Política de Segurança da Informação

Esta Política de Segurança da Informação foi atualizada pela última vez em 03/09/2025.

1. Propósito

Objetivo da Política

A presente Política de Segurança da Informação (PSI) define diretrizes para proteção dos ativos de informação da QFrotas, empresa que provê soluções tecnológicas completas para a gestão de frotas para órgãos públicos.

A Política visa garantir a confidencialidade, segurança, rastreabilidade, integridade e disponibilidade das informações, assegurando o seu uso adequado e a mitigação de riscos à segurança da informação, bem como o cumprimento das leis vigentes.

Esta política está alinhada com as boas práticas das Normas / Leis:

- ISO/IEC 27001 que estabelece os requisitos para um Sistema de Gestão de Segurança da Informação (SGSI), através de um conjunto de práticas e controles para gerenciar a segurança de suas informações e proteger seus ativos de informação, tendo como pilares a confidencialidade, integridade e disponibilidade;
- ISO/IEC 27002 que fornece diretrizes detalhadas para a implementação de controles de segurança da informação, como: controles organizacionais, controles de pessoas, controles físicos e controles tecnológicos.
- Lei Geral de Proteção de Dados (Lei nº 13.709/2018 - LGPD) que estabelece regras para garantir a proteção de dados pessoais, com o intuito de promover a segurança e privacidade dos indivíduos.

Demais objetivos desta política:

- Estabelecer orientações gerais de segurança da informação e, desta forma, contribuir para a gestão eficiente dos riscos, limitando-os a níveis aceitáveis;
- Preservar os princípios da disponibilidade, integridade, confiabilidade e autenticidade das informações;
- Estabelecer competências e responsabilidades quanto à segurança da informação;

- Promover o alinhamento das ações de segurança da informação com as estratégias de planejamento organizacional da QFrotas e do comitê de segurança e tecnologia da informação;
- Disponibilizar capacitação e treinamentos a todos os envolvidos, as fim de garantir a eficiência e aplicabilidade desta política.

2. Escopo

Aplica-se a todos os colaboradores, funcionários, contratados prestadores de serviço, usuários autorizados, credenciados, parceiros e terceiros com acesso aos sistemas, redes, aplicações, dados e informações sob responsabilidade da QFrotas.

Esta Política se aplica a todos os ativos de informações da QFrotas, incluindo dados, sistemas, aplicativos, dispositivos e redes.

Esta política se aplica em todas as instalações físicas administradas ou utilizadas pelos Órgãos e entidades subsidiárias.

3. Declarações da Política

Fica instituída a Política de Segurança da Informação da empresa QFrotas, com a finalidade de estabelecer princípios, diretrizes, responsabilidades e competências para a gestão da segurança da informação.

Esta Política de Segurança da Informação aplica-se a todos os mencionados no escopo, e deverá ser observada por todos os usuários de informação, seja servidor ou equiparado, empregado, prestador de serviços ou pessoa habilitada pela administração, por meio da assinatura de Termo de Responsabilidade, para acessar os ativos de informação sob responsabilidade deste Órgão ou entidade.

4. Princípios

As ações de segurança da informação da QFrotas são norteadas pelos princípios constitucionais e administrativos que norteiam o ordenamento jurídico brasileiro, bem como pelos seguintes princípios:

- Confidencialidade: impedir o acesso não autorizado às informações;
- Integridade: proteger a exatidão e completude das informações e métodos de processamento;

- Disponibilidade: assegurar que os usuários autorizados tenham acesso à informação e aos ativos correspondentes sempre que necessário;
- Legalidade: garantir que o tratamento de dados pessoais ocorra conforme a LGPD;
- Responsabilidade: definir obrigações claras sobre segurança para todas as partes envolvidas;
- Autenticidade das informações: garantir que dados, documentos ou informações são genuínas e não foram alteradas ou falsificadas;
- Rastreabilidade: garantir o rastreamento das ações em sistemas para investigar incidentes;
- Privacidade: Proteger não só dados pessoais, mas também metadados e informações sensíveis de colaboradores.

Também são considerados princípios desta política o respeito ao acesso à informação, à proteção de dados pessoais e à proteção da privacidade; a responsabilidade do usuário de informação pelos atos que comprometam a segurança dos ativos de informação; alinhamento estratégico da Política de Segurança da Informação com o planejamento estratégico da QFrotas, assim como demais normas específicas de segurança da informação do ordenamento jurídico brasileiro; conformidade das normas e das ações de segurança da informação com a legislação e regulamentos aplicáveis; educação e comunicação como alicerces fundamentais para o fomento da cultura e segurança da informação.

4. Diretrizes Gerais

A Política de Segurança da Informação e demais normativos decorrentes desta Política integram o arcabouço normativo da Gestão de Segurança da Informação.

A Gestão da Segurança da Informação é constituída, no mínimo, pelos seguintes processos:

- Tratamento da informação;
- Segurança física e do ambiente;
- Gestão de incidentes em segurança da informação;
- Gestão de ativos;
- Gestão do uso dos recursos operacionais e de comunicações, tais como e-mail, acesso à internet, mídias sociais e computação em nuvem;
- Controles de acesso;

- Gestão de riscos;
- Gestão de continuidade;
- Auditoria e conformidade.

4.1 Governança e Gestão de Riscos

- A segurança da informação está integrada à estratégia da organização;
- Riscos de segurança da informação serão identificados, avaliados, tratados e monitorados de forma contínua.

4.2 Acesso à Informação

- Atribuições de acesso seguirão o princípio do menor privilégio;
- A gestão de identidades será formalizada com controle de criação, alteração e revogação de acessos;
- O acesso será registrado e auditado periodicamente.

4.3 Proteção de Dados Pessoais (LGPD)

- Dados pessoais tratados no sistema terão finalidades claras e consentimento adequado quando necessário;
- Serão garantidos os direitos dos titulares de dados conforme a LGPD e política de privacidade;
- Dados pessoais serão armazenados de forma segura, com controle de acesso e criptografia.

4.4 Segurança de Sistemas e Aplicações

- Ambientes de desenvolvimento, teste e produção serão segregados;
- Mudanças devem serão controladas por processos formais (gestão de mudanças);
- Testes de segurança e auditorias devem serão realizados periodicamente.

4.5 Continuidade de Negócio e Backup

- A organização manterá planos de continuidade de serviços críticos;

- Backups serão realizados regularmente e armazenados em local seguro e redundante;
- Testes de restauração serão realizados periodicamente.

4.6 Registro e Tratamento de Incidentes

- Todos os incidentes de segurança devem ser reportados imediatamente;
- A resposta a incidentes seguirá plano formal, com registro, análise, comunicação e ações corretivas.

4.7 Segurança Física e do Ambiente

- Acesso físico aos ambientes críticos de TI serão controlados;
- Equipamentos fora de uso serão descartados de forma segura, com destruição de dados.

4.8 Capacitação

Todos os envolvidos com os sistemas e informações da QFrotas participarão de treinamentos regulares sobre segurança da informação, proteção de dados pessoais e no uso correto dos ativos de informação quando da realização de suas atribuições, de modo a minimizar possíveis riscos à segurança da informação.

A Política de Segurança da Informação e suas atualizações, bem como normas específicas de segurança da informação da QFrotas, serão divulgadas amplamente a todos os Usuários de Informação, a fim de promover sua observância, seu conhecimento, bem como a formação da cultura de segurança da informação.

As ações de capacitação serão conduzidas de modo a possibilitar o compartilhamento de materiais educacionais sobre segurança da informação.

Todos os contratos de prestação de serviços firmados conterão cláusula específica sobre a obrigatoriedade de atendimento à esta Política de Segurança da Informação, bem como se suas normas decorrentes.

5. Responsabilidades e Competências

Setor de Análise e Desenvolvimento de Sistemas

- Implementar controles técnicos e administrativos;
- Garantir conformidade com normas ISO/IEC 27001 e LGPD;
- Promover treinamentos periódicos e avaliar os riscos da informação;
- Planejar, implementar e melhorar continuamente os controles de privacidade e segurança da informação em soluções de tecnologia da informação e comunicações, considerando a cadeia de suprimentos relacionada à solução.

Usuários e Colaboradores

- Cumprir com as diretrizes desta política;
- Manter sigilo das informações acessadas;
- Reportar falhas ou incidentes de segurança.

Alta Administração

- Fornecer os recursos necessários para assegurar o desenvolvimento e a implementação da Gestão de Segurança da Informação da QFrotas, bem como com o tratamento das ações e decisões de segurança da informação em um nível de relevância e prioridade adequados;
- Formalizar e aprovar a Política de Segurança da Informação, bem como suas alterações.

Comitê de Segurança da Informação

- Assessorar na implementação das ações de segurança da informação;
- Constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre segurança da informação;
- Participar da elaboração da Política de Segurança da Informação e das normas internas de segurança da informação;

- Propor alterações à Política de Segurança da Informação e às normas internas de segurança da informação;
- Deliberar sobre normas internas de segurança da informação;
- Avaliar as ações propostas pelo gestor do comitê de segurança da informação.

O Comitê de Segurança da Informação poderá definir outros processos de Gestão de Segurança da Informação, desde que alinhados aos princípios e às diretrizes desta Política e destinados à implementação de ações de segurança da informação.

Equipe de Prevenção, Tratamento e Respostas a Incidentes Cibernéticos:

- Facilitar, coordenar e executar as atividades de prevenção, tratamento e resposta a incidentes cibernéticos na QFrotas;
- Monitorar as redes computacionais;
- Detectar e analisar ataques e intrusões;
- Tratar incidentes de segurança da informação;
- Identificar vulnerabilidades e artefatos maliciosos;
- Recuperar sistemas de informação.

6. Penalidades

O descumprimento desta política poderá resultar em advertência, suspensão, rescisão contratual, além das sanções legais previstas na LGPD e demais legislações aplicáveis.

8. Auditoria e Conformidade

A empresa poderá realizar auditorias internas e externas para verificar o cumprimento da PSI, da LGPD e das normas ISO aplicáveis.

9. Revisão e Atualização

Esta política será revista anualmente ou quando houver mudanças relevantes legais, tecnológicas ou operacionais.

Versão: 1.1

Data de Emissão: 09-2025

Responsável: Comitê de Segurança da Informação e DPO - QFrotas

Telefone: +55 41 3089-8113
E-mail: contato@qfrotas.com

Endereço: Alameda Doutor Carlos de Carvalho, 555, 12° andar
Curitiba - PR | CEP 80430-180