.

# 12 Contactos comerciales

| | |
|---|---|
| **Fabricante de MyQ®** | **MyQ® spol. s r.o.**<br>Harfa Business Center, Ceskomoravska 2532/19b, 190 00 Praga 9, República Checa<br>N.º de identificación 615 06 133<br>MyQ® spol. s r.o. está inscrita en el Registro Mercantil del Tribunal Municipal de Praga, con el número de expediente C 29842 (en lo sucesivo, «MyQ®») |
| **Información comercial** | http://www.myq-solution.com<br>info@myq-solution.com[5] |
| **Soporte técnico** | support@myq-solution.com[6] |
| **Aviso** | EL FABRICANTE NO SERÁ RESPONSABLE DE NINGUNA PÉRDIDA O DAÑO CAUSADO POR LA INSTALACIÓN O EL FUNCIONAMIENTO DEL SOFTWARE Y EL HARDWARE DE LA SOLUCIÓN DE IMPRESIÓN MyQ®.<br>Este manual, su contenido, diseño y estructura están protegidos por derechos de autor. Queda prohibida y puede ser sancionada la copia o cualquier otra reproducción total o parcial de esta guía, o de cualquier material protegido por derechos de autor, sin el consentimiento previo por escrito de MyQ®.<br>MyQ® no se hace responsable del contenido de este manual, en particular en lo que respecta a su integridad, actualidad y ocupación comercial. Todo el material aquí publicado tiene carácter exclusivamente informativo.<br>Este manual está sujeto a cambios sin previo aviso. MyQ® no está obligado a realizar estos cambios periódicamente ni a anunciarlos, y no se hace responsable de que la información publicada actualmente sea compatible con la última versión de la solución de impresión MyQ®. |

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

| | |
|---|---|
| **Marcas comerciales** | «MyQ®», incluidos sus logotipos, es una marca comercial registrada de MyQ®. Queda prohibido cualquier uso de las marcas comerciales de MyQ®, incluidos sus logotipos, sin el consentimiento previo por escrito de MyQ® Company. La marca comercial y el nombre del producto están protegidos por MyQ® y/o sus filiales locales. |

myQ roger

# AHORRE TIEMPO CON SOLUCIONES DE IMPRESIÓN PERSONALIZADAS

MyQ Roger es una solución nativa de la nube diseñada para oficinas modernas que priorizan la nube, simplificando los flujos de trabajo de documentos y permitiendo la navegación, impresión y escaneo seguros dondequiera que se encuentren los usuarios.

info@myq-solution.com

myq-solution.com


**Más de 50 millones**
de usuarios confiables

**Más de 1 millón**
de dispositivos activos

**Más de 26**
marcas compatibles

**Más de 1000**
socios certificados

Operando en más de **140** países

## Premiado y certificado

BuyersLab PLATINUM TESTED SOLUTION 2023

BuyersLab PLATINUM TESTED SOLUTION 2022

BuyersLab PLATINUM TESTED SOLUTION 2021

ISO 9001 TÜV SÜD ISO 14001 ISO/IEC 27001