

Política de Segurança da Informação

1. Objetivo

O objetivo da Política de Segurança da Informação ("Política") é estabelecer diretrizes, responsabilidades e princípios gerais de segurança da informação e Cibernética com objetivo de manter a confidencialidade, integridade, disponibilidade, autenticidade, irretratabilidade dos ativos de informação da Raízen S.A. ("Raízen" ou "Companhia"), observando as melhores práticas de mercado em conformidade com as regulamentações aplicáveis.

2. Diretrizes

A segurança da informação na Raízen é baseada em cinco pilares essenciais:

- **Confidencialidade:** Restringir o acesso à informação e ativos de informação somente aos usuários, processos e dispositivos autorizados, prevenindo divulgação, exposição ou uso indevido.
- **Disponibilidade:** Manter a informação e os ativos de informação disponíveis aos usuários autorizados sempre que necessário, durante todo o seu ciclo de vida;
- **Integridade:** Manter as informações e os ativos de informação íntegros e completos, protegendo-os contra alterações, exclusões ou inserções não autorizadas decorrentes de falhas;
- **Autenticidade:** Validar a origem e a propriedade da informação, confirmando que ela procede da fonte declarada e permanece inalterada durante o processo estabelecido.
- **Irretratabilidade (não repúdio):** Implementar mecanismos que permitam rastrear e comprovar a origem, o envio e o recebimento de informações, prevenindo a negação de autoria ou responsabilidade.

3. Aspectos Gerais

- A proteção das informações e dos ativos corporativos deve ser considerada em todos os processos e áreas de negócio.
- As informações e ativos da Raízen devem ser protegidos de acordo com seu nível de criticidade e impacto ao negócio, em conformidade com a legislação vigente, normas internas e apenas para a finalidade para a qual foram coletadas.
- A Raízen adota medidas para promover o uso seguro de recursos tecnológicos, com monitoramento e rastreabilidade sempre que necessário.
- Tecnologias, metodologias e dados corporativos não devem ser compartilhados ou utilizados para fins pessoais, salvo autorização expressa.

4. Classificação da Informação

- As informações são classificadas conforme seu grau de sensibilidade, impacto ao negócio e necessidade de proteção, podendo ser classificadas como: Pública, Interna, Confidencial ou Restrita. Cada colaborador é responsável pela correta classificação das informações que gera ou manipula.

5. Proteção de Dados Pessoais e Dados Sensíveis

- A Raízen possui um Programa de Privacidade e Proteção de Dados alinhado à Lei Geral de Proteção de Dados (LGPD), com ações estruturadas de governança, gestão de riscos e cultura de privacidade em toda a organização.

6. Segurança Cibernética

- São adotadas boas práticas e soluções de mercado para proteger os ativos digitais da organização, incluindo autenticação de usuários, criptografia, prevenção contra acessos não autorizados, proteção contra malwares, monitoramento de atividades, segregação de redes e gestão de vulnerabilidades.

7. Gestão de Incidentes e Riscos

- A companhia mantém processos estruturados para identificar, avaliar e tratar riscos de segurança da informação, bem como procedimentos específicos para resposta a incidentes em ambientes de tecnologia e negócio.

8. Treinamento e Conscientização

- Por meio do Programa Guardião, a Raízen promove capacitação contínua e ações de aculturação sobre segurança da informação, envolvendo todos os níveis da organização.

9. Segurança na Contratação de Fornecedores

- Fornecedores e parceiros devem cumprir com os requisitos de segurança da informação definidos pela Raízen, inclusive em contratos e avaliações de risco, de forma a manter o alinhamento com boas práticas de mercado.

10. Melhoria Contínua

- A Raízen compromete-se com a melhoria contínua de seus processos, controles e diretrizes de segurança da informação, promovendo revisões periódicas desta Política e de seus desdobramentos, a fim de manter sua eficácia, aderência às melhores práticas do mercado, evolução tecnológica e conformidade com requisitos legais e regulatórios aplicáveis.

11. Canal de Dúvidas e Denúncias

Colaboradores, parceiros e terceiros podem reportar dúvidas ou indícios de descumprimento desta Política por meio dos canais oficiais, preservando a confidencialidade e proteção contra retaliações.