RESUMO DAS REVISÕES		
Edição	**Data**	**Alteração**
01	05/05/2025	Emissão inicial
02	15/05/2026	Inclusão dos ODS e do Jeito de Cuidar Unimed

1. Objetivo

Esta política tem como objetivo estabelecer as diretrizes e procedimentos para a identificação, análise, priorização e remediação de vulnerabilidades nos ativos de tecnologia da informação da **Unimed Tupã**.

Busca-se minimizar a exposição a riscos cibernéticos, garantir a integridade dos sistemas e a proteção dos dados institucionais e de beneficiários.

Adicionalmente, esta política contribui diretamente para o **ODS 9 (Indústria, Inovação e Infraestrutura)** e **ODS 16 (Paz, Justiça e Instituições Eficazes)**, ao fortalecer a resiliência da infraestrutura tecnológica e garantir a proteção de dados contra ameaças externas, promovendo um ambiente digital seguro e confiável.

2. Aplicação

Esta política aplica-se a todos os colaboradores, prestadores de serviço, estagiários e parceiros que utilizam ou administram recursos de TI da Unimed Tupã, abrangendo servidores, estações de trabalho, dispositivos de rede, aplicações de software e serviços em nuvem.

3. Definições

- *Vulnerabilidade:* Qualquer fraqueza em um sistema, processo ou configuração que possa ser explorada para comprometer a segurança da informação.
- *Ameaça:* Qualquer evento ou condição que possa explorar uma vulnerabilidade e causar impacto negativo para a organização.
- *Mitigação:* Adoção de medidas para reduzir ou eliminar uma vulnerabilidade identificada.
- *Correção:* Implementação de soluções definitivas para eliminar uma vulnerabilidade.

4. Responsabilidades

✓ *TI / Segurança da Informação:* Responsável por executar as varreduras, analisar os relatórios, definir os planos de ação e monitorar a aplicação das correções.

✓ *Gestores de Áreas:* Responsáveis por viabilizar janelas de manutenção necessárias para a atualização de sistemas críticos sob sua gestão.

✓ *DPO (Encarregado de Dados):* Responsável por supervisionar se a gestão de vulnerabilidades atende aos requisitos de proteção de dados pessoais estabelecidos pela LGPD.

5. Diretrizes Gerais

A gestão de vulnerabilidades deve ser um processo contínuo e sistemático, integrado ao ciclo de vida de todos os ativos de TI.

Todas as ações de segurança devem ser pautadas pelo **Jeito de Cuidar Unimed (JCU)**, entendendo que a segurança da informação é uma forma de cuidado com a privacidade do beneficiário e com a sustentabilidade da cooperativa, exigindo agilidade técnica e responsabilidade ética em cada intervenção realizada nos sistemas.

5.1. Identificação de Vulnerabilidades

A identificação deve ocorrer por meio de varreduras automatizadas periódicas, análises de logs, monitoramento de boletins de segurança de fabricantes e testes de intrusão (pentests) realizados por equipes internas ou consultorias especializadas.

5.2. Classificação e Priorização

As vulnerabilidades identificadas devem ser classificadas de acordo com a severidade (ex: CVSS - Common Vulnerability Scoring System) e o impacto potencial no negócio. A priorização da remediação deve considerar a criticidade do ativo afetado e a probabilidade de exploração da falha.

5.3. Remediação e Mitigação

A remediação consiste na aplicação de patches de segurança, atualizações de firmware ou alterações de configuração. Caso a remediação imediata não seja

possível, devem ser implementados controles compensatórios para mitigar o risco até que a solução definitiva seja aplicada.

5.4. Verificação de Eficácia

Após a execução das ações de remediação, novas varreduras devem ser realizadas para confirmar que a vulnerabilidade foi efetivamente eliminada ou reduzida a níveis aceitáveis de risco.

5.5. Alinhamento com a Agenda 2030 (ODS)

A Unimed Tupã reconhece que a segurança digital é um pilar fundamental para o desenvolvimento sustentável. A mitigação proativa de vulnerabilidades garante a continuidade dos serviços de saúde e a robustez das instituições (**ODS 16**), evitando interrupções que possam comprometer o atendimento ao cidadão.

Além disso, ao manter sistemas atualizados e protegidos, a cooperativa fomenta a inovação segura (**ODS 9**), permitindo a adoção de novas tecnologias de telemedicina e gestão hospitalar sem comprometer a infraestrutura crítica do setor de saúde.

6. Processo de Gestão de Vulnerabilidades

O ciclo de gestão de vulnerabilidades seguirá as seguintes etapas obrigatórias:

- ✓ *Descoberta:* Inventário atualizado de todos os ativos de rede e software.
- ✓ *Inventário:* Identificação de vulnerabilidades nos ativos descobertos.
- ✓ *Classificação:* Atribuição de níveis de risco (Baixo, Médio, Alto, Crítico).
- ✓ *Remediação:* Correção das falhas conforme o cronograma de criticidade.
- ✓ *Verificação:* Auditoria pós-correção para validação do status de segurança.
- ✓ *Relatório:* Documentação do ciclo para fins de conformidade e auditoria.

7. Monitoramento

Esta política será revisada periodicamente para garantir sua adequação às melhores práticas de segurança e às normativas aplicáveis.

8. Distribuição de Cópias

Política disponível no Quallix

9. Registros

Política disponível no Quallix

10. Anexos

Não há

11. Referências

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO 9001:2015**: Sistemas de gestão da qualidade – Requisitos. Rio de Janeiro: ABNT, 2015.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Diário Oficial da União, 2018.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. **Objetivos de Desenvolvimento Sustentável**. Nova York: ONU, 2015.

Aprovação:

ANTONIO CARLOS ANDRADE:00190337885

Assinado de forma digital por ANTONIO CARLOS ANDRADE:00190337885
Dados: 2026.05.14 09:10:01 -03'00'

Presidente