GUIA ORIENTATIVO

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO (PSI)

Unimed Porto Velho

somos coop

OBJETIVO

Garantir a **proteção das informações** da Unimed Porto Velho e o cumprimento da LGPD (Lei Geral de Proteção de Dados), prevenindo acessos indevidos, vazamentos, fraudes e uso inadequado de dados.

A PSI fortalece a **confiança de beneficiários, médicos, colaboradores e parceiros**, promovendo uma cultura de segurança, ética e responsabilidade no tratamento das informações.

Toda informação tem valor e precisa ser protegida, independentemente do formato (digital, físico ou verbal).

A quem se aplica

Esta Política se aplica a todos que, de alguma forma, acessam, tratam ou armazenam informações da cooperativa, incluindo:

Importante: todos têm responsabilidade direta pela proteção das informações sob sua guarda. O descumprimento das normas pode gerar consequências disciplinares, contratuais e legais.

Colaboradores (efetivos, temporários e estagiários).

Cooperados e médicos credenciados.

Prestadores de serviços, fornecedores e parceiros.

Visitantes autorizados e usuários de sistemas corporativos.

Princípios Fundamentais da Segurança da Informação

Confidencialidade

Somente pessoas autorizadas podem acessar informações. Evite falar, enviar ou mostrar dados a quem não tem permissão.

Integridade

Os dados devem permanecer corretos e completos. Nunca altere, copie ou apague informações sem autorização.

Disponibilidade

As informações precisam estar acessíveis para quem tem permissão, sempre que necessário, garantindo continuidade das atividades.

Responsabilidade

Cada colaborador é guardião das informações que utiliza. Cuidar dos dados é parte do seu trabalho.

Conformidade

Cumprir a LGPD, as normas internas e as regulamentações do setor de saúde é obrigatório para todos.

Boas Práticas Diárias (Obrigatórias)

Estas atitudes simples previnem falhas e incidentes:

- **Bloqueie a tela sempre** que se ausentar, mesmo por alguns minutos.
- **Use senhas fortes:** com letras, números e símbolos. Troque a cada 60 dias e nunca compartilhe.
- **Evite anotar senhas** em papéis, agendas ou post-its.
- **Utilize apenas e-mails e sistemas corporativos.** É proibido usar e-mails pessoais, WhatsApp ou redes sociais para tratar dados da Unimed.
- **Guarde documentos físicos** em armários trancados; nunca deixe papéis sobre mesas ou impressoras.
- **Descarte com segurança:** entregue documentos à eliminação formal; nunca jogue dados no lixo comum.
- **Mantenha mesa e tela limpas:** sem informações expostas.
- **Evite instalar softwares sem aprovação da TI.**
- **Atenção a links e anexos:** desconfie de e-mails estranhos, promoções e solicitações de dados.
- **Comunique qualquer anormalidade** (falha, vazamento, e-mail suspeito, perda de equipamento, acesso indevido).

Lembre-se: a segurança começa em pequenos gestos diários, cada colaborador é parte da defesa da cooperativa.

Comunicação e Incidentes de Segurança

Identificou algo errado? Aja rápido!

Qualquer falha, suspeita ou incidente de segurança deve ser reportado imediatamente.

Como agir:

- Registre o ocorrido no **sistema ITOP** (chamado restrito).
- Avise **sua liderança imediata** ou a TI, caso não tenha acesso ao sistema.
- Em caso de dúvida sobre o que fazer, contate a **Encarregada de Proteção de Dados (DPO).**

Exemplos de incidentes:

- **E-mail enviado para pessoa errada.**
- **Perda ou roubo de notebook/celular corporativo.**
- **Falhas de login ou tentativas suspeitas de acesso.**
- **Documento esquecido em local público.**
- **Vazamento de informações em redes sociais.**

Importante: *relatar incidentes não é punição, é uma atitude responsável e necessária para evitar maiores prejuízos.*

Penalidades e Consequências

O descumprimento da PSI pode resultar em **advertência, suspensão, bloqueio de acesso, rescisão contratual ou responsabilização legal**, conforme a gravidade do caso.

Também pode gerar **multas e penalidades** à cooperativa pela LGPD.

As regras estão alinhadas ao **Código de Conduta** e ao Programa Nacional de Governança, Privacidade e Proteção de Dados **(PNGPPD)** do Sistema Unimed.

Atenção: a omissão também é considerada infração. se identificar um risco e não comunicar, o colaborador também responde pelo dano.

Dúvidas, suporte e contato

- **Encarregada de Proteção de Dados (DPO)**
  Email: *encarregadalgpd@unimedportovelho.coop.br*
- **ITOP:** para registrar incidentes e solicitações de segurança da informação.
- *A DPO e a equipe de TI estão à disposição para orientar, esclarecer dúvidas e apoiar as áreas na aplicação da PSI.*

“““Segurança da Informação é mais do que um dever: é um ato de cuidado, confiança e respeito por quem nos confia seus dados e sua saúde.”””

Unimed Porto Velho – Juntos pela proteção da informação.

Unimed Porto Velho

somos coop

ANS-33737-4