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

1. Objetivo

Esta política estabelece as diretrizes e procedimentos para a identificação, avaliação, teste e instalação de atualizações (*patches*) em todos os ativos de tecnologia da **Unimed de Tupã**.

O objetivo primordial é mitigar riscos de segurança, corrigir vulnerabilidades e garantir a estabilidade dos sistemas que sustentam a prestação de serviços de saúde, assegurando que a infraestrutura digital seja resiliente e confiável.

Sob a filosofia do **"Jeito de Cuidar Unimed"**, a gestão de patches deixa de ser uma tarefa meramente técnica para tornar-se um ato de cuidado preventivo. Manter sistemas atualizados é proteger a integridade dos dados de nossos beneficiários e garantir que o atendimento médico não sofra interrupções por incidentes cibernéticos.

Nossos valores de **Integridade** e **Cooperação** exigem que sejamos diligentes na proteção do ecossistema digital, tratando a segurança da informação como um pilar da confiança depositada pela sociedade em nossa cooperativa.

3. Aplicação

As normas aqui descritas aplicam-se a todos os colaboradores, prestadores de serviços e parceiros que possuam acesso ou responsabilidade sobre a infraestrutura tecnológica da cooperativa, abrangendo servidores, estações de trabalho, dispositivos de rede, sistemas operacionais e aplicações proprietárias ou de terceiros.

4. Definições

- ✓ *Patch:* Fragmento de código de software projetado para atualizar, corrigir ou melhorar um programa de computador, incluindo a correção de vulnerabilidades de segurança.
- ✓ *Vulnerabilidade:* Uma fraqueza em um ativo ou controle que pode ser explorada por uma ou mais ameaças.
- ✓ *Rollback:* Procedimento de reversão de uma atualização para um estado anterior estável em caso de falha crítica após a instalação.
- ✓ *CVE (Common Vulnerabilities and Exposures):* Lista de informações publicamente conhecidas sobre vulnerabilidades de segurança.

6. Alinhamento com os Objetivos de Desenvolvimento Sustentável (ODS)

Esta política está intrinsecamente ligada à Agenda 2030 da ONU, refletindo o compromisso socioambiental da Unimed de Tupã:

- ✓ *ODS 9 — Indústria, Inovação e Infraestrutura:* Ao implementar uma gestão rigorosa de atualizações, promovemos uma infraestrutura digital resiliente e sustentável, capaz de suportar inovações tecnológicas no setor de saúde com segurança e eficiência.
- ✓ *ODS 16 — Paz, Justiça e Instituições Eficazes:* A proteção contra ameaças cibernéticas fortalece a transparência institucional e a proteção de dados sensíveis, contribuindo para a construção de uma instituição confiável, ética e responsável perante seus cooperados e clientes.

7. Responsabilidades

- ✓ *TI:* Responsável por monitorar vulnerabilidades, testar patches e executar a implantação conforme o cronograma definido.
- ✓ *DPO (Encarregado de Dados):* Responsável por validar a conformidade da gestão de patches com a LGPD, garantindo que as atualizações protejam a privacidade dos titulares.
- ✓ *Gestores de Áreas:* Responsáveis por colaborar com as janelas de manutenção e reportar comportamentos anômalos nos sistemas após atualizações.
- ✓ *Comitê de Segurança da Informação:* Responsável por aprovar mudanças críticas e avaliar riscos em casos de impossibilidade técnica de atualização.

4. Descrição

- ✓ Todas as atualizações de patches de segurança devem ser revisadas e aprovadas pelo departamento de TI/SI antes de serem implantadas em produção.
- ✓ As atualizações de patches devem ser aplicadas o mais rápido possível após sua disponibilidade, levando em consideração a criticidade e a gravidade das vulnerabilidades corrigidas.
- ✓ O departamento de TI é responsável por agendar e realizar as atualizações de patches em um horário que cause o menor impacto possível nas operações da Unimed de Tupã
- ✓ Os testes de regressão devem ser realizados após a aplicação de patches para garantir que não haja impacto negativo nas funcionalidades dos sistemas e aplicativos.
- ✓ Os usuários devem reiniciar seus dispositivos conforme necessário para concluir a instalação de patches de segurança.
- ✓ Todos os sistemas e dispositivos devem ser configurados para receber automaticamente as atualizações de patches assim que estiverem disponíveis.
- ✓ Conformidade:

- ✓ O não cumprimento desta política pode resultar em medidas disciplinares, conforme

estabelecido nas políticas de segurança da informação da Unimed de Tupã.

- ✓ Os incidentes de segurança relacionados à falta de aplicação de patches serão investigados pelo departamento de TI e encaminhados para as autoridades competentes, se necessário.

✓ *Priorização de Patches:*

- ✓ Estabeleça critérios claros para priorizar a aplicação de patches com base na criticidade das vulnerabilidades corrigidas e no potencial impacto nos sistemas e operações da Unimed de Tupã
- ✓ Tenha estabelecido um plano de rollback para casos em que ocorrer problemas nas atualizações.

✓ *Comunicação e Conscientização:*

- ✓ Implemente um plano de comunicação eficaz para informar os usuários sobre a importância das atualizações de patches e os procedimentos a serem seguidos.
- ✓ Forneça treinamento e conscientização regular aos colaboradores sobre a importância de manter seus sistemas e dispositivos atualizados e os riscos associados à falta de aplicação de patches.

✓ *Monitoramento e Relatórios:*

- ✓ Estabeleça mecanismos de monitoramento contínuo para verificar o status das atualizações de patches e identificar quaisquer sistemas ou dispositivos que estejam desatualizados.
- ✓ Mantenha registros detalhados de todas as atualizações de patches aplicadas, incluindo datas, versões e sistemas afetados, para fins de auditoria e conformidade.

✓ Avaliação de Impacto e Testes:

- ✓ Realize avaliações de impacto antes de aplicar atualizações de patches críticas para entender como elas podem afetar os sistemas e operações da Unimed de Tupã.
- ✓ Conduza testes rigorosos em ambientes de desenvolvimento e teste antes de implementar atualizações de patches em produção para garantir compatibilidade e estabilidade no ambiente Unimed de Tupã.

5. Monitoramento

A eficácia desta política será medida através dos seguintes KPIs (Key Performance Indicators):

- ✓ Percentual de ativos atualizados dentro do prazo previsto.
- ✓ Número de vulnerabilidades críticas não corrigidas em 30 dias.
- ✓ Tempo médio de resposta para patches de emergência.

6. Distribuição de Cópias

Política disponível no Quallix e no site da Operadora.

7. Registros

Política disponível no Quallix

8. Anexos

Não há

9. Referências

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO/IEC 27001:2022**: Segurança da informação, cibersegurança e proteção à privacidade — Sistemas de gestão da segurança da informação — Requisitos. Rio de Janeiro: ABNT, 2022.

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: Presidência da República, 2018.

Aprovação:

ANTONIO CARLOS ANDRADE:00190337885

Assinado de forma digital por ANTONIO CARLOS ANDRADE:00190337885
Dados: 2026.05.14 09:00:22 -03'00'

Presidente