

	Título:	Código do Procedimento
	POLÍTICA DE SEGURANÇA DA INFORMAÇÃO - PSI	
Número de Revisão:	Data de Aprovação:	Página:
2	13/02/2023	1 / 8
Elaboração: Helio Henrique Kuronuma		Aprovação: Conselho de Administração

SUMÁRIO

1. OBJETIVO.....	1
2. ÂMBITO DE APLICAÇÃO.....	1
3. DEFINIÇÕES.....	2
4. DIRETRIZES	2
4.1. UTILIZAÇÃO DA INFORMAÇÃO	3
4.2. AMBIENTE FÍSICO	4
4.2.1. ACESSO E PERMANÊNCIA DE EMPREGADOS, PRESTADORES DE SERVIÇOS E VISITANTES..	4
4.2.2. SEGURANÇA NO AMBIENTE DE TRABALHO	4
4.3. AMBIENTE LÓGICO	5
4.3.1. CONTAS E SENHAS DE ACESSO A SISTEMAS.....	6
4.3.2. PERFIS DE ACESSO A SISTEMAS	6
4.3.3. E-MAIL.....	6
4.3.4. INTERNET	7
4.3.5. ATIVOS DE PROCESSAMENTO DE DADOS HARDWARE.....	7
4.3.6. ATIVOS DE PROCESSAMENTO DE DADOS SOFTWARE	7
4.4. GERENCIAMENTO DE RISCOS.....	8
4.5. PRAZOS DE REVISÕES	8
4.6. AUDITORIA DE SEGURANÇA DA INFORMAÇÃO	8
5. REGRAS DE CONSEQUÊNCIA.....	8
6. DISPOSIÇÕES FINAIS.....	8

1. OBJETIVO

Estabelecer as diretrizes de segurança da informação, visando garantir os princípios básicos de integridade, confidencialidade, disponibilidade, autenticidade e legalidade das informações da Cooperativa.

2. ÂMBITO DE APLICAÇÃO

Operadora de saúde, farmácia Unimed, Rede assistencial própria da Unimed Assis e suas partes Interessadas.

	Título: POLÍTICA DE SEGURANÇA DA INFORMAÇÃO - PSI	Código do Procedimento PL DIR-0022
Número de Revisão: 2	Data de Aprovação: 13/02/2023	Página: 2 / 8
Elaboração: Helio Henrique Kuronuma		Aprovação: Conselho de Administração

3. DEFINIÇÕES

Ativos - Consiste em todo e qualquer bem tangível ou intangível pertencente, administrado, locado ou custodiado pela Unimed Assis, sejam informações, sistemas ou dispositivos fixos e móveis.

Colaborador - Empregados, estagiários, menores aprendizes, que atuam na Cooperativa. Para fins de alcance de políticas corporativas, ficam incluídos os terceiros, os médicos do corpo clínico e residentes das unidades assistenciais próprias.

Confidencialidade - Consiste na propriedade da informação que determina que esta não esteja disponível ou não seja exposta a indivíduos, entidades e/ou processos que não tenham sido previamente autorizados pelo proprietário.

Disponibilidade - Consiste na propriedade da informação que garante que esta esteja disponível, sempre que necessário, para o uso legítimo, ou seja, por aqueles usuários autorizados pelo seu proprietário visando à continuidade do negócio.

Integridade - Consiste na propriedade da informação que garante que a informação manipulada mantenha todas as características originais estabelecidas pelo seu proprietário, incluindo controle de mudanças e garantia do seu ciclo de vida (nascimento, manutenção, armazenamento e descarte).

Segurança da Informação - Consiste na preservação da confidencialidade, da integridade e disponibilidade da informação; adicionalmente, outras propriedades, tais como autenticidade, responsabilidade e confiabilidade da informação.

Prontuário do paciente - É o conjunto de documentos padronizados, ordenados e concisos, destinados ao registro de todas as informações referentes aos cuidados médicos e paramédicos prestados ao paciente.

4. DIRETRIZES

A Unimed Assis considera que suas informações são bens importantes. Seu uso deve ser dimensionado para divulgação correta e no tempo devido, objetivando estabelecer uma comunicação eficiente e esclarecedora com os diversos públicos. A segurança da informação está baseada em 3 princípios: confidencialidade, integridade e disponibilidade.

Na Unimed Assis, todos os colaboradores têm o dever de conhecer e cumprir essas diretrizes, como responsáveis pela preservação da confidencialidade, integridade e disponibilidade das informações, e somente sendo permitido a utilização das informações da Cooperativa para fins internos.

Todos devem preservar a imagem e a integridade de clientes, médicos e colaboradores, observando sempre o sigilo das informações.

A utilização de internet, e-mail e mídias sociais por qualquer profissional que se relaciona com a Unimed Assis deve ser feita de forma responsável, ética e seguir as premissas de segurança da informação.

	Título:	Código do Procedimento
	POLÍTICA DE SEGURANÇA DA INFORMAÇÃO - PSI	PL DIR-0022
Número de Revisão: 2	Data de Aprovação: 13/02/2023	Página: 3 / 8
Elaboração: Helio Henrique Kuronuma		Aprovação: Conselho de Administração

A informação corporativa pode se apresentar em diferentes formas: estratégia, conhecimento, indicador, estatística, projeto, pesquisa, ação, receita, prática, parecer, análise, experiência, inspeção, especificação, configuração, resultado, dentre outras, e poderá existir como dados armazenados em computadores, dispositivos de armazenamento, dispositivos móveis, caixas de e-mail, escritas e/ou impressas em papel, transmitidas eletronicamente ou até em conversas.

4.1. UTILIZAÇÃO DA INFORMAÇÃO

A Unimed Assis monitora as informações corporativas, podendo estender ao recebimento, envio e armazenamento, utilização e manuseio, sem prévia notificação às áreas ou aos colaboradores, visando garantir e proteger o sigilo e a segurança das mesmas.

A utilização para outros fins e/ou divulgação de assuntos relacionados especialmente, mas não se limitando, a aspectos operacionais, comerciais, sobre pacientes, sobre cooperados, jurídicos, regulatórios, financeiros, contábeis, tecnológicos, sobre marketing, epidemiológico, assistencial ou qualquer outro que se relacione às atividades da Cooperativa obriga o colaborador a obter a autorização formal da Unimed Assis.

O conteúdo dos prontuários do paciente é amparado pelo sigilo profissional, conforme destacado na Constituição Federal e nos Conselhos de Classe dos profissionais da Saúde. O acesso às informações de pacientes é restrito aos profissionais envolvidos diretamente no atendimento ao cliente, devendo ser compartilhadas apenas com terceiros previamente autorizados e homologados, como por exemplos fornecedores de serviço de diagnósticos, serviço de transporte, serviço de guarda física de documentos, serviço de hospedagem de softwares, entre outros.

O sigilo das informações é responsabilidade de todos os colaboradores da Unimed Assis, seus cooperados e rede credenciada.

É proibida a utilização não autorizada de informações da cooperativa, de pacientes ou comentários pessoais que afetem a imagem da instituição em mecanismos de comunicação instantânea, bem como em e-mails, redes sociais ou quaisquer outros meios. Para mitigar o risco compartilhamento indevido as informações assistenciais, quando necessárias à atividade profissional, devem ser discutidas apenas pessoalmente, por telefone, por e-mail ou WhatsApp (ou instrumento de comunicação semelhante) desde que respeitadas às regras impostas pelos instrumentos normativos que tratam do sigilo e da proibição de ter pessoas alheias à medicina compondo grupos de discussão de casos onde se abordam formas de diagnosticar e da aplicação de condutas terapêuticas.

Todos os colaboradores, cooperados e rede credenciada que tenham acesso a informações da Unimed Assis ou sob a guarda da Unimed Assis - pessoais, sensíveis ou restritas - não poderão utilizá-las para fins pessoais ou divulgá-las a pessoas não autorizadas. As restrições incluem a utilização de dados em palestras, apresentações, publicações ou qualquer ato de divulgação para o público externo sem aprovação prévia da liderança responsável.

	Título: POLÍTICA DE SEGURANÇA DA INFORMAÇÃO - PSI	Código do Procedimento PL DIR-0022
Número de Revisão: 2	Data de Aprovação: 13/02/2023	Página: 4 / 8
Elaboração: Helio Henrique Kuronuma		Aprovação: Conselho de Administração

As informações devem ser classificadas como:

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 específicas 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 específicas 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.

O armazenamento das informações é realizado por tempo determinado pela Cooperativa e/ou legislação vigente.

4.2. AMBIENTE FÍSICO

4.2.1. ACESSO E PERMANÊNCIA DE EMPREGADOS, PRESTADORES DE SERVIÇOS E VISITANTES

Na Unimed Assis todos colaboradores devem estar devidamente identificados, com uso do crachá em local visível quando estiverem dentro dos prédios administrativos e unidades de atendimento, retirando-o ao sair das dependências.

Os prestadores de serviços terceirizados deverão estar identificados com crachás temporários e deverão ser acompanhados por um representante da área requisitante pelo serviço.

O acesso de visitantes é de responsabilidade das áreas visitadas, cabendo zelar pela aprovação, programação e acessos aos locais, com os cuidados necessários quanto ao registro de imagens e acesso às informações por qualquer meio. Os locais onde houver informações confidenciais devem ser excluídos das rotas de visitantes e da programação de qualquer visita.

4.2.2. SEGURANÇA NO AMBIENTE DE TRABALHO

A Unimed Assis não permite a divulgação de imagens da Cooperativa, de suas instalações e de colaboradores identificados com crachás e/ou uniformizados, bem como o compartilhamento de informações restritas, pessoais ou sensíveis em sites pessoais, redes sociais, aplicativos ou qualquer meio de comunicação sem o consentimento da Unimed Assis. Não é autorizada a exposição de imagem dos nossos clientes, a não ser que seja necessário e aprovado por escrito pela pessoa e pela Unimed Assis. Também não é permitida a divulgação de informações inverídicas de qualquer natureza em qualquer meio de comunicação.

	Título:	Código do Procedimento
	POLÍTICA DE SEGURANÇA DA INFORMAÇÃO - PSI	PL DIR-0022
Número de Revisão: 2	Data de Aprovação: 13/02/2023	Página: 5 / 8
Elaboração: Helio Henrique Kuronuma		Aprovação: Conselho de Administração

Os colaboradores têm o dever de assegurar que informações sensíveis, tanto em formato digital quanto físico, e ativos não sejam deixados desprotegidos em locais de trabalho pessoais ou públicos quando não estão em uso, mesmo que seja por um curto período de tempo ou ao final do dia.

Além da proteção contra acesso não autorizado, as informações devem ser protegidas contra desastres tais como incêndios, terremotos, inundações ou explosões.

No acesso à informação, somente devem ser usados recursos tecnológicos devidamente homologados e autorizados.

As informações com classificação “Restrita” ou “Confidencial” deverão ser descartadas utilizando métodos que impeçam a reconstrução, tal como a utilização de fragmentadoras.

Os colaboradores devem zelar pela guarda e integridade das informações nos ambientes onde atuam, protegendo os locais onde existem armazenamento de informações, sejam físicos ou eletrônicos, por meio da guarda ou proteção por senha, além da racionalização de recursos que realizam cópia de documentos.

As informações visuais em ambientes de reuniões requerem o mesmo grau de segurança, sigilo e zelo para não visualização por pessoas não autorizadas. O colaborador deve descartar apropriadamente tais informações, de acordo com a sensibilidade da informação. A falta de cuidado com uma área de trabalho pode levar ao comprometimento de informações pessoais e organizacionais.

4.3. AMBIENTE LÓGICO

O acesso às informações pelos colaboradores, como usuários de sistemas, é restrito às necessidades inerentes ao desempenho de suas funções e atribuições. Não é permitida a manipulação ou a utilização de informações ou contas de acesso às quais a pessoa não tem necessidade ou direito de uso.

O ambiente de armazenamento das informações deve ser apropriado e protegido contra sinistros e acessos não autorizados, garantindo a integridade, disponibilidade e confiabilidade das informações.

A Unimed Assis adota medidas técnicas apropriadas para prevenir que ativos de informação possam ser acessados ilegalmente, modificados sem autorização, falsificados, destruídos ou sofram interferências que afetem a confidencialidade, integridade e/ou disponibilidade das informações que eles suportam.

Todo sistema de informação desenvolvido ou adquirido pela Unimed Assis, que se utilize ou tenha acesso à informação confidencial, deve obrigatoriamente possuir uma especificação formalizada que tem de levar em conta a segurança dos sistemas, o controle de acesso e as devidas especificações para contingência.

Os processos de implantação de sistemas de informação devem respeitar as premissas de segregação de funções e de ambientes para serem executados. Mecanismos e soluções de continuidade

	Título: POLÍTICA DE SEGURANÇA DA INFORMAÇÃO - PSI		Código do Procedimento PL DIR-0022
	Número de Revisão: 2	Data de Aprovação: 13/02/2023	Página: 6 / 8
Elaboração: Helio Henrique Kuronuma		Aprovação: Conselho de Administração	

são identificados, definidos, implementados e mantidos para os processos de negócios considerados críticos para a Unimed Assis.

A Cooperativa não se responsabiliza por atualização, manutenção e garantia de conectividade de dispositivos que não sejam de sua propriedade ou não tenham sido homologados. É de responsabilidade do proprietário o uso de mecanismos de proteção em seus equipamentos.

A Unimed Assis reserva para si o direito de monitorar, auditar e intervir nos acessos de dados que trafegam na internet de modo a salvaguardar os interesses corporativos de acordo com a lei 12.965 (Marco Civil da Internet) consonantes com os objetivos dessa política.

4.3.1. CONTAS E SENHAS DE ACESSO A SISTEMAS

Na Unimed Assis toda conta de acesso a sistemas terá seu proprietário ou responsável unicamente e claramente identificado. Qualquer ação executada por intermédio de uma conta será de inteira responsabilidade de seu proprietário.

A senha de acesso de cada usuário é pessoal e intransferível, sendo do colaborador ou das partes interessadas a responsabilidade por garantir seu sigilo.

A Cooperativa utiliza procedimentos e mecanismos de proteção e de gerenciamento de senhas visam a manutenção da segurança das contas de acessos e às informações.

4.3.2. PERFIS DE ACESSO A SISTEMAS

Todos os perfis de acesso ao ambiente de produção dos sistemas são concedidos respeitando-se os princípios de segregação de funções. Conflitos dessa natureza serão permitidos apenas mediante criação de controle compensatório pela área solicitante devidamente documentado e posteriormente aprovado.

A concessão dos acessos ao ambiente de infraestrutura de produção por parte de analistas e prestadores de serviço da TI deverá ser realizada de forma temporária, devidamente documentada e aprovada.

4.3.3. E-MAIL

O e-mail corporativo é uma ferramenta de trabalho, comunicação e apoio para os processos de negócios da Cooperativa, não podendo ser utilizado para fins pessoais. Com razão análoga, as informações de trabalho não podem ser trafegadas utilizando e-mails pessoais.

O e-mail corporativo é de uso exclusivo para o exercício das suas atividades, não devendo ser utilizado para cadastro em sites comerciais, redes pessoais ou qualquer plataforma que vise a interesses particulares.

Caso ocorra o envio de e-mail contendo informações restritas ou confidenciais para o destinatário errado, o colaborador se obriga a reportar a falha para o DPO.

	Título: POLÍTICA DE SEGURANÇA DA INFORMAÇÃO - PSI	Código do Procedimento PL DIR-0022
Número de Revisão: 2	Data de Aprovação: 13/02/2023	Página: 7 / 8
Elaboração: Helio Henrique Kuronuma		Aprovação: Conselho de Administração

4.3.4. INTERNET

A Internet é ferramenta de trabalho para o desenvolvimento de atividades, processos, pesquisas, tecnologias e competências. A Unimed Assis mantém regras de utilização e bloqueio de acesso a determinados sites, caixas de e-mail, conteúdos, anexos, emitentes, destinatários, assinaturas, notas, limites de tráfego e armazenamentos.

A Unimed Assis não autoriza a utilização dos meios de comunicação da Cooperativa para divulgar mensagens com conteúdo ilegal, pornográfico, com qualquer sentido discriminatório, de cunho religioso, político-partidário, ideológico ou em desacordo com os princípios éticos e morais da Unimed Assis.

Ao cadastrar no perfil das redes sociais, que é um colaborador da Unimed Assis, o profissional não deve realizar qualquer ação que impacte a marca ou contrarie os valores da Cooperativa.

4.3.5. ATIVOS DE PROCESSAMENTO DE DADOS HARDWARE

Na Cooperativa, os ativos de processamento de dados são classificados quanto a critérios de criticidade e disponibilidade para os negócios da organização.

Os locais que hospedam ativos de processamentos de dados têm níveis adequados e são controlados de segurança física.

A Unimed Assis homologa e controla os ativos de processamentos de dados, incluindo equipamentos e ativos de tecnologia.

É proibida a saída de qualquer equipamento de propriedade da empresa pelo colaborador, exceto se houver autorização por expresso neste sentido formalizada por documento escrito e assinado.

A entrada e conseqüente uso de equipamentos de informática pessoais tais como celulares, tablets e notebooks, deverá ser autorizada pela empresa se for necessária utilização da rede. Em hipótese alguma a empresa será responsabilizada por danos no equipamento pessoal do colaborador ou ainda em casos de furto ou roubo.

4.3.6. ATIVOS DE PROCESSAMENTO DE DADOS SOFTWARE

A Unimed Assis homologa e controla os softwares e se dá o direito de excluir e bloquear o uso de softwares não autorizados sem comunicação prévia. Os critérios padrões de utilização são: softwares licenciados ou open source (gratuitos), que não apresentam risco de vazamento de dados.

É proibido downloads de arquivos de extensões tipo: exe, .mp3, .wav, .bat, .com, .sys, .scr, .ppt, .mpeg, .avi, .rmvb, .dll, e de programas de entretenimento ou jogos, exceto os estritamente relacionados aos serviços inerentes à função do colaborador com vistas às atividades da empresa.

É proibido o uso de jogos, inclusive os da Internet (onlines).

	Título:	Código do Procedimento
	POLÍTICA DE SEGURANÇA DA INFORMAÇÃO - PSI	PL DIR-0022
Número de Revisão: 2	Data de Aprovação: 13/02/2023	Página: 8 / 8
Elaboração: Helio Henrique Kuronuma		Aprovação: Conselho de Administração

4.4. GERENCIAMENTO DE RISCOS

Os riscos à segurança da informação são continuamente avaliados e monitorados, considerando-se as ameaças e vulnerabilidades que possam causar impactos ou danos aos processos de negócios e pessoas.

Os sistemas de proteção quanto às ameaças oriundas de ambientes externos e internos ao ambiente computacional devem ser mantidos, atualizados e monitorados.

4.5. PRAZOS DE REVISÕES

Esta política deve ser analisada anualmente e revisada caso haja necessidade.

Os acessos aos recursos tecnológicos da empresa deverão ser analisados a cada seis meses.

4.6. AUDITORIA DE SEGURANÇA DA INFORMAÇÃO

A empresa possui softwares e sistemas implantados que podem monitorar o uso da Internet, e-mails, chats, etc., através da rede local e das estações de trabalho da empresa.

A empresa se reserva o direito de inspecionar, sem a necessidade de aviso prévio, as estações de trabalho e qualquer arquivo armazenado, estejam no disco local da estação ou nas áreas privadas da rede, assim como monitorar o volume de tráfego na Internet e na Rede juntamente com os endereços web (<http://>) visitados, visando assegurar o cumprimento desta política.

5. REGRAS DE CONSEQUÊNCIA

As consequências em caso de descumprimento destas diretrizes serão tratadas em conformidade com o Código de Conduta e Relacionamento da Unimed Assis, tópico de penalidades e ações disciplinares. Situações excepcionais serão encaminhadas para o Comitê Executivo, Diretoria Colegiada e/ou demais órgãos de governança.

6. DISPOSIÇÕES FINAIS

Esta política passou a vigorar a partir da data de sua aprovação pela Diretoria Executiva em 16 de setembro de 2020, revisada em 03 de fevereiro de 2021 e aprovada pelo Conselho de Administração no dia 13 de fevereiro de 2023.