POLÍTICA DE GESTÃO DE VULNERABILIDADES

---

1. Objetivo

Estabelecer diretrizes para identificação, classificação, tratamento, mitigação e acompanhamento de vulnerabilidades nos ativos de tecnologia da informação da CREDLEVE, reduzindo riscos à disponibilidade, integridade e confidencialidade das informações.

---

2. Abrangência

Esta política aplica-se a todos os ativos tecnológicos da CREDLEVE, incluindo:

- Servidores;
- Estações de trabalho;
- Equipamentos de rede;
- Sistemas internos;
- Aplicações Web;
- Serviços em nuvem;
- Dispositivos utilizados nas operações da empresa.

---

3. Objetivos Específicos

A Gestão de Vulnerabilidades tem como objetivos:

- Identificar vulnerabilidades de segurança;
- Reduzir riscos tecnológicos;
- Manter sistemas atualizados;
- Corrigir falhas conhecidas;
- Minimizar a superfície de ataque;
- Promover a melhoria contínua dos controles de segurança.

---

4. Responsabilidades

Tecnologia da Informação

Compete à equipe de TI:

- Identificar vulnerabilidades;
- Avaliar os riscos;
- Definir prioridades;
- Executar correções;
- Validar as correções realizadas;
- Manter registros das ações executadas.

Gestores

Os gestores deverão apoiar a execução das correções quando houver impacto operacional.

---

5. Identificação das Vulnerabilidades

As vulnerabilidades poderão ser identificadas por meio de:

- Ferramentas automatizadas de análise;
- Atualizações de fabricantes;
- Alertas de segurança;
- Testes internos;
- Auditorias;
- Relatos de usuários;
- Análises da equipe de TI.

---

6. Classificação

Toda vulnerabilidade deverá ser classificada conforme seu impacto.

Criticidade	Descrição	Prazo recomendado
Crítica	Alto risco de exploração ou comprometimento	Imediato
Alta	Pode comprometer serviços importantes	Até 7 dias
Média	Risco moderado	Até 30 dias
Baixa	Baixo impacto operacional	Até 90 dias

---

7. Tratamento

Após a identificação, a equipe de TI deverá definir uma das seguintes ações:

Remediação

Correção definitiva da vulnerabilidade.

Exemplos:

- atualização;
- correção de configuração;
- substituição do software.

Mitigação

Quando não for possível corrigir imediatamente, deverão ser adotadas medidas que reduzam o risco.

Exemplos:

- restrição de acesso;
- bloqueio de portas;
- segmentação de rede;
- aplicação de regras de firewall.

Aceitação do Risco

Em situações justificadas, a vulnerabilidade poderá permanecer aberta mediante avaliação da equipe responsável e aprovação da Diretoria, quando aplicável.

---

8. Validação

Após a implementação da correção, a equipe de TI deverá verificar se:

- a vulnerabilidade foi eliminada;
- não houve impacto ao ambiente;
- os serviços permanecem funcionando normalmente.

Caso necessário, novas verificações poderão ser realizadas.

---

9. Atualizações de Segurança

Sempre que possível deverão ser aplicadas:

- atualizações do sistema operacional;
- patches de segurança;
- atualizações de firmware;
- correções dos fabricantes.

As atualizações deverão ser realizadas preferencialmente em janelas de manutenção.

---

10. Monitoramento

A equipe de TI deverá acompanhar continuamente:

- novas vulnerabilidades divulgadas;
- atualizações críticas;
- boletins de fabricantes;
- incidentes relacionados aos ativos da empresa.

11. Registros

As atividades relacionadas à gestão de vulnerabilidades deverão possuir registro contendo:

- ativo afetado;
- vulnerabilidade identificada;
- classificação;
- responsável;
- ação executada;
- data da correção;
- situação final.

12. Revisão da Política

Esta política deverá ser revisada anualmente ou sempre que ocorrerem alterações significativas na infraestrutura tecnológica da empresa.

13. Vigência

Esta política entra em vigor na data de sua aprovação.

Histórico de Revisões

Versão	Data		Revisões	Aprovador	Área
	Emissão	Aprovação			
01	09/02/2026	06/03/2026	Emissão da Política	Marcelo Carmanini	Diretoria