POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Governança · Compliance · Integridade

Documento	PSI-001 — Política de Segurança da Informação
Versão	1.0
Data de emissão	Julho/2026
Próxima revisão	Julho/2027
Classificação	Pública
Aprovado por	Giovani Cusinato — Diretor
Documento raiz	COD-001 — Código de Ética e Conduta

1. OBJETIVO

Estabelecer princípios, diretrizes e responsabilidades para a proteção das informações da FreeNetworks e de seus clientes, em escritório e em campo. Esta é a política de referência de segurança da informação da empresa, da qual derivam procedimentos específicos.

2. ABRANGÊNCIA

- Colaboradores de qualquer vínculo, prestadores e terceiros com acesso a sistemas ou informações;
- Sistemas administrativos, e-mail, armazenamento em nuvem e estações de trabalho;
- Equipamentos de campo: notebooks de comissionamento, instrumentos configuradores, mídias e dispositivos móveis;
- Informações de clientes sob custódia da FreeNetworks, incluindo projetos e documentação de infraestruturas críticas e sistemas de videomonitoramento.

3. PRINCÍPIOS

A FreeNetworks adota os pilares de confidencialidade (informação acessível apenas a autorizados), integridade (informação íntegra e fiel) e disponibilidade (informação acessível quando necessária), aplicados por meio de controle de acesso, autenticação, cópias de segurança e registro de atividades.

4. CLASSIFICAÇÃO DA INFORMAÇÃO

Nível	Descrição	Exemplos
Pública	Divulgação livre.	Site, materiais comerciais publicados.
Interna	Uso interno; divulgação causa baixo impacto.	Comunicados, procedimentos operacionais.
Confidencial	Divulgação causa impacto relevante à empresa ou a clientes.	Propostas, contratos, dados de colaboradores.
Restrita	Divulgação causa impacto grave; acesso mínimo e controlado.	Projetos de subestações e redes de clientes, diagramas de teleproteção, credenciais, imagens de CFTV.

Documentação técnica de infraestrutura crítica de clientes — plantas, diagramas unifilares, configurações de teleproteção e telecom — é classificada, no mínimo, como Restrita, e somente circula com autorização do cliente.

5. CONTROLE DE ACESSO E CREDENCIAIS

- Acessos seguem o princípio do menor privilégio e são individuais e intransferíveis;
- Autenticação multifator (MFA) é obrigatória em e-mail, nuvem e sistemas críticos;
- Senhas fortes e únicas por sistema, com uso de gerenciador de senhas corporativo;
- Acessos são revisados periodicamente e revogados imediatamente no desligamento;
- Credenciais de acesso a sistemas de clientes são pessoais, usadas somente no escopo contratado e devolvidas/revogadas ao término.

6. SEGURANÇA EM CAMPO

- Notebooks e instrumentos com dados de clientes usam cifragem de disco e bloqueio automático;
- É vedado conectar equipamentos não autorizados às redes de clientes, ou mídias de origem desconhecida aos equipamentos da empresa;
- Configurações e backups de equipamentos de clientes são armazenados nos repositórios corporativos, nunca em contas pessoais;
- Perda ou furto de equipamento é comunicado imediatamente como incidente de segurança (PSI-003).

7. BACKUP E RETENÇÃO

Informações corporativas são armazenadas nos repositórios oficiais em nuvem, com cópias de segurança automáticas e testes periódicos de restauração. Documentos são retidos pelos prazos legais e contratuais aplicáveis e descartados de forma segura.

8. RESPONSABILIDADES

A Diretoria patrocina a política e designa o responsável pela segurança da informação; gestores asseguram a aplicação em suas equipes; cada colaborador protege as credenciais e informações sob seu uso e reporta incidentes imediatamente.

9. VIGÊNCIA E REVISÃO

Esta política entra em vigor na data de sua aprovação e será revisada anualmente, ou antes disso sempre que mudanças legais, contratuais ou operacionais o exigirem. Casos omissos serão deliberados pela Diretoria.

10. CONTROLE DO DOCUMENTO

Versão	Data	Descrição	Autor
1.0	Julho/2026	Emissão inicial, com base na estrutura do programa de políticas da Blucom adaptada à FreeNetworks.	Giovani Cusinato — Diretor