

Política de Segurança da Informação

SUMÁRIO

1. Objetivo e Declaração da Política	2
2. Abrangência e Aplicação.....	2
3. Contratação, Conscientização E Treinamento.....	3
4. Proteção Da Informação E Privacidade Dos Dados	3
5. Avaliação De Riscos À Informação E Seleção De Controles.....	4
6. Controle De Acesso À Informação	4
6.1. Gerenciamento de Senhas.....	4
6.2. Gerenciamento de Perfis.....	5
6.3. Revisão de Acesso.....	5
7. Uso De Recursos Tecnológicos.....	5
8. Monitoramento E Auditoria	7
9. Gestão De Problemas De Infraestrutura De TI	7
10. Gestão De Incidentes De Segurança Da Informação.....	8
11. Descumprimento Da Política.....	8
12. Responsabilidades	8
• Sanções: O não cumprimento das diretrizes estabelecidas nesta política sujeitará o infrator a medidas disciplinares. Tais medidas podem variar de advertência verbal a demissão por justa causa, a depender da gravidade da infração e em conformidade com a legislação trabalhista vigente. A não comunicação de um incidente ou suspeita de violação de segurança será considerada uma falta grave. .	9
13. Ciência Da Política De Segurança Da Informação	9
14. Controle De Revisão	10
15. Referências.....	10

ATUALIZAÇÃO	REVISÃO	PROCESSO / AUTOR	CLASSIFICAÇÃO
15/12/2025	V2	Departamento de Tecnologia da Informação (TI)	Interna

1. Objetivo e Declaração da Política

A presente Política de Segurança da Informação (PSI) tem como objetivo estabelecer as diretrizes para o tratamento e a proteção das informações da Unimed Adamantina Cooperativa de Trabalhos Médico.

Esta política visa adequar a proteção dos ativos de informação às necessidades do negócio e aos requisitos regulatórios, sob os pilares da **Confidencialidade, Integridade, Disponibilidade, Legalidade e Autenticidade**.

A gestão da **Unimed Adamantina** está comprometida em promover uma cultura de segurança, e para tal, fica definido que o **proprietário da informação é o Gestor ou Diretor da área onde a informação se originou**, sendo este o principal responsável pela sua correta classificação e proteção.

Para garantir a transparência e o comprometimento, todos os usuários de informações e equipamentos de tecnologia que fazem parte do regimento interno da **Unimed Adamantina** (incluindo colaboradores em regime de CLT, Diretores Executivos, Conselheiros, Médicos e outros profissionais contratados) devem declarar sua ciência e compromisso com o cumprimento desta norma.

2. Abrangência e Aplicação

Esta política se aplica a todos os públicos, internos e externos, que manipulam, processam, transportam ou acessam os ativos de informação da **Unimed Adamantina**, incluindo, mas não se limitando a: colaboradores em regime CLT, diretores executivos, conselheiros, cooperados, estagiários, aprendizes, prestadores de serviço e terceiros. Aplica-se também a todos os ativos de informação, sistemas, redes de comunicação e instalações físicas. A gestão e supervisão desta política estão sob a responsabilidade do Comitê de Segurança da Informação.

Esta política se aplica a:

ATUALIZAÇÃO	REVISÃO	PROCESSO / AUTOR	CLASSIFICAÇÃO
15/12/2025	V2	Departamento de Tecnologia da Informação (TI)	Interna

- **Pessoas:** Todos os colaboradores, diretores, conselheiros, estagiários, aprendizes, prestadores de serviço, consultores e quaisquer terceiros que tenham acesso, autorizado ou não, aos ativos de informação da organização.
- **Informação:** Todos os dados e informações, em qualquer formato (digital, impresso, falado), criados, processados, armazenados ou transmitidos pela organização ou em seu nome.
- **Ativos:** Todos os ativos de tecnologia da informação, incluindo, mas não se limitando a, computadores, servidores, dispositivos móveis, sistemas de software, redes de comunicação, e instalações físicas que os abrigam.

3. Contratação, Conscientização E Treinamento

A responsabilidade com a Segurança da Informação inicia-se na fase de contratação, com o apoio da área de Recursos Humanos para formalização dos contratos de trabalho. As áreas de Tecnologia da Informação e Segurança da Informação, com o apoio da alta gestão, devem promover campanhas de conscientização e treinamentos periódicos para garantir que todos os colaboradores estejam qualificados e atualizados sobre as melhores práticas de segurança.

4. Proteção Da Informação E Privacidade Dos Dados

Toda informação, em formato físico ou digital, deve ser protegida de acordo com sua classificação.

- **Classificação:** As informações devem ser classificadas, no mínimo, em: Informação Pública, Informação Interna, Informação Confidencial, e Informação de Dados Pessoais e Sensíveis.
- **Controles:** Informações críticas, pessoais e sensíveis devem ser mantidas em áreas seguras, com acesso controlado e monitorado. Controles de segurança lógica, como segregação de funções, proteção contra malware, rotinas de backup e processos de descarte seguro, devem ser implementados e mantidos.

ATUALIZAÇÃO	REVISÃO	PROCESSO / AUTOR	CLASSIFICAÇÃO
15/12/2025	V2	Departamento de Tecnologia da Informação (TI)	Interna

5. Avaliação De Riscos À Informação E Seleção De Controles

Os requisitos de segurança devem ser identificados por meio de uma avaliação sistemática dos riscos.

- **Processo:** A avaliação de risco deve considerar o impacto potencial nos negócios em caso de falha de segurança (perda de confidencialidade, integridade ou disponibilidade) e a probabilidade de ocorrência da falha.
- **Tratamento:** Uma vez identificados, os riscos devem ser documentados e um plano de ação deve ser definido para corrigi-los, monitorá-los ou eliminá-los, com a aplicação de controles apropriados.
- **Revisão:** O processo de gerenciamento de riscos deve ser revisto, no mínimo, a cada 12 (doze) meses ou sempre que ocorrerem mudanças significativas no ambiente de negócio ou tecnológico.

6. Controle De Acesso À Informação

- **Princípio:** O acesso à informação deve ser baseado na necessidade de negócio ("need-to-know") e no princípio do menor privilégio ("least privilege"). Todo acesso deve ser formalmente autorizado pelo proprietário da informação.
- **Responsabilidade:** Todo usuário é responsável por cumprir os controles de segurança e privacidade da informação a que tem acesso, utilizando-a unicamente para as finalidades profissionais designadas.

6.1. Gerenciamento de Senhas

- **Complexidade:** As senhas devem possuir, no mínimo, 10 caracteres, contendo obrigatoriamente letras maiúsculas, minúsculas e números.
- **Ciclo de Vida:** As senhas devem ser trocadas a cada 60 (sessenta) dias, e o sistema não deve permitir a reutilização das últimas 03 (três) senhas.
- **Primeiro Acesso:** Toda senha inicial é temporária e deve ser obrigatoriamente alterada pelo usuário no primeiro acesso, em caso onde a primeira senha não é realizada pelo usuário.

ATUALIZAÇÃO	REVISÃO	PROCESSO / AUTOR	CLASSIFICAÇÃO
15/12/2025	V2	Departamento de Tecnologia da Informação (TI)	Interna

- **Bloqueio:** A conta do usuário será bloqueada após 5 (cinco) tentativas de autenticação sem sucesso. O desbloqueio requer contato formal com a Equipe de Suporte Técnico.
- **Proteção:** É responsabilidade exclusiva do usuário guardar e manter o sigilo de suas senhas, sendo proibido compartilhá-las.

6.2. Gerenciamento de Perfis

- **Suspensão:** As credenciais de acesso de colaboradores afastados (férias, licenças) devem ser suspensas durante o período.
- **Inatividade:** Contas não utilizadas por um período de 60 (sessenta) dias devem ser bloqueadas automaticamente, salvo exceções formalmente aprovadas.
- **Desligamento:** As contas de colaboradores demitidos devem ser bloqueadas imediatamente após a notificação do RH.

6.3. Revisão de Acesso

Periodicamente, em um prazo não superior a 12 (doze) meses, os gestores, na qualidade de proprietários da informação, devem revisar os acessos de suas equipes aos sistemas e recursos. Esta revisão visa garantir a manutenção do princípio do menor privilégio.

7. Uso De Recursos Tecnológicos

Os recursos tecnológicos são de propriedade da **Unimed Adamantina** e devem ser utilizados de forma profissional, ética e segura.

7.1 Comunicação Organizacional e Ferramentas Corporativas

- Toda comunicação e troca de informações relacionadas às atividades profissionais, tanto interna quanto externamente, deve ser realizada **exclusivamente** por meio das soluções de tecnologia homologadas e fornecidas pela Unimed Adamantina (e-mail corporativo, sistema de telefonia,

ATUALIZAÇÃO	REVISÃO	PROCESSO / AUTOR	CLASSIFICAÇÃO
15/12/2025	V2	Departamento de Tecnologia da Informação (TI)	Interna

plataformas de videoconferência e aplicativos de mensagens instantâneas institucionais).

- É expressamente proibido o uso de aplicativos de mensagens pessoais (como WhatsApp, Telegram, etc.), e-mails particulares ou outras plataformas não corporativas para armazenar, discutir ou transacionar qualquer informação de propriedade da Unimed Adamantina, de seus clientes ou parceiros.

Esta medida visa garantir a segurança, a rastreabilidade, a confidencialidade e o registro adequado das informações, em conformidade com os pilares dessa política.

- **É proibido:** Utilizar os recursos para receber, armazenar ou divulgar conteúdo ilícito, pornográfico, obsceno, racista, discriminatório, ofensivo, que viole propriedade intelectual ou que caracterize propaganda política. **Também é proibido utilizar ferramentas de comunicação não homologadas pela Unimed Adamantina para tratar de assuntos de trabalho**, bem como violar a privacidade de dados pessoais ou sensíveis.
- **Manutenção:** Nenhum colaborador deve alterar configurações, instalar softwares ou realizar reparos nos equipamentos. Tais atividades são de responsabilidade exclusiva da Equipe de Suporte Técnico.
- **Segurança Física:** O colaborador deve bloquear seu computador com senha sempre que se ausentar da estação de trabalho. Dispositivos portáteis (notebooks, celulares) devem ser manuseados com cuidado e protegidos contra perda e roubo.
- **Dispositivos Particulares (BYOD):** O uso de recurso tecnológico particular para acessar a rede corporativa não é permitido como regra. Exceções devem ser formalmente analisadas e aprovadas pelo Comitê de Segurança da Informação, e o dispositivo estará sujeito a auditorias de segurança.

ATUALIZAÇÃO	REVISÃO	PROCESSO / AUTOR	CLASSIFICAÇÃO
15/12/2025	V2	Departamento de Tecnologia da Informação (TI)	Interna

8. Monitoramento E Auditoria

A **Unimed Adamantina** reserva-se o direito de implantar sistemas de monitoramento em estações de trabalho, servidores, correio eletrônico (e-mail) e acesso à internet para prevenir, detectar e investigar violações a esta política. Os dados capturados poderão ser analisados para obter evidências e ser usados em processos investigatórios ou judiciais.

9. Gestão De Problemas De Infraestrutura De TI

A Gestão de Problemas visa identificar, analisar e resolver as causas raiz de um ou mais incidentes, prevenindo sua recorrência e minimizando o impacto adverso sobre os negócios. Este processo é reativo (iniciado após incidentes) e proativo (identificando problemas antes que gerem incidentes).

As etapas do processo são:

- **Identificação e Registro:** Um problema pode ser identificado a partir de incidentes recorrentes, um incidente maior com causa desconhecida, ou pela análise de tendências pela equipe de TI. Todo problema deve ser formalmente registrado como um "Problema" no sistema de gestão de serviços de TI (ex: GLPI), recebendo uma identificação única para rastreamento.
- **Análise e Diagnóstico (Análise de Causa Raiz - RCA):** Para cada problema registrado, uma investigação formal deve ser conduzida para determinar sua causa raiz. O objetivo é entender a falha fundamental, e não apenas tratar seus sintomas.
- **Resolução e Implementação de Soluções:** Uma vez identificada a causa raiz, a equipe de TI deve planejar e implementar uma solução duradoura. Isso pode envolver mudanças de configuração, desenvolvimento de correções de software (patches), substituição de hardware ou otimização de processos.

ATUALIZAÇÃO	REVISÃO	PROCESSO / AUTOR	CLASSIFICAÇÃO
15/12/2025	V2	Departamento de Tecnologia da Informação (TI)	Interna

Enquanto a solução definitiva é desenvolvida, uma solução de contorno (workaround) pode ser implementada e comunicada para restaurar o serviço temporariamente.

- **Prevenção e Base de Conhecimento:** Após a resolução, todos os detalhes do problema, incluindo os sintomas, a causa raiz identificada e a solução definitiva aplicada, devem ser rigorosamente documentados na **Base de Conhecimento** do sistema de gestão. Esta base de conhecimento servirá para acelerar a resolução de incidentes futuros e para fornecer dados para uma gestão de problemas proativa, evitando que novas falhas ocorram.

10. Gestão De Incidentes De Segurança Da Informação

Todos os colaboradores têm a obrigação de reportar, formal e imediatamente, qualquer incidente ou suspeita de violação de segurança para a Equipe de Segurança da Informação. A não comunicação será considerada falta grave.

11. Descumprimento Da Política

O não cumprimento das diretrizes estabelecidas nesta política sujeitará o infrator a medidas disciplinares, que podem variar de advertência verbal a demissão por justa causa, conforme a gravidade da infração e em conformidade com a legislação trabalhista vigente.

12. Responsabilidades

- Cabe a todos os Colaboradores: Cumprir esta política; utilizar exclusivamente as ferramentas corporativas para comunicação profissional; zelar pelos recursos; comunicar incidentes; e manter o sigilo das informações e senha.
- **Cabe aos Gestores:** Fazer cumprir a política em suas equipes; servir como modelo de conduta; garantir que seus liderados assinem o termo de ciência; e informar o RH e a TI imediatamente em casos de desligamento para a revogação dos acessos.

ATUALIZAÇÃO	REVISÃO	PROCESSO / AUTOR	CLASSIFICAÇÃO
15/12/2025	V2	Departamento de Tecnologia da Informação (TI)	Interna

- **Cabe aos Recursos Humanos:** Incluir as responsabilidades de segurança da informação nos contratos de trabalho e auxiliar nos processos de conscientização e desligamento.
- **Cabe ao Comitê de Segurança da Informação:** Propor alterações nesta política; priorizar investimentos em segurança; e avaliar incidentes graves e suas penalidades.
- **Cabe à Equipe de Segurança da Informação/TI:** Gerenciar os ativos de segurança; monitorar o ambiente; e apoiar na resposta a incidentes e problemas.
- **Cabe ao DPO (Encarregado de Proteção de Dados):** Controlar a conformidade desta PSI com a LGPD, prestar aconselhamento sobre proteção de dados e cooperar com a Autoridade Nacional de Proteção de Dados (ANPD).
- **Sanções:** O não cumprimento das diretrizes estabelecidas nesta política sujeitará o infrator a medidas disciplinares. Tais medidas podem variar de advertência verbal a demissão por justa causa, a depender da gravidade da infração e em conformidade com a legislação trabalhista vigente. A não comunicação de um incidente ou suspeita de violação de segurança será considerada uma falta grave.

13. Ciência Da Política De Segurança Da Informação

A ciência do colaborador com as disposições contidas nesta Política de Segurança da Informação é requisito essencial para seu acesso às informações e aos recursos disponibilizados pela Unimed Adamantina Cooperativa de Trabalhos Médico.

O colaborador manifesta sua ciência com as disposições contidas nesta Política de Segurança da Informação e compromete-se ao cumprimento de todas as suas disposições.

ATUALIZAÇÃO	REVISÃO	PROCESSO / AUTOR	CLASSIFICAÇÃO
15/12/2025	V2	Departamento de Tecnologia da Informação (TI)	Interna

14. HISTÓRICO DE ALTERAÇÕES

EMISSÃO	REVISÃO	DESCRIÇÃO DA ALTERAÇÃO	ELABORADO POR	APROVADO POR
15/12/2025	01	Revisão de versão inicial da política	Tecnologia da Informação	Comitê LGPD

15. Referências

Norma ABNT NBR ISO/IEC 27001 - Tecnologia da informação — Técnicas de segurança — Sistemas de gestão da segurança da informação — Requisitos.

Norma ABNT NBR ISO/IEC 27002 - Tecnologia da informação — Técnicas de segurança — Código de prática para controles de segurança da informação.

Lei Geral de Proteção de Dados Pessoais (LGPD) - Lei Nº 13.709/2018.

Adamantina, 15 de dezembro de 2025.

ATUALIZAÇÃO	REVISÃO	PROCESSO / AUTOR	CLASSIFICAÇÃO
15/12/2025	V2	Departamento de Tecnologia da Informação (TI)	Interna