SUMÁRIO

1. OBJETIVO

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

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 Assis 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 Código de Conduta da Assis (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 APLICAÇÃO

Esta política se aplica a todos os públicos, internos e externos, que manipulam, processam, transportam ou acessam os ativos de informação da Assis, 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 Proteção e Privacidade de Dados.

Esta política se aplica a:

- **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, abrangendo tanto colaboradores quanto terceiros, com o apoio da área de Recursos Humanos para formalização dos contratos de trabalho e do setor Jurídico para a formalização dos contratos de prestação de serviços. O Comitê de Proteção e Privacidade de Dados, com o apoio da alta gestão, deve promover campanhas de conscientização e treinamentos periódicos para garantir que todos as partes interessadas, como colaboradores, cooperados e terceiros 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 e classificadas, no mínimo de acordo em:

- **Públicas** – São documentos sem nenhum dado pessoal e tem sua visualização permitida para qualquer tipo de público;

- **Restritas** – Contém dados pessoais, cuja permissão de acesso é restrita apenas o público interno e/ou para pessoas especificas externas à cooperativa relacionadas a finalidade do tratamento do dado;
- **Confidenciais** - Contém dados pessoais sensíveis, cuja permissão de acesso é restrita apenas o público interno e/ou para pessoas especificas externas à cooperativa, seguindo os critérios estabelecidos relacionadas a finalidade do tratamento do dado.

A ausência de classificação formal ocasiona a classificação automática de "Restrita", devendo ser manuseadas e protegidas com cuidado compatível com sua classificação, não sendo deixadas expostas ou desprotegidas.

Quanto aos controles as 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.

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 e no princípio do menor privilégio. 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, números e preferencialmente caracteres especiais.
- **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.
- **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, a Equipe de suporte técnico, deve revisar os acessos 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 Assis 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 Assis (e-mail corporativo, sistema de telefonia, plataformas de videoconferência e aplicativos de mensagens instantâneas institucionais).
- É expressamente proibido utilizar informações de propriedade da Unimed Assis, de seus clientes ou parceiros para fins pessoais, independentemente do meio de comunicação utilizado, seja aplicativos de mensagens, e-mails, plataformas corporativas ou não corporativas.

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 Assis 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 Gestor de Segurança da Informação, e o dispositivo estará sujeito a revisões de segurança.

8. MONITORAMENTO E AUDITORIA

A Unimed Assis reserva-se o direito de implantar sistemas de monitoramento em estações de trabalho, servidores, 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 a causa 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, recebendo uma identificação única para rastreamento.
- **Análise e Diagnóstico (Análise de Causa Raiz):** 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. Enquanto a solução definitiva é desenvolvida, uma solução de contorno 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 as áreas de Governança, Riscos e Compliance e Tecnologia de Informação. A não comunicação será considerada falta grave.

11. DESCUMPRIMENTO DA POLÍTICA

O não cumprimento das diretrizes estabelecidas nesta política sujeitará o infrator — seja colaborador, cooperado ou terceiro — às medidas disciplinares cabíveis, conforme a gravidade da infração e em conformidade com a legislação vigente, contratos firmados, estatuto, regimentos internos e/ou código de conduta. As penalidades podem variar desde advertência verbal, advertência por escrito, suspensão, demissão sem justa causa ou demissão por justa causa, até o desligamento do cooperado, a rescisão do contrato de trabalho ou de prestação de serviços e a aplicação de multa prevista em contrato. Todas as medidas serão aplicadas de forma proporcional à gravidade da infração, garantindo o cumprimento das normas internas e a preservação da integridade e segurança das informações da Unimed Assis.

12. RESPONSABILIDADES

- **Cabe a todos os Colaboradores**: Cumprir esta política; utilizar as ferramentas corporativas para comunicação profissional; zelar pelos recursos; comunicar incidentes; e manter o sigilo das informações e senha.
- **Cabe aos cooperados e terceiros**: Cumprir esta política e manter o sigilo das informações.
- **Cabe aos Gestores**: Fazer cumprir a política em suas equipes, fornecedores e cooperados; servir como modelo de conduta; garantir que suas partes interessadas tenham ciência da política; e informar o RH e a TI imediatamente em casos de desligamento para a revogação dos acessos.
- **Cabe aos Recursos Humanos:** formalizar os contratos de trabalho com as responsabilidades de segurança da informação e auxiliar nos processos de conscientização e desligamento.

- **Cabe a Área de Governança, Riscos e Compliance** apoiar na formalização dos contratos de prestação de serviço para conter as responsabilidades de segurança da informação e dar suporte no registro de incidentes e problemas.
- **Cabe ao Comitê de Proteção e Privacidade de Dados:** Propor alterações nesta política; priorizar investimentos em segurança; e avaliar incidentes graves e suas penalidades.
- **Cabe à Equipe de Tecnologia da Informação**: 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).
-

13. CIÊNCIA DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

A ciência das partes interessadas quanto às disposições desta Política de Segurança da Informação é requisito indispensável para o acesso às informações e aos recursos disponibilizados pela Unimed Assis. Ao assinar o Código de Conduta, as partes interessadas declaram estar cientes das diretrizes estabelecidas e comprometem-se a cumprir integralmente todas as disposições, incluindo a conduta esperada de seguir rigorosamente a Política de Segurança da Informação.

14. DISPOSIÇÕES FINAIS

Esta política entrou em vigor em 16 de setembro de 2020 e passou por revisões e aprovações pelo Conselho de Administração em 3 de fevereiro de 2021, 13 de fevereiro de 2023 e 9 de dezembro de 2024. A revisão mais recente foi realizada e aprovada pelo Conselho de Administração em 8 de dezembro de 2025.

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.