



DOCUMENTO 07 · SEGURANÇA

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Esta Política estabelece os princípios, os controles e as responsabilidades adotados pela Rede Buscador para proteger a confidencialidade, a integridade e a disponibilidade das informações e dos Sistemas que mantém.

VIGENTE DESDE 14 DE SETEMBRO DE 2026 · VERSÃO 1.0

A FONTE PÚBLICA. A REDE APURA. VOCÊ GANHA TEMPO.

EMITENTE

REDE BUSCADOR TECNOLOGIA E COMUNICAÇÃO
LTDA.

SEDE

Rua da Bahia, nº 1148, sala 1208, Centro, Belo
Horizonte, Minas Gerais, CEP 30160-906

CNPJ · INSCRIÇÃO MUNICIPAL

69.040.312/0001-25 · 1.812.949/001-9

VERSÃO PÚBLICA

redebuscador.com.br/seguranca

IDENTIFICAÇÃO E ABRANGÊNCIA

Esta Política é adotada pela **REDE BUSCADOR TECNOLOGIA E COMUNICAÇÃO LTDA.**, sociedade empresária limitada inscrita no CNPJ sob o nº 69.040.312/0001-25 e na Prefeitura de Belo Horizonte sob a inscrição municipal nº 1.812.949/001-9, com sede na Rua da Bahia, nº 1148, sala 1208, Centro, Belo Horizonte, Minas Gerais, CEP 30160-906, doravante denominada "Rede Buscador".

Aplica-se a todos os Sistemas, às bases de dados, aos ambientes de desenvolvimento e produção e a todas as pessoas e fornecedores que tenham acesso a eles. Complementa a Política de Privacidade e o Código de Conduta e Integridade.

PRINCÍPIOS

- **Confidencialidade, integridade e disponibilidade:** a informação é acessível somente a quem está autorizado, mantém-se exata e completa e permanece disponível quando necessária;
- **Segurança desde a concepção:** requisitos de segurança são considerados desde o projeto de cada funcionalidade;
- **Defesa em profundidade:** a proteção é organizada em camadas independentes, de modo que a falha de um controle não comprometa o conjunto;
- **Menor privilégio:** cada pessoa, processo e integração recebe somente o acesso indispensável à sua função;
- **Minimização de dados:** dados pessoais são coletados apenas quando necessários, o que reduz a superfície de exposição.

REFERÊNCIAS

Os controles desta Política são orientados pelo artigo 46 da Lei nº 13.709/2018, pelas boas práticas das normas ABNT NBR ISO/IEC 27001 e 27002 e pelas listas OWASP Top 10 e OWASP API Security Top 10, publicadas pela OWASP Foundation. A adoção dessas referências não constitui declaração de certificação.

DESENVOLVIMENTO SEGURO

- as funcionalidades são revisadas com base nas categorias de risco do OWASP Top 10 e do OWASP API Security Top 10, incluindo controle de acesso, falhas criptográficas, injeção, configuração insegura e autenticação;
- as entradas de dados são validadas e as consultas a bancos de dados são parametrizadas;
- as páginas adotam política de segurança de conteúdo que restringe a execução de código a origens autorizadas;

- componentes externos são incorporados de origem controlada, sem carregamento de código de terceiros não declarado;
- credenciais e chaves de integração são mantidas fora do código-fonte, em repositórios cifrados;
- alterações passam por verificações automatizadas antes da publicação.

05

PROTEÇÃO DAS COMUNICAÇÕES

Todo o tráfego entre os Usuários e os Sistemas é cifrado por protocolo seguro, com redirecionamento obrigatório de conexões não cifradas e política de transporte estrito. Os Sistemas enviam cabeçalhos de segurança que restringem o enquadramento das páginas por terceiros, a interpretação indevida de conteúdo e o compartilhamento de informações de navegação.

06

CONTROLE DE ACESSO E AUTENTICAÇÃO

- o acesso de Usuários à Área Restrita é feito por código de uso único enviado ao endereço eletrônico cadastrado, com prazo de validade curto e limite de tentativas, sem armazenamento de senha;
- as sessões expiram automaticamente e são mantidas em identificadores protegidos contra leitura por código de terceiros;
- as funções administrativas são restritas a pessoas previamente autorizadas, com verificação de permissão em cada operação;
- o acesso administrativo aos servidores exige chave criptográfica, sem autenticação por senha.

07

PROTEÇÃO DOS DADOS ARMAZENADOS

Códigos de acesso e demais credenciais são armazenados de forma cifrada e irreversível. Os dados são mantidos em provedores de infraestrutura que aplicam criptografia em repouso e detêm certificações de segurança reconhecidas internacionalmente. Registros técnicos são produzidos com mascaramento de dados pessoais.

08

SEGURANÇA DE PAGAMENTOS

- os pagamentos são realizados no ambiente da ASAAS Gestão Financeira Instituição de Pagamento S.A., instituição de pagamento autorizada pelo Banco Central do Brasil e aderente ao padrão de segurança da indústria de cartões de pagamento (PCI DSS);
- os dados de cartão são informados exclusivamente nesse ambiente e não trafegam pelos Sistemas nem são armazenados pela Rede Buscador;

- a confirmação de pagamento é recebida por notificação autenticada da instituição de pagamento e registrada em trilha própria;
- a liberação de funcionalidades contratadas depende da confirmação do pagamento pela instituição de pagamento.

09

PROTEÇÃO CONTRA ABUSO E ATAQUES

- mitigação de ataques de negação de serviço e de tráfego automatizado malicioso na camada de distribuição de conteúdo;
- limites de frequência de requisições, mais restritivos nas operações sensíveis;
- bloqueio automático de origens com tentativas repetidas de acesso indevido;
- exposição mínima de serviços, com portas de acesso restritas ao estritamente necessário.

10

MONITORAMENTO, REGISTROS E AUDITORIA

A disponibilidade dos Sistemas e a execução das rotinas de atualização de dados são monitoradas continuamente, com alertas automáticos em caso de falha. As correções de segurança dos servidores são aplicadas de forma contínua.

- **Trilhas de auditoria:** ações administrativas, acessos às contas da Área Restrita e eventos de pagamento são registrados com data, hora e identificação de quem os realizou, permitindo a reconstrução de operações;
- **Registros de falhas:** erros de aplicação são registrados, classificados e analisados para correção da causa;
- **Proteção dos registros:** os registros têm acesso restrito, são conservados pelo tempo necessário à sua finalidade e observam o mascaramento de dados pessoais;
- **Revisões de segurança:** os Sistemas são submetidos a revisões periódicas de segurança, incluindo análise do código e testes que simulam a atuação de um atacante, sempre que há alteração relevante.

11

RESILIÊNCIA E CONTINUIDADE

- **Arquitetura distribuída:** as páginas de consulta são geradas previamente e entregues por rede de distribuição com presença em diversas regiões, o que reduz a dependência de um ponto único de falha;
- **Cópias de segurança:** as bases de dados são copiadas periodicamente, em frequência compatível com a criticidade de cada uma. As cópias são armazenadas em mais de um provedor, incluindo local independente da infraestrutura principal, com cifragem das informações sensíveis;

- **Recuperação de desastres:** a Rede Buscador mantém plano de recuperação com procedimentos por cenário de falha e objetivos definidos de tempo e de ponto de recuperação;
- **Código-fonte:** o código dos Sistemas é mantido em repositórios com cópia em provedor independente.

12

GESTÃO DE VULNERABILIDADES

Vulnerabilidades identificadas em revisões internas, em componentes utilizados ou por comunicação externa são avaliadas conforme a gravidade e corrigidas com prioridade proporcional ao risco.

Pesquisadores e Usuários podem comunicar vulnerabilidades a compliance@redebuscador.com.br, nos termos da cláusula de comunicação de vulnerabilidades do [Código de Conduta e Integridade](#).

13

RESPOSTA A INCIDENTES

Incidentes de segurança são tratados nas etapas de identificação, contenção, eliminação da causa, recuperação e registro das lições aprendidas. Quando o incidente puder acarretar risco ou dano relevante aos titulares de dados pessoais, a Rede Buscador comunicará a Autoridade Nacional de Proteção de Dados e os titulares afetados, nos termos do artigo 48 da Lei nº 13.709/2018.

14

FORNECEDORES

Os fornecedores que tratam informações em nome da Rede Buscador são selecionados considerando suas práticas de segurança e certificações. Sujeitam-se a obrigações contratuais de confidencialidade e proteção de dados. A relação de operadores de dados pessoais consta da [Política de Privacidade](#).

15

RESPONSABILIDADES E REVISÃO

A administração da Rede Buscador é responsável pela aplicação desta Política e a revisa sempre que houver alteração relevante nos Sistemas, na infraestrutura, no cenário de ameaças ou na legislação aplicável. A data de vigência e a versão constam do início do documento.

Informações adicionais para processos de avaliação de fornecedores podem ser solicitadas em contato@redebuscador.com.br.