ANS 30.439-5 DSGS.3050

Política de Segurança da Informação

Edição: 005

Unimed Inconfidentes

somos coop

A Política de Segurança da Informação (PSI) tem como objetivo estabelecer as diretrizes e requisitos para preservar a confidencialidade, integridade e disponibilidade da informação dentro da Unimed Inconfidentes, objetivando a proteção de seus ativos e adequando as necessidades de negócio à proteção legal da empresa e do indivíduo.

Boa leitura a todos!

Siglas e Definições

Ataque: evento de exploração de vulnerabilidades, ocorre quando um atacante tenta executar ações maliciosas, como invadir um sistema, acessar informações confidenciais ou tornar um serviço inacessível;
Incidente de Segurança: qualquer ato, suspeita, ameaça ou circunstância que comprometa a confidencialidade, integridade ou a disponibilidade de informações que estão em posse da Unimed Inconfidentes ou que ela venha a ter acesso;
Banco de dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico;
Compartilhamento: comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados;
Violação de Privacidade: qualquer violação à legislação aplicável ou conduta e evento que resulte na destruição acidental ou ilícita dos dados, bem como sua perda, roubo, alteração, divulgação ou acesso não autorizado, danos ou desvio de finalidade em seu tratamento;
Confidencialidade: Garantia de que a informação estará disponível ou será divulgada somente para indivíduos, entidades pessoas ou processos devidamente autorizados;
Integridade: Garantia de que a informação, armazenada ou em trânsito, não sofrerá qualquer modificação não autorizada, seja esta intencional ou não;
Disponibilidade: Garantia de que a informação estará disponível sempre que se fizer necessária;

Abrangência

Este documento é aplicável a todos os diretores, membros de conselho, membros de comitês, cooperados, colaboradores, estagiários, jovens aprendizes, terceiros, parceiros, prestadores e fornecedores em quaisquer das dependências da Unimed Inconfidentes ou locais onde estes se façam presentes através da utilização, manuseio ou processamento das informações, cujo acesso seja controlado.

Diretrizes

1. Responsabilidades

O Responsável pela Segurança da Informação coordena as áreas técnicas, as áreas de apoio e as áreas de negócio para o desenvolvimento e implantação de projetos, procedimentos, ações, instruções e normativos que possibilitem a operacionalização, comunicação e manutenção desta política.
A alta direção e os gestores devem garantir que as diretrizes presentes nessa política sejam consideradas no projeto dos processos, sistemas de informação e controles, assegurando que os recursos necessários para a segurança da informação estejam disponíveis, comunicando a importância, orientando e apoiando no cumprimento das diretrizes propostas.
Os usuários dos ativos da Unimed Inconfidentes devem seguir as diretrizes desta política, sendo responsáveis pela proteção física e lógica contra danos e prejuízos materiais, morais e intelectuais, assim como pela manutenção do sigilo profissional e confidencialidade das informações de seu conhecimento em função do cumprimento de suas atividades na empresa.

2. Diretrizes Gerais

I. Materiais de cunho sexual não poderão ser expostos, acessados, armazenados, distribuídos, editados, impressos ou gravados por meio de qualquer recurso;

II. Documentos de condutas consideradas ilícitas, como por exemplo apologia ao tráfico de drogas e pedofilia, são expressamente proibidos e não devem ser acessados, expostos, armazenados, distribuídos, editados, impressos ou gravados por meio de qualquer recurso;

III. O uso, a cópia ou a distribuição não autorizada de softwares que tenham direitos autorais, marca registrada ou patente são expressamente proibidos;

IV. O uso, a cópia ou a distribuição não autorizada de conteúdo áudio visual, em mídia física ou digital, que tenham direitos autorais, marca registrada ou patente são expressamente proibidas;

V. Independentemente da forma apresentada, compartilhada ou armazenada, a informação deve ser utilizada em alinhamento com o Sistema de Gestão da Qualidade e para a sua finalidade devidamente autorizada, respeitado a classificação de níveis de acesso, sendo sujeita a monitoração e auditoria;

VI. Os usuários da informação não deverão testar fragilidades de segurança, pois tais eventos serão interpretados como uso impróprio do sistema ou exploração de vulnerabilidades;

VII. Cada usuário é responsável por manter sua senha confidencial, pois se utilizada por terceiros, todas as operações efetuadas com a senha concedida, serão de exclusiva responsabilidade do usuário.

VIII. Ao usuário é expressamente vedada a realização de manutenção física e lógica em ativos da organização, incluindo instalação, desinstalação ou solicitação a terceiros, sem prévio conhecimento e acompanhamento da Gestão de Tecnologia da Informação, ou da pessoa por ela designada.

IX. Não é permitido aos colaboradores, cooperados, parceiros, clientes, fornecedores, associadas e terceiros em geral, tirar fotos, gravar, filmar, publicar e/ou compartilhar imagens dos ambientes internos da Unimed Inconfidentes que possam:

a. Comprometer a segurança dos demais colaboradores e diretoria executiva;
b. Comprometer o sigilo das informações;
c. Impactar negativamente a imagem da Unimed Inconfidentes, outros colaboradores, cooperados, beneficiários, clientes, parceiros e visitantes.

3. Classificação da Informação

A informação é um importante ativo para a operação das atividades institucionais da Unimed Inconfidentes, para garantir que a informação seja adequadamente manuseada e protegida, toda e qualquer informação deve possuir um responsável e ser classificada num nível de restrição de acesso, conforme a importância para os negócios da Unimed Inconfidentes e seja adequadamente protegida de quaisquer riscos e ameaças que possam comprometer o negócio.

A Unimed Inconfidentes classifica as informações conforme os padrões de classificação de ativos da informação descritos a seguir:

- Confidencial é o mais alto nível de segurança dentro da organização, sendo considerada as informações em que a perda de confidencialidade causará eventual comprometimento das operações, resultando em perdas financeiras, de competitividade, de imagem, risco de ações judiciais à Unimed Inconfidentes e a seus executivos.

- Restrita é um nível médio de confidencialidade, sendo considerada as informações estratégicas que devem estar disponíveis apenas para grupos restritos de colaboradores, cooperados ou prestadores de serviço.

- Uso interno representa um baixo nível de confidencialidade, sendo considerada as informações que não podem ser divulgadas para pessoas de fora da organização, mas que, caso isso aconteça, não causarão grandes prejuízos.

- Pública são os dados que não necessitam de proteção sofisticada contra vazamentos, pois podem ser de conhecimento público, contudo eles necessitam de maior atenção quanto aos requisitos de disponibilidade e integridade.

4. Segregação de Funções

A segregação de funções conflitantes tem o objetivo de reduzir as oportunidades de modificação não autorizada ou não intencional, ou uso indevido dos ativos da organização.

A segregação de funções conflitantes na admissão e movimentação funcional de colaborador é realizada pelo gestor da área, garantindo que as atividades exercidas pelo colaborador estejam alinhadas no momento da definição do perfil de acesso.

Para os processos conflitantes na contratação de prestadores de serviço, rede credenciada, terceiros entre outros, é de responsabilidade do gestor responsável pela contratação.

5. Acordos de Confidencialidade

A disponibilização de informações, seja para execução de projetos ou elaboração de propostas de consultorias, auditorias e fornecedores, deverá ser precedida da assinatura de um Acordo de Confidencialidade.

Os gestores devem garantir que todos os contratos com prestadores de serviços, colaboradores ou demais entidades que irão se relacionar com a Unimed Inconfidentes e que venham a acessar informações privilegiadas contenha, obrigatoriamente, a cláusula de sigilo e confidencialidade, mesmo após rescisão contratual, a não observância de determinadas cláusulas implicará em falta grave.

6. Gestão de Mudanças

Todos os projetos e iniciativas que envolvam diversas atividades e que possam impactar na interação entre setores e no atendimento ao cliente externo, devem ser direcionadas a área de Gestão de Projetos e Mudanças, conforme alinhado no procedimento sistêmico "Solicitar e Gerir Mudanças", para que sejam verificados os potenciais riscos de segurança da informação e os controles necessários durante os estágios iniciais os projeto, independentemente do tipo de projeto, garantindo sua conformidade com as legislações vigentes e diretrizes dessa política.

7. Proteção e Continuidade do Uso da Informação

Os gestores asseguram que toda a informação da organização seja protegida para que não seja alterada, acessada e destruída indevidamente, utilizando de controles de acessos apropriados as atividades do usuário, conscientizando sobre o uso dos ativos da organização e promovendo treinamentos.
Os locais onde se encontram os recursos de informação possuem proteção e controle de acesso físico compatível com o seu nível de criticidade.

Toda informação utilizada nos processos críticos, conforme "Mapa de Contexto" definido no sistema de gestão da qualidade, deve possuir, pelo menos, uma cópia de segurança atualizada e guardada em local remoto, com proteção equivalente ao local principal. Esta informação deve ser suficiente para a garantir a eficácia do Plano de Contingência.

A criação das cópias de segurança considera os aspectos legais, históricos, auditorias e recuperação do ambiente.

Os gestores asseguram que os recursos tecnológicos, de infraestrutura e os ambientes físicos onde são realizadas as atividades operacionais da organização sejam protegidas contra situação de indisponibilidade, definindo e implementando medidas de prevenção e recuperação, para situações de desastre e contingências.

Todos os procedimentos que possibilitam a proteção da informação e a continuidade do seu uso devem ser documentados, de tal forma que possibilite que a organização continue a operacionalização desses procedimentos, mesmo na ausência do usuário responsável.

8. Conscientização

O responsável pela segurança da informação, promove treinamentos e campanhas de conscientização, semestralmente ou quando esta política passar por revisão, de forma a garantir o entendimento da Política de Segurança da Informação, sua internalização e suas contribuições para a eficácia do sistema de segurança da informação, por todas as partes interessadas pertinentes.

9. Controle de Acesso

O acesso ao Centro de Processamento de Dados (CPD) deve ser controlado e monitorado pelo setor de Tecnologia da Informação de forma a limitar o acesso de pessoas não autorizadas.

Dentro das dependências da Unimed Inconfidentes, cada pessoa, independentemente de seu cargo ou função, deverá usar um crachá de identificação de forma visível.

O controle de acesso à informação e aos recursos de processamento da informação é realizado pelo responsável por cada sistema que acessa a informação na organização. O responsável considera junto ao gestor da área a necessidade do colaborador ou provedor de serviços de conhecer a informação e a necessidade de uso no desempenho de sua atividade profissional, garantindo que nenhuma das diretrizes desta política ou legislação vigente seja infringida.

Cada usuário está autorizado a acessar apenas as informações e ambientes previamente designados. Qualquer tentativa deliberada de acesso a ambientes não autorizados será tratada conforme as penalidades estabelecidas no *Capítulo 12 - Penalidades.*

O acesso à informação armazenada e processada no ambiente de tecnologia é individual e intransferível. Este acesso acontece através da identificação e da autenticação do usuário. Os dados para a autenticação do usuário devem ser mantidos em segredo.

Todo usuário, independentemente do vínculo com a Unimed Inconfidentes, cargo ou função, deve zelar para que qualquer material, contendo dados pessoais, regras de negócio, contratos, políticas, procedimentos internos, planos estratégicos e marketing, propostas comerciais, descrição de sistemas, produtos ou programas automatizados, dentre outras informações que esteja sob sua guarda, seja mantida inacessível a pessoas não autorizadas, principalmente durante sua ausência do posto de trabalho.

Todos os usuários devem ter seus acessos removidos durante o período de férias, licença maternidade ou afastamento de suas atividades profissionais, devendo o gestor responsável, solicitar ao setor de Tecnologia da Informação o bloqueio dos acessos.

O responsável por cada sistema deve remover os direitos de acesso à informação e aos recursos de processamento da informação dos usuários logo após o encerramento das atividades, contratos ou acordos, ou ajustados após a mudança de atividade.

10. Computação Pessoal e Móvel

Os recursos de tecnologia da organização disponibilizados para os usuários têm como objetivo a realização de atividades profissionais, o tratamento de dados da organização deverá ser realizado em ativos da organização autorizados.

As mensagens do correio eletrônico e aplicativos de chat, disponibilizados para os usuários obrigatoriamente são escritas em linguagem profissional, que não comprometa a imagem da cooperativa, não vá de encontro a legislação vigente e nem aos princípios éticos da organização. Cada usuário é responsável pela conta de correio eletrônico e aplicativo de chat que lhe foi disponibilizada pela cooperativa. O usuário não deve ter expectativa de sigilo da sua conta de correio eletrônico e chat disponibilizada pela organização para o seu uso pessoal.

Os serviços de internet serão cedidos a todos os colaboradores, prestadores de serviço e terceiros autorizados, presentes nas dependências da Unimed Inconfidentes e suas filiais, para a realização de atividades profissionais, devendo o gestor da área ou setor acompanhar o bom uso deste serviço.

O acesso à internet pelos usuários é de responsabilidade do gestor da área, devendo o gestor restringir os acessos e realizar o monitoramento de uso do serviço junto ao setor de Tecnologia da Informação.

11. Incidentes de Segurança da Informação

O usuário da informação deverá comunicar imediatamente o seu gestor e a área de Segurança da Informação qualquer Incidente de Segurança da Informação, registrando-o no sistema TopDesk, ou outro que vier a substituir para o registro, fornecendo o máximo de informações possíveis para auxiliar o processo de Responder Incidente de Segurança e Privacidade de Dados.

12. Penalidades

A identificação do tratamento de dados, condutas e ações em dissonância às diretrizes desta política poderá ensejar as seguintes sanções: advertência verbal ou escrita, suspensão, rescisão contratual, abertura de processo disciplinar/administrativo e aplicação de penalidades contratualmente definidas, a depender do vínculo da parte com a Unimed Inconfidentes.

Essas penalidades não interferem na possibilidade de direcionamento de ações ético disciplinares, cíveis e criminais, se cabíveis, aos órgãos externos competentes.

13. Disposições Finais

A utilização das informações do ambiente de tecnologia ou do ambiente convencional pelos usuários contemplados por esta política, não deve infringir as normas, documentos institucionais, demais políticas, Código de Conduta ou a legislações vigentes.

A segurança e proteção da informação é uma responsabilidade contínua de cada usuário da cooperativa em relação às informações que acessa e gerencia.

Todos os usuários devem utilizar a informação da cooperativa, de acordo com as determinações desta Política de Segurança da Informação.

O não cumprimento desta política e/ou dos demais instrumentos normativos que complementarão o processo de segurança constitui em falta grave, e o usuário está sujeito a penalidades administrativas e/ou contratuais.

Registros

AN.SI.001 – Termo de Sigilo e Confidencialidade

Legislação

Lei nº 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados Pessoais (LGPD).
Lei nº 12.965, de 23 de abril de 2014 – Marco Civil da Internet

Referências Bibliográficas

ABNT, NBR ISO/IEC 27001 Tecnologia da informação - Técnicas de segurança - Sistemas de gestão da segurança da informação - Requisitos. Rio de Janeiro: Associação Brasileira de Normas Técnicas, 2013.

ABNT, NBR ISO/IEC 27002 Tecnologia da informação - Técnicas de segurança - Código de prática para controles de segurança da informação. Rio de Janeiro: Associação Brasileira de Normas Técnicas, 2013.

FONTES, Edison. Políticas e Normas para a Segurança da Informação. 1. ed. Rio de Janeiro, 2012.

HINTZBERGEN, J. HINTZBERGEN, K. SMULDERS, A. et al. Fundamentos de Segurança da Informação. 1. ed. Rio de Janeiro, 2018.

Histórico de Revisões

Revisão: 000 - inicial **Data:** 01/07/2018, **Responsável:** Adalmir Moreira

Revisão: 001 - Atualizações nos itens: Ficha técnica, I - conceitos, II – objetivos, IV - normas da política de segurança, 2. Correio eletrônico – e-mail, 3 – internet, 4 – computador e recursos tecnológicos, V – penalidades, **Data:** 09/04/2020 **Responsável:** Anderson Rodrigues

Revisão: 002 Atualizações nos itens: Responsável: Analista de Tecnologia da Informação Exclusão da logo do selo de e Governança e Sustentabilidade, **Data:** 30/04/2020, **Responsável:** Anderson Rodrigues

Revisão: 003 Atualizações nos itens: Alteração total do documento **Data:** 28/09/2020, **responsável:** Ramon Willer

Revisão: 004 Alteração na estrutura do documento, inclusão de diretrizes gerais e restrições e acordo de confidencialidade. **Data:** 24/02/2022, **responsável:** Ramon Willer

Revisão: 005 Alteração no controle de acesso e responsabilidades do Recursos Humanos **Data:** 14/11/2023, **responsável:** Ramon Willer

Aprovação

Documento aprovado pelo Conselho de Administração em 16/01/2024.

Diretor Presidente: Wilson Pena
Diretor Financeiro: Vicente de Paulo Silva
Diretor Administrativo: André Pereira Pinto
Diretor Vogal: Felipe de Oliveira Tinoco
Diretor Vogal: Navarro Santos Gribel
Diretor Vogal: Thiago Marton Azzi
Diretor Vogal: Lucimar Gonçalves S. Assunção
Diretor Vogal: Lander Braga Calais C. Pinto

Unimed
Inconfidentes

somos coop