CLASSIFICAÇÃO DA INFORMAÇÃO: PÚBLICA

Pode ser acessada por qualquer pessoa dentro ou fora da Infosimples.

INFOSIMPLES

PSI - Política de Segurança da Informação

29/04/2025

Infosimples Processamento de Dados LTDA
Avenida Paulista, 1636, sala 1504, CEP 01310-200, Bela Vista, São Paulo, SP.
privacidade@infosimples.com.br

1. OBJETIVO

Esta **Política de Segurança da Informação (PSI)** define diretrizes gerais que nortearão a conduta da Infosimples como organização e também dos seus colaboradores visando o tratamento seguro de ativos, computacionais ou não, e informações no âmbito da empresa, promovendo, assim, a segurança da própria empresa, dos seus colaboradores, clientes, fornecedores e da sociedade.

A Infosimples está comprometida com a manutenção da confidencialidade, integridade e disponibilidade de suas informações, implementando medidas de segurança técnicas e organizacionais para proteger informações contra acesso, uso, divulgação, alteração ou destruição não autorizados.

2. ABRANGÊNCIA

Esta política é aplicável à Infosimples, aos seus sócios, colaboradores, fornecedores, consultores, prestadores de serviços e parceiros.

3. PRINCÍPIOS

A preservação da segurança da informação é caracterizada aqui pela manutenção dos seguinte pilares:

- **Confidencialidade:** garantia de que a informação seja acessada somente pelas pessoas para as quais é destinada, que possuam as devidas autorizações.
- **Integridade:** garantia de que a informação esteja completa e não sofra alterações indevidas, de forma acidental ou intencional.
- **Disponibilidade:** garantia de que a informação esteja acessível sempre que necessário às pessoas autorizadas.
- **Legalidade:** cumprimento da legislação vigente e atendimento às boas práticas de segurança da informação.

4. DIRETRIZES

1. Operar de forma ética, moral, em concordância com a legislação vigente e atender às boas práticas de segurança da informação e de tratamento de

dados, inclusive os pessoais. Toda conduta na empresa deve ser pautada com esta base.
2. O acesso a qualquer sistema ou informação deve ser concedido mediante comprovação de necessidade, autorização, com o menor privilégio e pelo menor tempo possível.
3. Os colaboradores devem seguir as orientações da empresa no que diz respeito aos seus acessos, uso de múltiplo fator de autenticação, uso de recursos com licenças adequadas, treinamentos (LGPD, princípios de segurança da informação, direitos humanos, trabalho, ambiental e anticorrupção), confidencialidade e demais pontos pertinentes.
4. Manter logs, restritos e protegidos, dos sistemas de produção que permitam investigar eventuais incidentes.
5. Manter backups dos sistemas de produção que sejam suficientes para restabelecer a operação da empresa em caso de incidentes.
6. Criptografar dados em repouso ou em trânsito/uso sempre que possível. Manter dados armazenados apenas pelo mínimo período necessário, considerando os limites da legislação.
7. Monitorar o ambiente de produção e atuar em todas as atividades atípicas e/ou suspeitas envolvendo informações, reportando sempre que necessário para as autoridades competentes.
8. Seguir os princípios e diretrizes de segurança durante o desenvolvimento de software ou adoção de novas tecnologias, ferramentas, recursos ou fornecedores.
9. Classificar informações de acordo com o seu nível de proteção necessário, dando visibilidade à sua correta manipulação.
10. Manter um Plano de Continuidade de Negócios (PCN) para que, na eventualidade de um incidente, a empresa esteja apta a responder rapidamente, restaurar sua operação crítica e dar continuidade aos seus negócios.
11. Revisar a PSI pelo menos anualmente.

5. RECOMENDAÇÕES PARA CLIENTES

1. Utilizar senhas complexas, sem informações pessoais na composição, que não estejam em uso em outros serviços e mantê-las armazenadas em um cofre de senhas protegido. Fazer a alteração da senha sempre que houver qualquer indício ou suspeita de comprometimento.
2. Sempre habilitar autenticação de dois fatores.

3. Ajustar as permissões de acesso de todos os usuários vinculados à conta, restringindo sempre o acesso ao menor conjunto possível de informações.
4. Ter atenção no uso dos tokens (chave de autenticação para uso das APIs) da conta, não os mantendo em texto aberto em repositórios de código (Git, SVN, Mercurial, etc) privados e especialmente públicos (GitHub, Bitbucket, etc), não os deixando expostos em integrações através de frontend e não os enviando via e-mail ou aplicativos de troca de mensagens, nem mesmo para a Infosimples.
5. Utilizar a ferramenta de compartilhamento seguro de informações da Infosimples para troca de informações com o setor suporte da empresa.
6. Atuar de forma ética e moral, adotar boas práticas de segurança da informação e cumprir a legislação na condução dos seus negócios, garantindo que qualquer integração com serviços da Infosimples aconteçam nessas bases.