Sumário

1. OBJETIVO

O objetivo desta política é fornecer diretrizes destinadas a proteger as informações da Cooperativa, reduzir o risco comercial e jurídico e salvaguardar os investimentos e a reputação da Cooperativa. Ademais, busca-se nortear a definição de normas e procedimentos específicos de segurança da informação, bem como a implementação de controles e processos para seu atendimento, com o fim de preservar as informações da Unimed Santos quanto à:

- Integridade: garantia de que a informação seja mantida em seu estado original, visando protegê-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais.
- Confidencialidade: garantia de que o acesso à informação seja obtido somente por pessoas autorizadas.
- Disponibilidade: garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

2. ÂMBITO DE APLICAÇÃO

Esta política e seus controles, processos e procedimentos de suporte se aplicam:

- A todas as unidades, áreas, setores e departamentos da Unimed Santos.
- A todos os analistas de segurança da informação e administradores de sistemas responsáveis pela manutenção de sistemas, softwares, aplicativos, programas, dispositivos e equipamentos de TI gerenciados pela Cooperativa.
- A todos os dirigentes, colaboradores em tempo integral, colaboradores em meio período, colaboradores em tempo parcial, trabalhadores contratados, consultores, estagiários, aprendizes, trabalhadores temporários, prestadores de serviços, agentes, parceiros, fornecedores e usuários autorizados que acessam as dependências da Cooperativa.
- A todos os sistemas, aplicativos, dispositivos e equipamentos de TI gerenciados pela Cooperativa que armazenam, processam ou transmitem dados e informações, incluindo redes de computadores, hardwares, softwares e aplicativos, dispositivos móveis e sistemas de telecomunicações.
- A todas as informações utilizadas na Cooperativa, em todos os formatos. Isso inclui informações processadas por outras organizações em suas relações comerciais com a Unimed Santos.
- A todos na Unimed Santos e partes interessadas.

3. DEFINIÇÕES

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

Colaborador: Empregados, estagiários, *office boys/girls*, 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.

ABNT NBR ISO/IEC 27701: Norma Brasileira de Técnicas de segurança.

ABNT NBR ISO/IEC 27002: Norma Brasileira de Gestão de Segurança da Informação.

Hardware: É a parte física do computador, ou seja, peças e equipamentos utilizados para que o computador funcione.

Malware: Termo genérico usado para se referir a programas desenvolvidos para executar ações danosas e atividades maliciosas em um computador ou dispositivo móvel. Tipos específicos de códigos maliciosos são: vírus, worm, bot, spyware, backdoor, cavalo de troia e rootkit.

PGSI: Política Geral de Segurança da Informação.

Software: Todo programa rodado em um computador, celular ou dispositivo que permita ao mesmo executar suas funções.

TI: Tecnologia da Informação.

Walk-through: Processo de verificação.

4. DIRETRIZES

4.1 Das Diretrizes Gerais

Esta Política visa garantir uma gestão sistêmica e efetiva da Governança da Tecnologia da Informação e em todos os aspectos relacionados à Segurança da informação, provendo suporte as operações críticas do negócio e minimizando riscos identificados e seus eventuais impactos a instituição através de uma Gestão de Segurança da Informação.

A Segurança da Informação será tema tratado pelo Comitê de Proteção de Dados que contará com a participação de pelo menos um representante da diretoria executiva e um membro das seguintes áreas: Tecnologia da Informação, Jurídico, Recursos Humanos, Governança, Riscos e Compliance (GRC).

Serão adotadas medidas cabíveis para garantir que esta política seja adequadamente comunicada, entendida e seguida por todos os níveis da organização. Para isto serão executadas revisões periódicas para garantir a contínua pertinência e adequação as necessidades da Unimed Santos. Toda informação produzida ou recebida pelos colaboradores como resultado da atividade profissional contratada pela Unimed Santos pertence à referida instituição.

Os tipos de informações geradas, coletadas e utilizadas para alimentar os processos internos e externos de toda a organização e os métodos de obtenção, análise e tratativa dessas informações serão minimamente abordadas em documento da descrição de cada processo.

O uso dos equipamentos computacionais da Unimed Santos deverá estar direcionado apenas para fins de pesquisa, consultas, prestações de serviços e o desenvolvimento dos trabalhos voltados às atividades da Cooperativa. Todos os

equipamentos utilizados devem ser homologados pelo Departamento de TI da Unimed Santos e somente estes equipamentos estão autorizados a ter acesso à Rede.

Todos os colaboradores da Unimed Santos 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 Santos deve ser feita de forma responsável, ética e seguir as premissas de segurança da informação.

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.

4.2 Normas, controles, processos e procedimentos complementares e auxiliares

Um conjunto complementar e auxiliar de políticas, controles, processos e procedimentos de nível inferior para a segurança da informação foi definido, em apoio a esta Política Geral de Segurança da Informação e seus objetivos declarados. Este conjunto de documentação de apoio deverá ser aprovado, publicado e comunicado aos colaboradores da Cooperativa e partes externas relevantes.

4.3 Organização da Segurança da Informação

A Alta Direção define que a área de Tecnologia da Informação – TI é responsável pelo Sistema de Segurança da Informação à Governança – SGSI e Governança da Tecnologia da Informação. Isso incluirá a identificação e alocação de responsabilidades de segurança, para iniciar e controlar a implementação e operação da segurança da informação dentro da Cooperativa.

O Comitê Proteção de Dados deverá ser instituído com intuito de dar suporte e apoio as atividades do Sistema de Gestão e Segurança da informação, ajudando no cumprimento e apoio as atividades referentes ao cumprimento da Lei Geral de Proteção de Dados – LGPD.

4.4 Segurança de Recursos Humanos

A política de segurança da Cooperativa, seu conjunto complementar e auxiliar de normas, controles, processos e procedimentos de nível inferior e as expectativas de uso aceitável deverão ser comunicadas a todos os usuários para garantir que eles entendam suas responsabilidades. A educação e o treinamento em segurança da informação deverão ser disponibilizados a todos os colaboradores, e o comportamento inadequado será abordado.

A depender do caso, as responsabilidades de segurança deverão ser incluídas nas descrições de funções,

especificações pessoais e planos de desenvolvimento pessoal. A responsabilidade em relação à segurança da informação deve ser comunicada na fase de contratação dos colaboradores, mediante assinatura de termo de responsabilidade. Todos os colaboradores devem ser orientados sobre os procedimentos de segurança, bem como o uso correto dos ativos, a fim de reduzir possíveis riscos.

4.5 Utilização da informação

A Unimed Santos 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 Santos.

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, não devendo ser compartilhadas com terceiros por nenhum meio.

O sigilo das informações é responsabilidade de todos os colaboradores da Unimed Santos. 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.

As informações assistenciais, quando necessárias à atividade profissional, devem ser discutidas apenas pessoalmente ou por e-mail 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. Assim, evitaremos que os dados sejam compartilhados indevidamente.

Todos os colaboradores que tenham acesso a informações da Unimed Santos ou sob a guarda da Unimed Santos privilegiadas, pessoais ou sensíveis ou não – 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.

As informações devem ser classificadas como **Confidencial, Restrita, Interna e Pública**, seguindo os critérios estabelecidos abaixo, 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.

Classificação	Critério	Publico alvo	Exemplo(s)
CONFIDENCIAL	Informações de carater estratégico. A informação confidencial é restringida dentro da	Pessoas elegíveis pela	Reunião de Conselhos de Administração, Técnico e

	Unimed Santos e protegida de acesso externo. Qualquer perda de confidencialidade causará eventual comprometimento das operações, resultando em perdas financeiras, de competitividade, de imagem, risco de ações judiciais para a Unimed Santos e a seus administradores.	Diretoria Executiva	Fiscal. Reunião da Diretoria Executiva.
RESTRITA	Informações de carater restrito e circulação controlada envolvendo dados pessoais e sensíveis. Este tipo de informação é de uso restrito a um grupo de pessoas, departamentos específicos, equipes de um projeto, etc., divulgada de forma seletiva e mediante o conhecimento e autorização expressa do responsável pela informação. (informações de projetos e processos)	Somente pessoas elegíveis para tomar conhecimento e uso dos administradores.	Fórmulas e ativos protegidos por direitos autorais, Assuntos de comitês e Grupos de Trabalho, Notas Fiscais, informações pessoais, dados de saúde.
INTERNA	Informações de conhecimento e circulação interna. A informação de uso interno é tratada como importante e mantida dentro do domínio da Unimed Santos, divulgada de forma seletiva e mediante o conhecimento e a autorização do responsável pela informação. (informações publicadas na intranet).	Integrantes para o uso destas informações	Comunicações internas; procedimentos internos.
PÚBLICA	Informações de circulação geral, de conhecimento público. Toda informação que não necessite sigilo terá livre acesso e não causará qualquer prejuízo para a Unimed Santos (informações publicadas em plataformas oficiais Unimed Santos	Público geral	Noticias; campanhas sociais, campanhas de vendas, etc.

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

4.6 Ambiente Físico

4.6.1. Acesso e permanência de empregados e visitantes

Na Unimed Santos 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. Este controle de acesso é de responsabilidade da Segurança Patrimonial de cada sede.

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.

4.6.2 Gestão de ativos

Todos os ativos (informações, softwares, equipamentos de processamento eletrônico de informações, etc.) deverão ser documentados e registrados. Os proprietários deverão ser identificados para todos os ativos e deverão ser responsáveis pela manutenção e proteção de seus ativos. Todos os ativos de informação deverão ser classificados de acordo com seus requisitos legais, valor do negócio, criticidade e sensibilidade, e a classificação indicará os requisitos de manuseio apropriados. Todos os ativos de informação terão normas apropriadas para o seu descarte adequado e seguro.

4.6.3 Controle de acesso

Os acessos a todas as informações deverão ser controlados e orientados pelos requisitos de negócios. O acesso deverá ser concedido ou providenciado para os usuários de acordo com sua função e a classificação da informação, apenas até um nível que lhes permita cumprir suas funções.

Um procedimento formal de registro e cancelamento de registro deverá ser mantido para o acesso a todos os sistemas e serviços de informação. Isso incluirá métodos de autenticação obrigatórios com base na confidencialidade das informações acessadas e incluirá a consideração de vários fatores, conforme apropriado.

Controles específicos deverão ser implementados para usuários com privilégios elevados de acesso, para reduzir o risco de uso negligente ou deliberado do sistema. A segregação de funções deverá ser implementada, sempre que possível. Para concessão de acesso aos ativos de informação disponibilizados pela Unimed Santos, faz-se necessário, formalização do Termo de Confidencialidade e Uso de Rede Corporativa.

4.6.4 Segurança Física e Ambiental

As instalações de processamento de informações deverão estar alojadas em áreas seguras, fisicamente protegidas contra acesso não autorizado, danos e interferência por perímetros de segurança definidos. Além da proteção contra acesso não autorizado, as informações devem ser protegidas contra desastres tais como incêndios, terremotos, inundações ou explosões.

Controles de segurança internos e externos deverão ser implementados para impedir o acesso não autorizado e proteger os ativos, especialmente aqueles que são críticos ou sensíveis, contra ataques cibernéticos. A Unimed Santos 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 Santos. 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 Santos. Também não é permitida a divulgação de informações inverídicas de qualquer natureza em qualquer meio de comunicação.

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.

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.

A informação exposta de forma inadequada ou sem o zelo requerido pode ser o suficiente para pessoas mal intencionadas descobrirem aspectos corporativos ou pessoais, fazendo uso indevido de tais informações. 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.

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

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 Santos 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.

4.7.1 Segurança de operações

O Sistema de Gestão da Segurança da Informação deverá garantir o funcionamento correto e seguro dos sistemas de processamento de informações. Isso inclui:

- Procedimentos operacionais documentados;
- O uso de mudança formal e gerenciamento de capacidade;
- Controles contra *malwares;*
- Controles de acesso;
- Gerenciamento de vulnerabilidade.

I - Contas e senhas de acesso a sistemas

Na Unimed Santos 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.

II - 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.

III - 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.

IV - Internet

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

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

V - Ativos de Processamento de Dados (hardware e software)

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 Santos homologa e controla os ativos de processamentos de dados, incluindo equipamentos e sistemas de informação.

4.7.2 Segurança das comunicações

A Cooperativa deverá manter controles de segurança de rede para garantir a proteção da informação dentro de suas redes, e deverá fornecer as ferramentas e orientações para garantir a transferência segura de informação tanto dentro de suas redes quanto com entidades externas, de acordo com os requisitos de classificação e tratamento associados.

4.7.3 Aquisição, desenvolvimento e manutenção do sistema

Os requisitos de segurança da informação serão definidos durante o desenvolvimento dos requisitos de negócios para novos sistemas de informação ou mudanças nos sistemas de informação existentes. Controles para mitigar quaisquer riscos identificados serão implementados quando apropriado.

Os ambientes de produção devem ser segregados e rigidamente controlados, garantindo o isolamento necessário em relação aos ambientes de desenvolvimento, testes e homologação. Toda a aquisição de softwares e/ou componentes de TI deve ser solicitado ao Sistema de Gestão da Segurança da Informação, via ticket, para que possa ser avaliado e mapeado pela TI, antes de sua aquisição. O departamento de TI deverá manter atualizado o Mapa de dados da cooperativa.

4.7.4 Relações com fornecedores

Os requisitos de segurança da informação da Cooperativa deverão ser considerados no estabelecimento de relações com fornecedores, para garantir que os ativos acessíveis aos fornecedores sejam protegidos. A atividade do fornecedor será monitorada e auditada de acordo com o valor dos ativos e os riscos associados.

4.8 Governança da Tecnologia da Informação

Cabe a área de Tecnologia da Informação implementar e manter um Sistema de Gestão de Segurança da Informação, provendo a Governança e Segurança das informações, baseado na ABNT NBR ISO/IEC 27014:2013.

4.8.1 Aspectos de Segurança da Informação da Gestão de Continuidade de Negócios

A Governança de TI deverá estabelecer mecanismos para proteger processos de negócios críticos dos efeitos de

grandes falhas de sistemas de informação ou desastres e para garantir sua recuperação oportuna de acordo com as necessidades de negócios documentadas, através da implementação do Sistema de Gestão de Segurança da Informação. Isso incluirá rotinas de backup adequadas e resiliência integrada.

Os planos de contingência e a continuidade dos principais sistemas e serviços deverão ser implantados e testados, no mínimo, anualmente, visando reduzir riscos de perda de confidencialidade, integridade e disponibilidade dos ativos de informação. Todos os requisitos de segurança da informação, incluindo a necessidade de planos de contingência, devem ser identificados na fase de levantamento de escopo de um projeto ou sistema, e justificados, acordados, documentados, implantados e testados durante a fase de execução.

4.8.2 Gerenciamento de Incidentes de Segurança da Informação

Cabe a Governança de TI estabelecer a Gestão de incidentes internos e externos. Onde a orientação deverá abordar o que constitui um incidente de segurança da informação e como isso deve ser relatado. Violações reais ou suspeitas de segurança da informação deverão ser relatadas e serão investigadas.

Em caso de incidente que afete a segurança da informação, o mesmo deverá ser registrado em uma das seguintes formas:

- Incidente detectado internamente: deverá ser registrado o ticket através do sistema de atendimento (SAUS), gerado protocolo específico e direcionado para o SGSI – Sistema de Gestão da Segurança da Informação, onde o mesmo será analisado previamente e/ou dará a tratativa, e sendo necessário, será encaminhado posteriormente ao Comitê Proteção de Dados para análise.
- Incidente detectado externamente: Através de um dos canais de comunicação da Cooperativa (como o Canal do titular, por exemplo), onde o mesmo será analisado previamente e/ou dará a tratativa, e sendo necessário, será encaminhado posteriormente ao Comitê Proteção de Dados para análise.
- Outras partes interessadas deverá ser enviado um email para sgsi@unimedsantos.coop.br .

4.8.3 Conformidade

O Sistema de gestão da Segurança da Informação através de seu projeto, operação, uso e gerenciamento de sistemas de informação deverão cumprir todos os requisitos de segurança estatutários, regulamentares e contratuais. Atualmente, isso inclui a legislação de proteção de dados e as normas e padrões nacionais e internacionais voltados à segurança da informação.

O Sistema de Gestão da Segurança da Informação usará uma combinação de auditoria interna e externa para demonstrar conformidade com os padrões e melhores práticas escolhidos, incluindo políticas e procedimentos internos. Isso incluirá verificações da “saúde” da TI, análises de lacunas em relação a padrões documentados, verificações internas de conformidade da equipe e feedbacks dos responsáveis pelos ativos de informação.

4.8.4 Verificação da Conformidade

A Governança de TI, o departamento de Gestão de Pessoas e os coordenadores de cada departamento, área, setor ou

unidade da Cooperativa verificarão a conformidade com esta política por meio de vários métodos, incluindo, mas não se limitando a, *walk-through* periódicos, logs de auditoria de sistemas e banco de dados, auditorias de TI e feedbacks para o responsável pela política

5. COMUNICAÇÃO E REPORTE

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. Devem ser realizadas em conjunto com as áreas de TI e Gestão de risco.

A Governança de TI deverá no mínimo anualmente apresentar os resultados desta avaliação e monitoramento à Diretoria Executiva e ao Conselho de Administração.

6. PAPÉIS E RESPONSABILIDADES

É responsabilidade da área de Governança de TI da Unimed Santos:

- Elaborar, implantar e seguir por completo Sistema de Gestão da Segurança da Informação, através de cumprimento de política, normas e procedimentos de segurança da informação, garantindo confidencialidade, integridade e disponibilidade da informação da Unimed Santos através da adoção de controles contra ameaças provenientes de fontes tanto externas quanto internas.
- Disponibilizar para todos os colaboradores, terceiros e fornecedores os procedimentos e normas de Segurança da Informação.
- Garantir a conscientização e educação de todos os colaboradores, terceiros e fornecedores das práticas adotadas pela Unimed Santos referente a Segurança da Informação.
- Atender a todos os requisitos de Segurança da Informação aplicáveis ou exigidos por regulamentações, Leis ou Cláusulas Contratuais.
- Tratar todos os incidentes de Segurança da Informação registrando, classificando, investigando, corrigindo, documentando e quando necessário comunicando as autoridades apropriadas.
- Garantir através de adoção de implantação, testes e melhoria contínua a continuidade do negócio.
- Trazer sempre melhorias à Gestão de Segurança da Informação através da definição e revisão sistemática de objetivos de segurança em todos os níveis da organização.

É responsabilidade de cada líder de departamento, área, setor ou unidade da Cooperativa garantir a aplicação desta política.

7. GESTÃO DE CONSEQUÊNCIA

As consequências em caso de descumprimento destas diretrizes serão tratadas em conformidade com o Código de Conduta da Unimed Santos e suas Políticas vigentes. Situações excepcionais serão encaminhadas para Diretoria Executiva e/ou demais órgãos de governança.

8. REFERÊNCIAS

- ANS. RESOLUÇÃO NORMATIVA - RN Nº 452, DE 09 DE MARÇO DE 2020. Brasil. Disponível em: https://www.ans.gov.br/component/legislacao/?view=legislacao&task=TextoLei&format=raw&id=Mzg2NA==
- ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR ISO/IEC 27001 – tecnologia da informação – técnicas de segurança – sistema de gestão de segurança da informação - requisitos.
- ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR ISO /IEC 31001 – gestão de riscos – técnicas para o processo de avaliação de riscos.
- ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR ISO /IEC 27002 – tecnologia da informação – técnicas de segurança – código de prática para a gestão da segurança da informação.
- ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR ISO /IEC 27005 – tecnologia da informação – técnicas de segurança – gestão de riscos de segurança da informação.
- ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR 15999-1:2007 - gestão da continuidade de negócios – parte 1: código de prática.
- COBIT 5: A Business Framework for the Governance and Management of Enterprise IT. USA, 2012. USA, 2012BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm Acessado em: 10/12/2018.
- BRASIL. Constituição da República Federativa do Brasil de 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm Acessado em: 10/12/2018
- BRASIL. Código Civil Brasileiro - Lei 10.406 de 10 de janeiro de 2002 em vigor desde 11 de janeiro de 2003, sendo a última atualização pela lei nº 12.607, de 4 de abril de 2012. Disponível em: http://presrepublica.jusbrasil.com.br/legislacao/91577/codigo-civil-lei-10406-02 Acessado em: 10/12/2018
- BRASIL. Conselho Federal de Medicina - instituído pelo decreto-lei nº 7.955, de 13 de setembro de 1945 e adquiriu suas características atuais a partir da lei nº 3.268, de 30 de setembro de 1957.
- BRASIL. Lei 13.709 de 14 de agosto de 2018. Lei Geral de Proteção de Dados. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm Acessado em 10/12/2018.
- ORGANIZAÇÃO NACIONAL DE ACREDITAÇÃO. SEÇÃO 1. SUBSEÇÃO 1.1 REQ. 10**:** Manual para organizações prestadores de serviços de saúde. São Paulo: 2022-2026.
- UNIMED SANTOS. Código de Conduta disponível na intranet .

9. DOCUMENTAÇÃO COMPLEMENTAR

- Código de Conduta
- Política Governança de TI
- Política Geral de Proteção de Dados Pessoais
- Política de Gestão de Riscos

10. DISPOSIÇÕES GERAIS

Qualquer mudança nesta política deve ser aprovada pela área de Governança de TI.

Tanto a Política Geral de Segurança da Informação quanto as demais normas deverão ser revistas e atualizadas periodicamente, sempre que algum fato relevante ou evento motive sua revisão antecipada, conforme análise e decisão do Comitê responsável.

Esta Política entra em vigor na data de sua aprovação pela Diretoria Executiva e revoga quaisquer normas e procedimentos em contrário. Caso haja dúvidas sobre esta política e sua aplicação, entre em contato pelo e-mail sgsi@unimedsantos.coop.br.

Identificação das Alterações		
Revisão	Data da revisão	Alterações efetuadas
00	11/01/2022	Elaborado pela TI.

Áreas envolvidas	Validação	Data
Diretoria Executiva	Política aprovada em reunião do Conselho de Administração	18/01/2022
Dr. Claudino Guerra Zenaide Diretor Presidente cguerra@unimedsantos.coop.br	DocuSigned by: Claudino Guerra Zenaide C01E365683D6461...	25/1/2022 | 09:47:53 PST
Dr. Luiz Arnaldo Vanzato Diretor de Controladoria lvanzato@unimedsantos.coop.br	DocuSigned by: Dr. Luiz Arnaldo Vanzato 10FDE1B0E8C8433...	25/1/2022 | 10:17:09 PST
Dr. José Roberto Del Sant Diretor de Provimento e Saúde jrdelsant@unimedsantos.coop.br	DocuSigned by: Dr. José Roberto Del Sant 52D397EE48E445F...	27/1/2022 | 05:33:23 PST
Dr. Ivan Akaoui Vianna Diretor de Mercado iavianna@unimedsantos.coop.br	DocuSigned by: Dr. Ivan Akaoui Vianna 2CC47619A51044D...	28/1/2022 | 04:33:08 PST
Dr. José Bento Toledo Piza Diretor de Relacionamento e Atendimento ao Cooperado jbentopiza@unimedsantos.coop.br	DocuSigned by: José Bento Toledo Piza F6B4E2272CA3456...	25/1/2022 | 11:17:02 PST