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 estabelece as diretrizes e normas para o controle de acesso lógico e físico aos ativos de informação da **Unimed Tupã**.

O objetivo primordial é assegurar a confidencialidade, integridade e disponibilidade dos dados de beneficiários, cooperados e colaboradores, refletindo o **Jeito de Cuidar Unimed** através da proteção rigorosa das informações que sustentam a assistência à saúde e a excelência operacional da cooperativa.

2. APLICAÇÃO

As normas aqui contidas aplicam-se a todos os colaboradores, médicos cooperados, prestadores de serviço, estagiários e terceiros que possuam acesso, de forma direta ou indireta, aos sistemas de informação, redes, dispositivos e dependências físicas da **Unimed Tupã**.

3. ALINHAMENTO COM OS OBJETIVOS DE DESENVOLVIMENTO SUSTENTÁVEL (ODS)

A Unimed Tupã reafirma seu compromisso com a Agenda 2030 da ONU, integrando esta política aos seguintes objetivos:

- ✓ *ODS 9 (Indústria, Inovação e Infraestrutura*): Investimento em infraestrutura digital resiliente e segura, promovendo a inovação tecnológica protegida contra ameaças cibernéticas.
- ✓ *ODS 16 (Paz, Justiça e Instituições Eficazes):* Promoção de instituições transparentes e responsáveis por meio da proteção de dados e combate ao uso indevido de informações, fortalecendo a confiança da sociedade na cooperativa.

4. DEFINIÇÕES

- ✓ *Acesso Lógico:* Capacidade de interagir com sistemas, arquivos e redes por meio de credenciais eletrônicas.
- ✓ *MFA (Multi-Factor Authentication):* Método de autenticação que exige dois ou mais fatores de verificação independentes.
- ✓ *Princípio do Menor Privilégio:* Concessão apenas do nível de acesso estritamente necessário para a execução das funções laborais.

- ✓ *Ativos de Informação:* Qualquer dado, sistema, hardware ou software que possua valor para a cooperativa.

5. Responsabilidades

É de responsabilidade da Gestão de Pessoas: a comunicação imediata a gerencia de TI sobre desligamentos, férias e licenças de servidores e estagiários, para que seja efetuado o bloqueio momentâneo ou a revogação definitiva da permissão de acesso aos recursos:

a. Os serviços serão filtrados por programas de antivírus, anti-phishing e anti-spam e, caso violem alguma regra de configuração, serão bloqueados ou excluídos automaticamente.
b. Nenhum técnico de qualquer empresa terceira de tecnologia, que possa vir a prestar serviç, terá acesso ao conteúdo das informações armazenadas nos equipamentos servidores da Unimed de Tupã.

É de responsabilidade da Tecnologia da Informação: o monitoramento da utilização de serviços de rede e de acesso à Internet, podendo ainda exercer fiscalização nos casos de apuração de uso indevido desses recursos, bem como bloquear, temporariamente, sem aviso prévio, a estação de trabalho que esteja realizando atividade que coloque em risco a segurança da rede, até que seja verificada a situação e descartada qualquer hipótese de dano à infraestrutura tecnológica da Unimed de Tupã.

O colaborador é responsável: por todos os acessos realizados através de sua conta de acesso e por possíveis danos causados à Rede Local e a recursos de tecnologia custodiados ou de propriedade da Unimed de Tupã:

a) O usuário é responsável pela integridade e utilização de sua estação de trabalho, devendo, no caso de sua ausência temporária do local onde se encontra o equipamento, bloqueá-lo ou desconectar-se da estação, para coibir acessos indevidos.
b) A utilização simultânea da conta de acesso à Rede Local em mais de uma estação de trabalho ou notebook deve ser evitada, sendo responsabilidade do usuário titular da conta de acesso os riscos que a utilização paralela implica.
c) O usuário não poderá, em hipótese alguma, transferir ou compartilhar com outrem sua conta de acesso e respectiva senha à Rede Local.

O usuário deve informar a área de Tecnologia da Informação qualquer situação da qual tenha conhecimento que configure violação de sigilo ou que possa colocar em risco a segurança inclusive de terceiros.

É dever de o usuário zelar pelo uso dos sistemas informatizados, tomando as medidas necessárias para restringir ou eliminar riscos para a Instituição, a saber:

a) Não permitir a interferência externa caracterizada como invasão, monitoramento ou utilização de sistemas por terceiros, e outras formas;
b) Evitar sobrecarga de redes, de dispositivos de armazenamento de dados ou de outros, para não gerar indisponibilidade de informações internas e externas;
c) Interromper a conexão aos sistemas e adotar medidas que bloqueiem o acesso de terceiros, sempre que completarem suas atividades ou quando se ausentarem do local de trabalho por qualquer motivo;
d) Não se conectar a sistemas e não buscar acesso a informações para as quais não lhe tenham sido dadas senhas e/ou autorização de acesso;
e) Não divulgar a terceiros ou a outros usuários dispositivos ou programas de segurança existentes em seus equipamentos ou sistemas;
f) Utilizar corretamente os equipamentos de informática e conservá-los conforme os cuidados e medidas preventivas estabelecidas;
g) Não divulgar suas senhas e nem permitir que terceiros tomem conhecimento delas, reconhecendo-as como pessoais e intransferíveis;

6. Descrição

O acesso lógico aos recursos da Rede Local deve ser realizado por meio de sistema de controle de acesso. O acesso deve ser concedido e mantido pela área da TI , baseado nas responsabilidades e tarefas de cada usuário:

a. Terão direito a acesso lógico aos recursos da Rede Local os usuários de recursos de tecnologia da informação.
b. Para fins desta Resolução, consideram-se usuários de recursos de tecnologia da informação servidores ocupantes de cargo efetivo ou cargo em comissão, ocupantes de emprego público em exercício, assim como funcionários de empresas prestadoras de serviços, estagiários e demais usuários temporários em atividade na Unimed de Tupã.
c. O acesso remoto deve ser realizado por meio de VPN – Rede Virtual Privada, após as devidas autorizações.
d. Deve ser utilizado o MFA para a autenticação de acesso remoto.
e. O acesso a todas as aplicações corporativas ou de terceiros que estejam hospedados em fornecedores deve utilizar MFA.

A área de TI deve estabelecer e manter um inventário de todas as contas gerenciadas, este deve incluir contas de usuário, administrativas, testes e serviço. Em caso de contas de serviço, o inventário deve conter no mínimo informações de:

a) Departamento proprietário.

b) Data de criação/última autorização de renovação de acesso;

c) A área de TI deve é responsável por validar todas as contas ativas do órgão, a *cada 90 (noventa), dias.*

✓ A área de TI deve implementar a centralização da gestão de contas por meio de serviço de diretório e/ou identidade.

✓ Deve estabelecer e manter um inventário dos sistemas de autenticação e autorização da organização, tal inventário deve ser revisado periodicamente.

✓ Deve centralizar o controle de acesso para todos os ativos de informação da organização por meio de um serviço de diretório ou provedor de SSO.

✓ Deve definir e manter o controle de acesso dos usuários baseado em funções:

a) Deve ser elaborada a documentação dos direitos dos acessos para cada função dentro da organização.

b) Deverá realizar análises de controle de acesso aos ativos institucionais para validar se todos os privilégios estão autorizados para a execução de atividades de cada função, este processo deve ser repetido de forma periódica ou quando novas funções e ativos de informação forem inseridos na organização.

6.1 CONTA DE ACESSO LÓGICO E SENHA

Para utilização das estações de trabalho da Unimed de Tupã, será obrigatório o uso de uma única identificação (login) e de senha de acesso, fornecidos pela Tecnologia da informação, mediante solicitação formal pelo titular da unidade do requisitante:

a) Os privilégios de acesso dos usuários à Rede Local devem ser definidos pela unidade requisitante ao qual o usuário está vinculado, limitando-se a atividades estritamente necessárias à realização de suas tarefas.

b) Na necessidade de utilização de perfil diferente do disponibilizado, o titular da unidade do usuário deverá encaminhar solicitação para a TI que a examinará, podendo negá-la nos casos em que a entender desnecessária.

O login e senha são de uso pessoal e intransferível, sendo proibida a sua divulgação, sob pena de serem bloqueados pela TI quando constatada qualquer irregularidade.

✓ Para retomar o acesso à rede, deverá ser formalizada nova requisição pelo titular da unidade do requisitante.

O padrão adotado para o formato da conta de acesso do usuário é a sequência primeiro nome + ponto + último nome do usuário, como por exemplo, João.silva.

✓ Nos casos de já existência de conta de acesso para outro usuário, a TI realizará outra combinação utilizando o nome completo do usuário para o qual a conta está sendo criada.

O padrão adotado para o formato da senha é o definido pela TI, que considera o tamanho

mínimo de caracteres, a tipologia (letras, número e símbolos) e a proibição de repetição de senhas anteriores. A formação da senha da identificação (login) de acesso à Rede Local deve seguir as regras de:

a) Possuir tamanho mínimo de dez caracteres, sendo obrigatório o uso de letras e números, para contas que utilizam MFA e 10 caracteres para contas que não utilizam MFA;
b) Recomenda-se a utilização de letras maiúsculas, minúsculas e caracteres especiais ($, %, &,...);
c) Não ser formada por sequência numérica (123...), alfabética (abc...), nomes próprios, palavras de fácil dedução, datas, placa de carro, número de telefone, a própria conta de acesso, apelidos ou abreviações;
d) Não utilizar termos óbvios, tais como: Brasil, senha, usuário, password ou system.
e) Não reutilizar as últimas *[05 (cinco)] senhas.*

A TI fornecerá uma senha temporária para cada conta de acesso criada no momento da liberação dessa conta e a mesma deverá ser alterada pelo usuário quando do primeiro acesso à Rede Local.

As senhas de acesso serão renovadas a cada 3 meses, devendo o usuário ser informado antecipadamente a fim de que ele próprio efetue a mudança.

✓ Caso não efetue a troca no prazo estabelecido, será bloqueado seu acesso à Rede Local até que a nova senha seja configurada.

6.2 BLOQUEIO, DESBLOQUEIO E CANCELAMENTO DA CONTA DE ACESSO

A conta de acesso será bloqueada nos seguintes casos:

a) Após 5 (cinco) tentativas consecutivas de acesso errado;
b) Solicitação do superior imediato do usuário com a devida justificativa;
c) Quando da suspeita de mau uso dos serviços disponibilizados pela Unimed de Tupã ou descumprimento da Política de Segurança da Informação e normas correlatas em vigência.
d) Após 30 dias consecutivos sem movimentação pelo usuário.

O desbloqueio da conta de acesso à Rede Local será realizado apenas após solicitação formal do superior imediato do usuário a área de TI.

Quando do afastamento temporário do usuário, a conta de acesso deve ser bloqueada a pedido do superior imediato a área de TI.

A conta de acesso não utilizada há mais de 180 (cento e oitenta) dias poderá ser cancelada.

A área de Tecnologia da Informação deve configurar o bloqueio automático de sessão nos ativos após um período de inatividade preestabelecido.

Tal prazo pode ser específico para cada tipo de ativo.

Ainda deve, sempre que possível, priorizar a revogação/desativação de contas com o

objetivo de manter dados e logs para possíveis auditorias.

6.3 MOVIMENTAÇÃO INTERNA

Quando houver mudança do usuário para outro setor ou o usuário ocupar uma nova função, os direitos de acesso à Rede Local devem ser revogados.

a) O novo superior imediato ou o setor responsável pela Gestão de Pessoas deve realizar a solicitação de novos acessos de acordo com novo setor / função do usuário.
b) Os direitos de acesso antigos devem ser imediatamente cancelados conforme solicitação do antigo superior imediato a área de TI.

6.4 CONTA DE ACESSO BIOMÉTRICO

A conta de acesso biométrico, quando implementada, deve ser vinculada a uma conta de acesso lógico e ambas devem ser utilizadas para se obter um acesso, a fim de atender os conceitos da autenticação de multifatores.

✓ A Unimed de Tupã deverá tratar seus respectivos dados biométricos como dados sigilosos, preferencialmente, utilizando-se de criptografia, na forma da legislação vigente.

Os incidentes que afetem a Segurança das Informações, assim como o descumprimento da Política de Segurança da Informação e Normas de Segurança devem ser obrigatoriamente comunicados pelos usuários á gerencia de TI.

Quando houver suspeita de quebra da segurança da informação que exponha ao risco os serviços ou recursos de tecnologia, a área de TI fará a investigação, podendo interromper temporariamente o serviço afetado, sem prévia autorização.

a) Nos casos em que o ator da quebra de segurança for um usuário, a TI comunicará os resultados ao superior imediato do mesmo para adoção de medidas cabíveis.
b) Ações que violem a PSI ou que quebrem os controles de Segurança da Informação serão passíveis de sanções civis, penais e administrativas, conforme a legislação em vigor, que podem ser aplicadas isoladamente ou cumulativamente.
c) Processo administrativo disciplinar específico deverá ser instaurado para apurar as ações que constituem em quebra das diretrizes impostas por esta Norma e pela PSI.
d) A resolução de casos de violação/transgressões omissas nas legislações correlatas será resolvida pelo Comitê de LGPD da Unimed de Tupã.

7. Monitoramento

A Unimed Tupã mantém logs de acesso de todos os sistemas críticos. Auditorias periódicas serão realizadas pela Coordenação do SGQ para verificar a conformidade dos acessos concedidos versus a necessidade real das áreas, garantindo a melhoria contínua do sistema.

8. Distribuição de Cópias

Disponível no Quallix

9. REGISTROS

- ✓ Logs de criação e exclusão de usuários.
- ✓ Relatórios de auditoria de permissões.

10. ANEXOS

- ✓ Anexo I: Matriz de Responsabilidades e Perfis de Acesso.
- ✓ Anexo II: Termo de Uso de Ativos Tecnológicos.

16. REFERÊNCIAS

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

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **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 08:56:50 -03'00'

Presidente