Unimed
Porto Velho

somos coop

ANS-33737-4

GUIA ORIENTATIVO

SEGURANÇA NO ACESSO AOS SISTEMAS

INTRODUÇÃO

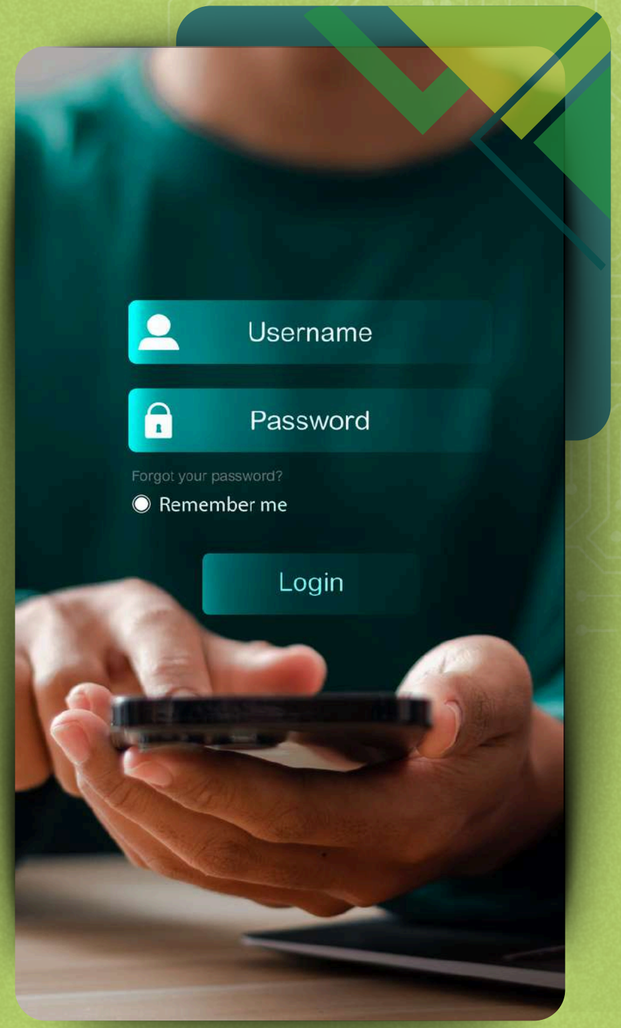
A segurança da informação é fundamental para a proteção dos dados pessoais e sensíveis no ambiente de trabalho. O uso adequado de logins, senhas e registros de acesso é essencial para garantir a **rastreabilidade**, **evitar incidentes de segurança** e **proteger informações** contra invasões maliciosas.

Este guia tem como objetivo orientar colaboradores da Operadora de Plano de Saúde, Hospital Unimed, Consultórios Médicos CIAS I e II, Espaço Multiterapias e Espaço Viver Bem sobre as melhores práticas relacionadas a esses temas.

Unimed
Porto Velho

Login e Acesso

- Sempre encerre (logoff) ou bloqueie sua sessão de usuário(a) no Windows, em sistemas e aplicativos ao terminar suas atividades ou se afastar do dispositivo mesmo que por poucos minutos, principalmente em computadores de uso compartilhado e em notebooks; estes últimos, em especial, por sua portabilidade que possibilita seu furto rapidamente com pouquíssima dificuldade.
- Evite salvar senhas em navegadores ou fazer anotações físicas visíveis.
- Utilize apenas dispositivos autorizados e redes seguras para acessar sistemas e aplicativos corporativos.
- Sua conta de usuário(a) (login) é pessoal e intransferível. Nunca compartilhe suas credenciais com terceiros, nem mesmo com colegas de mesmo setor/cargo/função.



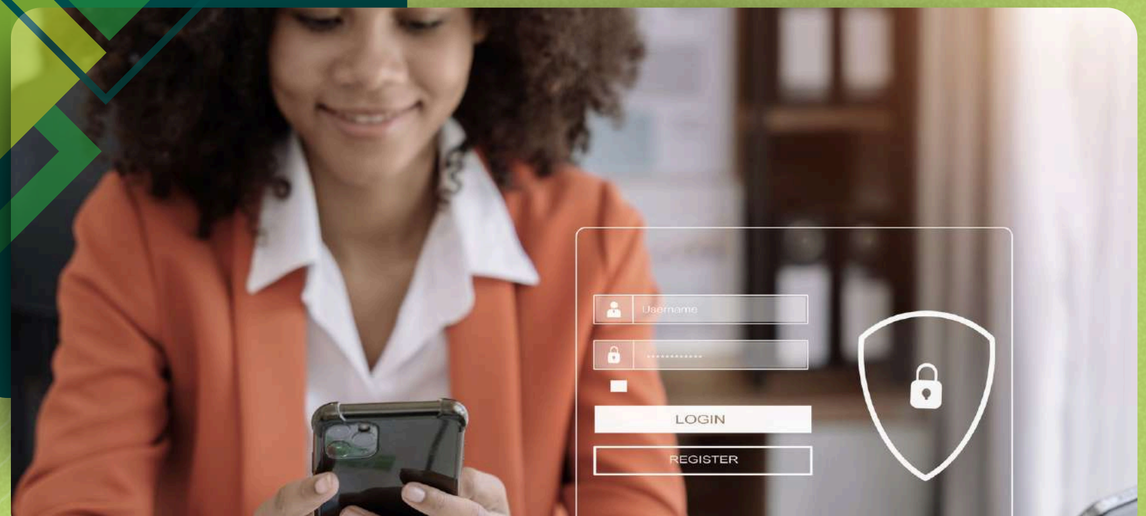
Unimed
Porto Velho

Senhas seguras

- **Crie senhas fortes:** Utilize combinação de letras maiúsculas e minúsculas, números e caracteres especiais (@, $, #, & etc.).
- **Evite senhas fracas ou fáceis de adivinhar**, como: unimed@123, recepcao@569, senha123, admin2024; que contenham partes de seu nome/sobrenome, de familiares, parentes ou animais de estimação.
- **Não reutilize senhas antigas** e evite usar a mesma senha para diferentes sistemas, aplicativos e serviços.
- **Atualize suas senhas periodicamente** e ative a verificação em duas ou múltiplas etapas quando disponível.

Rastreabilidade e Registros (Logs) de Acessos

- Os acessos realizados a dispositivos, sistemas e aplicativos corporativos são registrados para garantir segurança e conformidade com a LGPD.
- O monitoramento dos registros de eventos (logs) de acessos é essencial para identificar tentativas de acesso indevido.
- O compartilhamento de credenciais pode levar à sua responsabilização por acessos indevidos.
- ***Em caso de suspeita de acesso não autorizado***, informe imediatamente ao setor de TI e/ou Segurança da Informação.



Riscos e Consequências

- **Invasão Hacker:** Senhas fracas podem facilitar ataques cibernéticos ecomprometimento de dados.
- Exposição de Dados Sensíveis: Dados de pacientes podem ser acessados indevidamente, levando a penalidades legais.
- **Perda ou Roubo de Dados**: A falta de controle sobre acessos pode resultar emvazação de informações críticas.
- **Sanções Legais e Administrativas:** O descumprimento das diretrizes desegurança pode gerar medidas disciplinares, demissão e penalidades conforme a LGPD.

Boas práticas

- **Educação Contínua:** Participe de treinamentos e conscientização sobresegurança da informação.
- **Relate Incidentes:** Informe qualquer suspeita de fraude, vazamento ou acesso indevido ao setor responsável.
- **Siga as Políticas Internas:** Cumprir as diretrizes da instituição protege você eos dados dos pacientes.

Unimed
Porto Velho
somos coop

A adoção dessas medidas é essencial para garantir a segurança digital da nossa instituição e a proteção dos dados dos pacientes.

Dúvidas ou Incidentes?

Entre em contato com o setor de Tecnologia da Informação ou Segurança da Informação.

TI – ti@unimedportovelho.coop.br, pelo ITOP

LGPD – encarregadalgpd@unimedportovelho.coop.br ou pelo Canal do Colaborador

Contamos com sua colaboração!

ACESSE O QR CODE E
SAIBA MAIS SOBRE LGPD

Aqui tem cuidado.

Aqui tem segurança.