POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA

Quick Soft Tecnologia da Informação S.A.

---

1. OBJETIVO E ABRANGÊNCIA

Esta política tem como objetivo definir as diretrizes para assegurar a proteção das informações da Companhia, resguardando sua confidencialidade, integridade, disponibilidade, rastreabilidade e autenticidade, bem como estabelecer um padrão de segurança cibernética que minimize riscos e previna incidentes cibernéticos e de segurança da informação.

Aplica-se a todos os colaboradores, terceiros, prestadores de serviços, fornecedores e qualquer parte que tenha acesso às informações e ativos da Companhia, abrangendo a segurança de todos os sistemas, redes, dispositivos, documentos e dados tratados, independentemente da forma como são armazenados ou transmitidos.

2. PRINCÍPIOS FUNDAMENTAIS

A Companhia adota os seguintes princípios fundamentais para a segurança da informação e cibernética:

- **Confidencialidade:** Assegurar que as informações da Companhia sejam acessadas apenas por pessoas autorizadas, limitando o acesso a quem realmente precisa.
- **Integridade:** Assegurar que as informações não sejam alteradas ou manipuladas indevidamente durante seu ciclo de vida, preservando sua exatidão e confiabilidade.
- **Disponibilidade:** Garantir que os sistemas e informações estejam acessíveis sempre que necessário, prevenindo interrupções que possam comprometer as atividades da Companhia.
- **Rastreabilidade:** Manter registros detalhados (logs) de todas as atividades realizadas nos sistemas e redes da Companhia, permitindo auditorias, investigações e o monitoramento de eventos e acessos relevantes.
- **Autenticidade**: Verificar a legitimidade das informações e a identidade dos agentes que interagem com os sistemas corporativos.

3. DIRETRIZES GERAIS

3.1. Segurança Lógica

Os mecanismos de segurança lógica abrangem **procedimentos e controles específicos** para a proteção de sistemas, redes e dados, incluindo:

- **Acesso à Internet e Rede Corporativa:** Todos os acessos à internet e à rede corporativa devem ser autenticados e monitorados. O uso pessoal da internet será permitido em momentos não prejudiciais ao desempenho profissional, sendo vedado o acesso a sites de risco.
- **Autenticação e Criptografia:** Procedimentos de autenticação forte (dois ou mais fatores) serão adotados para o acesso a sistemas críticos. Todos os dados sensíveis transmitidos ou armazenados devem ser criptografados utilizando algoritmos robustos e certificados.
- **Controle de Acessos:** A Companhia implementará mecanismos de segurança, como o controle de acesso físico e digital, e a segmentação de redes. O acesso aos sistemas corporativos será limitado com base na necessidade de cada colaborador.
- **Prevenção de Vazamento de Informações e Detecção de Intrusões:** Serão implementados sistemas de Detecção e Prevenção de Intrusão (IDS/IPS) e *Data Loss Prevention* (DLP) para monitorar e mitigar riscos de vazamento ou acesso não autorizado.

Para informações complementares, acesse o Manifesto da Administração e o Glossário de Termos.

- **Realização de Testes de Segurança e Varreduras:** Testes de vulnerabilidade e Pentests serão realizados periodicamente para identificar falhas nos sistemas, bem como varreduras regulares para detecção de softwares maliciosos e outras ameaças cibernéticas.

3.2. Segurança Física

- **Ambientes Críticos:** O acesso a ambientes sensíveis, como datacenters e arquivos de documentos confidenciais, será restrito a pessoas autorizadas mediante dispositivos de controle (cartões de acesso, biometria).

- **Manuseio de Documentos Físicos:** Documentos físicos sensíveis deverão ser guardados em locais seguros, e o descarte deverá ser feito de maneira a garantir sua destruição completa, por meio de trituradores ou outros métodos que inviabilizem a recuperação da informação.

3.3. Gestão de Incidentes

A gestão de incidentes é um componente central desta política e abrange a prevenção, detecção, resposta e recuperação, abrangendo:

- **Monitoramento e Prevenção:** A Companhia implementará uma estrutura de monitoramento contínuo para detectar anomalias ou atividades suspeitas, utilizando ferramentas como DLP (*Data Loss Prevention*), IDS/IPS (*Intrusion Detection/Prevention Systems*) e antivírus. A prevenção de incidentes será garantida por atualizações periódicas de segurança, como patches e correções de vulnerabilidades.

- **Registro e Análise de Incidentes**: Todos os incidentes devem ser registrados, analisados quanto à causa raiz, impacto e extensão, conforme estabelecido pelo Plano de Ação e Resposta a Incidentes (PARI). Os registros incluirão informações recebidas de prestadores de serviços terceirizados,

- **Resposta a Incidentes:** O PARI detalha as etapas de identificação, contenção, erradicação e recuperação de incidentes. Após a contenção de um incidente, uma análise completa deve ser realizada para garantir que todos os riscos sejam mitigados e o incidente não se repita.

- **Notificação de Incidentes Relevantes:** Em caso de incidentes significativos, as partes interessadas, como clientes e órgãos reguladores, serão notificadas em tempo hábil, conforme os requisitos normativos e contratuais.

3.4. Plano de Continuidade de Negócios (PCN)

O PCN deverá garantir a continuidade das operações críticas em caso de falhas ou incidentes, considerando:

- **Cenários de Incidentes:** O plano incluirá cenários de incidentes considerados nos testes de continuidade de negócios e operações, abrangendo riscos significativos, como interrupções de larga escala e falhas em sistemas críticos.

- **Backup e Recuperação de Desastres:** Backups serão realizados periodicamente e testados para assegurar sua integridade. Data centers alternativos estarão preparados para ativação em caso de incidentes.

3.5. Prestadores de Serviços Terceirizados

A Companhia implementará diretrizes específicas para prestadores de serviços terceirizados:

- **Procedimentos e Controles:** Os prestadores de serviços devem adotar controles de segurança compatíveis com os padrões estabelecidos pela Companhia, sendo responsáveis por implementar medidas de prevenção e resposta a incidentes cibernéticos. Auditorias periódicas serão realizadas para garantir a conformidade.

Para informações complementares, acesse o Manifesto da Administração e o Glossário de Termos.

- **Classificação e Proteção de Dados:** Todos os prestadores deverão classificar as informações conforme sua relevância e garantir a adoção de mecanismos de proteção adequados, como criptografia e controle de acesso.

4. CONSCIENTIZAÇÃO E TREINAMENTO

Treinamentos periódicos serão realizados para capacitar os colaboradores sobre boas práticas de segurança da informação e cibernética, incluindo um programa de conscientização contínuo com foco em riscos cibernéticos, proteção de dados e privacidade.

5. GESTÃO DE RISCOS E CONFORMIDADE

A Companhia conduzirá análises periódicas de riscos para identificar e mitigar riscos relacionados à segurança da informação e cibernética, em conformidade com as normativas de supervisão vigentes e as melhores práticas do mercado.

6. CONTROLE DOCUMENTAL

Esta política será revisada periodicamente, e sempre que necessário, para garantir sua eficácia e adequação às mudanças normativas, à evolução das melhores práticas de governança corporativa e às necessidades específicas da Companhia.

Responsável	Controle de Revisões	
CEO	Versão Atual	1.0
	Data da Aprovação	16/10/2024
	Versão Anterior	-
	Ata de Aprovação	Conselho de Administração

Principais Modificações	Legislações e Documentos Relacionados
- Criação da política	- Resolução 304/2023 BCB

Para informações complementares, acesse o Manifesto da Administração e o Glossário de Termos.