RESUMO DAS REVISÕES		
Edição	**Data**	**Alteração**
01	05/05/2025	Emissão inicial
02	07/11/2025	Análise gerla pela Diretoria. Ajustes no intem 5 sobre a utilização dos dispositivos móveis.
03	15/05/206	Inlusão dos ODS e do Jeito de Cuidar Unimed

1. Objetivo

Esta política estabelece as normas e diretrizes para a utilização de dispositivos móveis pessoais (smartphones, tablets e notebooks) para fins profissionais na **Unimed Tupã**, prática conhecida como *Bring Your Own Device* (BYOD).

O objetivo é garantir a segurança das informações institucionais, a proteção de dados pessoais e a integridade da infraestrutura tecnológica.

Adicionalmente, esta política contribui diretamente para o **ODS 9 (Indústria, Inovação e Infraestrutura)** e o **ODS 12 (Consumo e Produção Responsáveis)**, ao promover o uso eficiente da infraestrutura tecnológica e a gestão consciente do ciclo de vida dos dispositivos.

2. Aplicação

Esta norma aplica-se a todos os colaboradores, prestadores de serviço, estagiários e parceiros que possuam autorização formal para acessar sistemas, e-mails ou dados da Unimed Tupã através de seus dispositivos particulares.

3. Diretrizes Gerais

A adesão ao modelo BYOD é facultativa e depende de autorização prévia da Gerência de TI e da Diretoria.

A utilização de dispositivos móveis para o trabalho deve ser pautada pelo **Jeito de Cuidar Unimed (JCU)**, equilibrando a agilidade tecnológica com o respeito à privacidade, ao tempo de descanso do colaborador e à segurança absoluta das informações dos beneficiários.

3.1. Requisitos Técnicos Mínimos

Para que um dispositivo seja homologado, ele deve possuir sistema operacional atualizado, suporte a criptografia de dados e capacidade de instalação de softwares de gerenciamento de dispositivos móveis (MDM), caso solicitado pela TI.

3.2. Responsabilidade do Usuário

O colaborador é o único responsável pela integridade física do aparelho, bem como pelos custos de aquisição, manutenção e planos de dados, salvo acordos específicos em contrato de trabalho.

3.3. Segurança da Informação

É obrigatória a utilização de senhas fortes, biometria e bloqueio automático de tela. É terminantemente proibido o armazenamento de dados sensíveis de beneficiários diretamente na memória local do dispositivo, devendo-se priorizar o acesso via nuvem ou sistemas oficiais.

3.4. Alinhamento com a Agenda 2030 (ODS)

A Unimed Tupã reconhece que a prática de BYOD é um vetor de sustentabilidade. Ao otimizar os recursos tecnológicos existentes (**ODS 9**), a cooperativa reduz a necessidade de aquisição de novos hardwares, diminuindo a pegada de carbono institucional. Além disso, incentiva a responsabilidade no ciclo de vida dos dispositivos (**ODS 12**), promovendo a conscientização sobre o descarte correto de resíduos eletrônicos e o consumo consciente de tecnologia.

4. Privacidade e Monitoramento

A Unimed Tupã respeita a privacidade dos dados pessoais contidos no dispositivo (fotos, mensagens privadas, aplicativos pessoais). No entanto, a cooperativa reserva-se o direito de monitorar e auditar o tráfego de dados profissionais e o acesso aos sistemas corporativos para garantir a conformidade com a **LGPD**.

Atenção: Em caso de desligamento ou suspeita de violação de segurança, a Unimed Tupã poderá realizar o "Remote Wipe" (apagamento remoto) exclusivamente dos dados e aplicativos corporativos instalados no dispositivo.

5. Suporte Técnico

O suporte da TI limita-se exclusivamente à configuração de e-mails corporativos, instalação de certificados de segurança e acesso aos sistemas da Unimed. Problemas de hardware ou falhas no sistema operacional do dispositivo pessoal são de inteira responsabilidade do proprietário.

6. Perda, Roubo ou Furto

Em caso de perda, roubo ou furto do dispositivo, o colaborador deve comunicar imediatamente o Departamento de TI e o DPO (Encarregado de Dados) em um prazo máximo de **2 horas** após a ciência do fato, para que as credenciais de acesso sejam revogadas e o apagamento remoto dos dados corporativos seja iniciado.

7. Desconexão e Bem-estar

Em consonância com o **Jeito de Cuidar Unimed**, o uso de dispositivos móveis para fins profissionais fora do horário de expediente deve ser evitado, respeitando-se o direito à desconexão e o equilíbrio entre vida pessoal e profissional, exceto para cargos de prontidão ou em situações de emergência devidamente justificadas.

8. Termo de Aceite e Responsabilidade

A utilização do dispositivo pessoal para fins de trabalho implica na aceitação plena desta política. O descumprimento das normas aqui estabelecidas poderá acarretar sanções disciplinares, conforme previsto no Código de Conduta e na legislação trabalhista vigente.

9. Vigência

Esta política entra em vigor na data de sua publicação e deve ser revisada anualmente ou sempre que houver mudanças significativas na infraestrutura tecnológica ou na legislação de proteção de dados.

10. 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 08:57:24 -03'00'

Presidente