Política de Segurança da Informação

reAvalie LTDA

Aprovações		
Nome	Designação	Data e Assinatura.
Mateus Albuquerque	Diretor	
Mateus Albuquerque	CEO / Signatário Autorizado	
		Date: 28.11.2024

1. Objetivo

Estabelecer diretrizes, responsabilidades e procedimentos para garantir a proteção dos ativos de informação da plataforma reAvalie, assegurando a confidencialidade, integridade, disponibilidade e autenticidade dos dados tratados.

2. Âmbito de Aplicação

Esta política aplica-se a todos os usuários cadastrados (avaliadores e empresas), colaboradores, executivos e administradores, parceiros, fornecedores e prestadores de serviços com acesso a informações, toda a infraestrutura tecnológica, sistemas, aplicativos, bancos de dados e ambientes físicos da organização.

3. Definições

Informação: Conjunto de dados que possuem valor para a organização.
Ativo de Informação: Qualquer recurso que armazene, processe ou transmita informação.
Titular de Dados: Pessoa natural a quem se referem os dados pessoais tratados.
Incidente de Segurança: Evento adverso real ou potencial que comprometa a proteção da informação.

4. Princípios de Segurança

A proteção da informação é baseada nos seguintes princípios:
Confidencialidade: Garantir que a informação esteja disponível apenas para pessoas autorizadas.
Integridade: Proteger a precisão e a completude da informação.
Disponibilidade: Garantir que usuários autorizados tenham acesso à informação quando necessário.
Autenticidade: Assegurar a identidade de quem cria, modifica ou acessa dados.

5. Diretrizes de Segurança

5.1 Gestão de Acessos

Princípio do mínimo privilégio: acesso apenas ao necessário para a função.
Autenticação de dois fatores (2FA) para usuários administradores.
Controle de senhas com padrões de complexidade e expiração.

5.2 Proteção de Dados

Criptografia de dados em trânsito (TLS 1.2 ou superior) e em repouso.

Armazenamento de senhas utilizando algoritmos de hashing (bcrypt, scrypt ou equivalente).

Segregação de ambientes (produção, desenvolvimento e testes).

5.3 Monitoramento e Resposta

Monitoramento contínuo de atividades e eventos de segurança.

Sistema de detecção de intrusão (IDS) e resposta a incidentes (SIEM).

Planos de resposta e recuperação de incidentes (IRP).

5.4 Gestão de Riscos

Avaliação periódica de riscos e vulnerabilidades.

Implementação de controles mitigatórios baseados em frameworks internacionais (ex: ISO 27001, NIST).

5.5 Continuidade de Negócios

Manutenção de Plano de Continuidade de Negócios (PCN).

Procedimentos de backup automatizados, testados regularmente.

Estratégias de Disaster Recovery em ambientes redundantes.

5.6 Treinamento e Conscientização

Programas regulares de treinamento em segurança para colaboradores e prestadores de serviço.

Campanhas de sensibilização para práticas seguras de navegação e manipulação de dados.

5.7 Auditoria e Conformidade

Auditorias internas e externas anuais de segurança da informação.

Compliance com legislações aplicáveis, incluindo: Lei Geral de Proteção de Dados (LGPD), General Data Protection Regulation (GDPR), Marco Civil da Internet (Brasil) e Children's Online Privacy Protection Act (COPPA), se aplicável.

6. Proteção contra Ameaças

Implementação de soluções de antivírus, antimalware e firewall de nova geração.

Proteção contra ataques DDoS.

Monitoramento de vulnerabilidades conhecidas (CVEs) e aplicação rápida de patches de segurança.

7. Gestão de Incidentes de Segurança

Definição clara de papéis e responsabilidades na resposta a incidentes.

Comunicação imediata de incidentes críticos aos titulares de dados afetados, conforme obrigação legal.

Manutenção de registros completos de todos os incidentes de segurança.

8. Proteção de Dados Pessoais

Tratamento de dados pessoais limitado à finalidade para a qual foram coletados.

Consentimento expresso e informado dos titulares, quando necessário.

Garantia de direitos dos titulares: acesso, correção, exclusão e portabilidade dos dados.

9. Responsabilidades

Usuários:

Zelar pela confidencialidade de suas credenciais.

Cumprir os Termos de Uso e demais políticas de segurança da plataforma.

Colaboradores:

Manter sigilo sobre informações acessadas no exercício de suas funções.

Reportar imediatamente qualquer suspeita de incidente de segurança.

Fornecedores e Parceiros:

Cumprir com cláusulas contratuais de confidencialidade e segurança da informação.

Submeter-se às políticas de segurança aplicáveis.

10. Sanções

O descumprimento desta política poderá resultar em advertências, suspensão de acesso, rescisão contratual e ações judiciais para reparação de danos.

11. Transferência Internacional de Dados

Os dados poderão ser transferidos para servidores fora do país de origem, observando-se garantias adequadas de proteção, adoção de cláusulas contratuais padrão e consentimento explícito do titular de dados, quando necessário.

12. Atualização e Revisão
Esta política será revisada anualmente ou em caso de mudanças relevantes no ambiente regulatório ou tecnológico.
Última atualização: 28.11.2024.

13. Contato
Para dúvidas, solicitações ou denúncias de incidentes de segurança:
E-mail: seguranca@reavalie.com