POLÍTICA GLOBAL DE SEGURANÇA DA INFORMAÇÃO E GOVERNANÇA DE TI

Identificação do Documento: POL-SEG-INF-002

Versão: 1.0 (Maio/2026)

Responsabilidade: Diretoria de Governança, Riscos e Compliance (GRC)

Sumário

1. DECLARAÇÃO DE PROPÓSITO E ESCOPO

A segurança da informação não é tratada como um departamento isolado na Quark, mas como o alicerce fundamental de nossa cultura e arquitetura de software. Atuamos como o elo central de confiança entre bases de dados governamentais e transportadoras, mitigando riscos por meio de tecnologia antifraude. O escopo desta política abrange todos os colaboradores, prestadores de serviço, infraestruturas de nuvem, bancos de dados relacionais e integrações via API que compõem nosso ecossistema de validação de identidades e gestão de risco.

2. REFERÊNCIAS NORMATIVAS E FRAMEWORKS DE GOVERNANÇA

Nossa arquitetura de governança e nossos controles operacionais são estruturados, auditados e mantidos sob as diretrizes dos mais rigorosos padrões globais:

- **Família ISO/IEC 27000:** Aderência aos requisitos do Sistema de Gestão de Segurança da Informação (ISO 27001), código de práticas para controles (ISO 27002), gestão de incidentes (ISO 27035), segurança em nuvem (ISO 27017) e proteção de dados em nuvem (ISO 27018).
- **ISO/IEC 27701:** Extensão do SGSI para o Sistema de Gestão de Privacidade da Informação (SGPI), alicerçando nosso *Privacy by Design*.
- **COBIT 2019:** Alinhamento estratégico entre os objetivos de negócio da Quark e a governança de TI corporativa, focando nos domínios de Avaliar, Direcionar e Monitorar (EDM).
- **ITIL v4:** Aplicação das melhores práticas em Gerenciamento de Serviços de TI (ITSM), garantindo que a gestão de mudanças e de incidentes opere com SLAs definidos e mínimo impacto operacional.
- **NIST Cybersecurity Framework (CSF):** Adoção das funções *Identify, Protect, Detect, Respond,* e *Recover* para resiliência cibernética contínua.
- **Arcabouço Legal:** Conformidade estrita com a Lei Geral de Proteção de Dados Pessoais (LGPD - Lei nº 13.709/2018) e com o *General Data Protection Regulation* (GDPR).

3. SEGURANÇA EM ARQUITETURA DE NUVEM E RESILIÊNCIA (CONTROLE 8.1 - ISO 27002)

Operamos em uma arquitetura 100% *Cloud-Native*, hospedada na Amazon Web Services (AWS) em zonas de disponibilidade redundantes e internacionais.

- **Disponibilidade e Tolerância a Falhas:** Desenhamos nossa infraestrutura para suportar o ritmo ininterrupto (24/7) do setor logístico, utilizando balanceamento de carga, escalonamento automático e replicação síncrona de bancos de dados PostgreSQL para garantir alta disponibilidade.
- **Isolamento e *Multitenancy* Seguro:** Garantimos o isolamento lógico total dos dados de nossos clientes e parceiros por meio de segmentação de redes virtuais (VPCs), sub-redes privadas e *Security Groups* restritivos, neutralizando riscos de vazamento lateral.
- **Conformidade Cross-Border:** A infraestrutura global permite transferências internacionais de dados em total conformidade com o GDPR e a LGPD, garantindo proteções jurídicas e criptográficas equivalentes ou superiores às exigidas pela legislação local.

4. CLASSIFICAÇÃO, CRIPTOGRAFIA E MINIMIZAÇÃO DE DADOS

Um dado verdadeiramente protegido é aquele que, mesmo em cenários de interceptação ou exfiltração, permanece matematicamente inútil para atores maliciosos.

- **Criptografia de Ponta a Ponta:** Toda comunicação com serviços governamentais externos de fontes públicas ou publicizadas e tráfego interno ocorre via canais TLS 1.2+ e HTTPS. O armazenamento (dados em repouso) em nossos bancos de dados utiliza o padrão AES-256.
- **Tratamento de Dados Sensíveis:** O fluxo de validação de motoristas, que abrange desde a conferência de CNHs até verificações biométricas de prova de vida (liveness), é regido pelo princípio da Minimização de Dados.
- **Segregação Funcional:** Nossos motores orquestram milhares de consultas, porém extraem e processam estritamente os metadados necessários para a composição do "Score de Risco" final. Dados brutos descartáveis não compõem armazenamentos persistentes e redundantes.

5. GESTÃO DE IDENTIDADE E ACESSO (IAM) - ABORDAGEM ZERO TRUST

Fundamentados no Controle 9.2 da ISO 27002, rechaçamos o conceito de "rede interna confiável".

- **Autenticação Robusta:** Exigimos Autenticação de Múltiplos Fatores (MFA) obrigatória para o acesso a painéis de administração, ambientes de desenvolvimento e produção. Os fluxos de identidade são geridos por soluções modernas de autenticação de usuários (ex: fluxos cognitivos de acesso).
- **Privilégio Mínimo (PoLP):** Nenhum engenheiro, desenvolvedor ou sistema de terceiro retém privilégios de administrador de forma irrestrita ou perpétua. Acessos são granulares, atrelados a funções específicas (RBAC - *Role-Based Access Control*) e revogados imediatamente após o término da necessidade de negócio.

6. SECURE DEVELOPMENT LIFECYCLE (DEVSECOPS)

A segurança não é uma etapa de verificação posterior, mas o DNA das nossas soluções logísticas e de monitoramento veicular. Seguindo os preceitos da ISO 27701 (*Privacy by Design*):

- Cada alteração no código-fonte é submetida a esteiras automatizadas de integração e entrega contínuas (CI/CD) que incluem testes de Análise Estática (SAST) e Dinâmica (DAST) contra vulnerabilidades conhecidas (OWASP Top 10).
- Realizamos auditorias periódicas e testes de intrusão (*Penetration Testing*) em nossas APIs e aplicações web para assegurar a blindagem contra injeções de SQL, *Cross-Site Scripting* (XSS) e sequestro de sessões.

7. GESTÃO DE INCIDENTES, MONITORAMENTO CONTÍNUO E RESPOSTA (CSIRT)

Agimos com a premissa de que a prontidão estruturada é o contrapeso vital à prevenção técnica. Nossa estratégia de Resposta a Incidentes (padrão ISO 27035) inclui:

- **Monitoramento em Tempo Real:** Utilizamos ferramentas de SIEM (*Security Information and Event Management*) e monitoramento de performance de infraestrutura para

identificar anomalias, picos de requisições irregulares e comportamentos atípicos em nossas APIs.

- **Comitê de Resposta Rápida (CSIRT):** Mantemos um esquadrão multidisciplinar treinado para as fases de identificação, contenção, erradicação, recuperação e análise pós-incidente, visando minimizar o *Mean Time To Recover* (MTTR).
- **Transparência e Notificação Compulsória:** Em caso de incidentes que resultem em acesso não autorizado a dados pessoais ou risco aos titulares, cumpriremos rigorosamente:
    - Notificação à Autoridade Nacional de Proteção de Dados (ANPD) no Brasil e aos titulares afetados nos prazos estipulados.
    - Observância estrita do Art. 48 da LGPD e Artigos 33 e 34 do GDPR, fornecendo dados auditáveis sobre a extensão do impacto e as contramedidas técnicas adotadas.

8. GESTÃO DE RISCOS DE TERCEIROS (SUPPLY CHAIN SECURITY)

A Quark entende que a segurança do nosso ambiente estende-se aos nossos parceiros. Fornecedores, APIs de background check e provedores de nuvem são homologados mediante *Due Diligence* de segurança e assunção de Acordos de Nível de Serviço (SLA) de segurança e Acordos de Confidencialidade (NDA).

9. AUDITORIA, CONSCIENTIZAÇÃO E RESPONSABILIDADE CORPORATIVA

- **Engajamento Humano:** Compreendemos que as mais sofisticadas barreiras perimetrais falham sem a conscientização do fator humano. Promovemos treinamentos contínuos de *Security Awareness*, simulações de *phishing* e capacitações técnicas em desenvolvimento seguro para nossa equipe.
- **Governança Ativa:** O gerenciamento do risco das operações dos nossos clientes exige a proteção inflexível do nosso principal ativo: a informação de inteligência logística. O não cumprimento das diretrizes desta política está sujeito a medidas disciplinares e legais cabíveis.

Canal de Ética, Privacidade e Resposta de Segurança (CSIRT Quark): Incidentes, requisições de titulares de dados e denúncias devem ser reportados imediatamente ao canal oficial: privacidade@idquark.io.