POLÍTICA DE GESTÃO DE INCIDENTES E CONTINUIDADE

Governança · Compliance · Integridade

Documento	PSI-003 — Política de Gestão de Incidentes e Continuidade
Versão	1.0
Data de emissão	Julho/2026
Próxima revisão	Julho/2027
Classificação	Pública
Aprovado por	Giovani Cusinato — Diretor
Documento raiz	PSI-001 — Política de Segurança da Informação

1. OBJETIVO

Definir o processo de resposta a incidentes de segurança e operacionais e as diretrizes de continuidade dos serviços da FreeNetworks, incluindo os contratos com níveis de serviço (SLA) de manutenção e operação.

2. DEFINIÇÕES

Incidente é qualquer evento que comprometa, ou possa comprometer, a segurança das informações, a integridade das pessoas, a disponibilidade dos serviços prestados ou o cumprimento de obrigações contratuais. Quase acidentes e eventos de SSMA seguem também a política SSMA-001; incidentes com dados pessoais seguem também a PSI-002.

3. CLASSIFICAÇÃO DE SEVERIDADE

Severidade	Critério	Exemplos
Crítica	Risco à vida, indisponibilidade total de serviço essencial ao cliente ou vazamento confirmado de dados.	Acidente com afastamento; rompimento de backbone; comprometimento de credenciais de sistemas de cliente.
Alta	Serviço degradado com impacto relevante ou risco de descumprimento de SLA.	Falha parcial de sistema de CFTV; perda de equipamento com dados.
Média	Impacto limitado, sem afetar obrigações contratuais.	Falha de equipamento com redundância; indisponibilidade breve de sistema interno.
Baixa	Evento pontual sem impacto em clientes.	Tentativas de phishing bloqueadas; falha de estação individual.

4. PROCESSO DE RESPOSTA

- Detecção e comunicação imediata ao responsável designado;
- Registro do incidente com data, descrição, sistemas e pessoas afetadas;
- Classificação de severidade e acionamento dos protocolos específicos (SSMA-001 para pessoas, PSI-002 para dados pessoais);
- Contenção e correção, com comunicação ao cliente nos prazos contratuais quando serviços forem afetados;
- Encerramento com registro de causa raiz e lições aprendidas; incidentes Críticos e Altos são analisados pela Diretoria.

5. CONTINUIDADE DE NEGÓCIO

A FreeNetworks identifica como processos críticos: o atendimento aos contratos com SLA, a disponibilidade de equipes de campo habilitadas, o acesso aos sistemas e repositórios corporativos e a disponibilidade de materiais sobressalentes.

- Equipes: manutenção de mais de um profissional habilitado por competência crítica e documentação de procedimentos, reduzindo dependência de pessoas-chave;
- Materiais: estoque mínimo de sobressalentes definidos por contrato de manutenção;
- Sistemas: repositórios em nuvem com backup e possibilidade de trabalho remoto;
- Fornecedores críticos: alternativas homologadas para insumos e serviços essenciais (INT-004).

6. COMUNICAÇÃO EM CRISE

Em eventos que afetem serviços contratados, o gestor do contrato comunica o cliente com transparência: o que ocorreu, impacto, ações em curso e previsão de restabelecimento, com atualizações periódicas até a normalização.

7. TESTES E MELHORIA

O plano de continuidade é revisado anualmente e exercitado por meio de simulados ou testes de mesa. As lições de incidentes reais alimentam a revisão das políticas e procedimentos.

8. RESPONSABILIDADES

A Diretoria aprova o plano e os investimentos de resiliência; os gestores de contrato conduzem a comunicação com clientes; todos os colaboradores comunicam incidentes imediatamente pelos canais internos.

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