Política de segurança da informação

Unimed
Oeste do Paraná

Este documento é público

Unimed Oeste do Paraná
2023 – 2027

Estrutura de Governança

Dr. Marco Aurélio Farinazzo
Presidente e Diretor de Saúde

Dr. Rodrigo Otavio Gama França
Diretor de Mercado e Estratégia

Dr. Henrique Bertassoni Alves
Diretor Administrativo e Financeiro

Conselhos

Conselho de Administração

Dr. Marcelo Yuji Cinagava
Dr. Jose Augusto de Oliveira Monteiro
Dr. Maurício Diegoli Moritz
Dra. Andrea Leda Klos
Dr. Emilio Driessen Junior
Dra. Adriana Zanella Borba

Conselho Técnico

Dr. Wil Oliveira da Costa
Dr. Flavio Carmelo Sampaio Saraiva
Dr. Luiz Gustavo Deconto Neves
Dr. Paulo Tranmontin Marques
Dr. João Augusto Hidalgo Barros Abomorad
Dr. Antonio Ricardo Andrade Souza

Conselho Fiscal 2026/2027

Dr. Alex Junior Schafer
Dr. Anderson Antônio Pavan
Dr. Sidinei Elzinga Rimoldi
Dra. Nadia Lorena Mendoza
Dra. Layara Lenardon Mehanna
Dra. Thaisa Aires Marques

ESSÊNCIA UNIMED

Crenças

A vida é o bem maior do ser humano.

A vida boa deve ser possível para todos.

Saúde é condição essencial para uma vida boa.

A vida só acontece na cooperação, na natureza e em sociedade.

Propósito

Promover saúde e qualidade de vida em nossas cidades por meio do cooperativismo médico e do conhecimento em saúde para que o maior número de pessoas possa viver mais e melhor.

Princípios

- Atratividade para médicos
- Pessoas
- Sustentabilidade
- Conhecimento
- Visão sistêmica
- Inovação
- Agilidade
- Princípios Cooperativistas

Valores

- Integridade
- Respeito
- Solidariedade
- Espírito Cooperativista

Negócio

Cooperativa médica, saúde e sustentabilidade.

Política da Qualidade:

A Política da Qualidade da Unimed Oeste do Paraná tem como princípio assegurar uma experiência positiva e segura para cada cliente, promovendo a melhoria contínua dos serviços e fortalecendo os processos assistenciais e administrativos, sempre alinhados à cultura cooperativista. Seu propósito é garantir elevados padrões na oferta e gestão de planos de saúde e recursos próprios, estimulando a evolução contínua dos processos, a satisfação dos clientes e a sustentabilidade da organização. A Unimed compromete-se a oferecer serviços de saúde com excelência, alinhados às expectativas dos clientes, às normas do setor e à busca permanente por inovação e melhoria contínua.

SUMÁRIO

APRESENTAÇÃO ____ 6

OBJETIVO ____ 6

A QUEM SE APLICA ____ 7

DEFINIÇÕES E SIGLAS ____ 7

PAPÉIS E RESPONSABILIDADES ____ 9

COMITÊ EM PROTEÇÃO E PRIVACIDADE DE DADOS ... 10

ÁREA DE PROTEÇÃO E PRIVACIDADE DE DADOS (PPD / DPO) ... 10

DIRETORIA EXECUTIVA ... 12

GESTÃO DE NEGÓCIOS – GERÊNCIA COMERCIAL ... 13

DEPARTAMENTO PESSOAL ... 13

GESTÃO DE RECURSOS FINANCEIROS ... 14

GESTÃO DE TECNOLOGIA DA INFORMAÇÃO ... 14

USUÁRIOS INTERNOS E EXTERNOS ... 15

PROPRIETÁRIO DA INFORMAÇÃO ... 15

PRINCÍPIOS E DIRETRIZES ____ 16

ESTRUTURA NORMATIVA DA SEGURANÇA DA INFORMAÇÃO ... 16

DECLARAÇÃO DE COMPROMETIMENTO DA DIREÇÃO ... 17

PRINCÍPIOS DE SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE ... 17

DIRETRIZES GERAIS DE SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE ... 18

DIRETRIZES PARA GESTÃO DE ATIVOS ... 19

DIRETRIZES PARA CLASSIFICAÇÃO DA INFORMAÇÃO ... 19

DIRETRIZES PARA CONTROLE DE ACESSO ... 20

DIRETRIZES PARA SEGURANÇA EM PESSOAS ... 22

SEGURANÇA OPERACIONAL ... 24

CRIPTOGRAFIA 27
SEGURANÇA FÍSICA E DO AMBIENTE 28
COMUNICAÇÕES E REDES 28
SISTEMAS E DESENVOLVIMENTO 29
TERCEIROS 30
GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE 31
CONTINUIDADE DE NEGÓCIOS 32
MONITORAMENTO, AUDITORIA E MELHORIA CONTÍNUA 32
GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE 34
DIRETRIZES PARA USO ACEITÁVEL E COMPORTAMENTO DO USUÁRIO 37

PENALIDADES / PROCESSO DISCIPLINAR ____ 38

VIOLAÇÕES 38
NÃO CONFORMIDADE E AÇÃO CORRETIVA 39
SANÇÕES 39

ATUALIZAÇÃO E REVISÃO DA POLÍTICA ____ 40

DISPOSIÇÕES FINAIS ____ 40

REFERÊNCIAS LEGAIS E NORMATIVAS ____ 41

APRESENTAÇÃO

A informação é um dos ativos mais relevantes para a sustentabilidade e a continuidade dos negócios da Unimed do Oeste do Paraná, especialmente considerando a natureza sensível dos dados tratados, incluindo informações de saúde e dados pessoais de beneficiários, colaboradores e parceiros.

Neste contexto, a segurança da informação e a proteção da privacidade assumem papel estratégico, sendo fundamentais para a manutenção da confiança, da conformidade regulatória e da integridade das operações da cooperativa.

A crescente digitalização dos processos e a ampliação do uso de tecnologias da informação aumentam significativamente a exposição a riscos cibernéticos, operacionais e legais, exigindo a adoção de medidas técnicas, administrativas e organizacionais capazes de prevenir, detectar, responder e mitigar incidentes de segurança da informação e de privacidade.

A Unimed do Oeste do Paraná estabelece, por meio desta Política, as diretrizes institucionais para proteção dos ativos de informação, assegurando os princípios de confidencialidade, integridade, disponibilidade, autenticidade e, adicionalmente, os princípios de proteção de dados pessoais previstos na legislação vigente.

Esta Política está alinhada às melhores práticas internacionais, incluindo as normas da família ABNT NBR ISO/IEC 27000 e a ABNT NBR ISO/IEC 27701, bem como à Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018), refletindo o compromisso da cooperativa com a governança, a segurança e a privacidade da informação.

A adoção e a manutenção de um Sistema de Gestão de Segurança da Informação (SGSI) integrado a um Sistema de Gestão de Privacidade da Informação (SGPI) representam uma decisão estratégica da organização, visando à melhoria contínua dos controles de segurança, à mitigação de riscos e à proteção dos direitos dos titulares de dados.

OBJETIVO

O objetivo desta Política de Segurança da Informação é estabelecer as diretrizes institucionais para a proteção dos ativos de informação da **Unimed Oeste do Paraná**, assegurando a confidencialidade, integridade, disponibilidade, autenticidade e a proteção da privacidade dos dados pessoais tratados pela organização.

Esta Política define os princípios e orientações para a implementação, manutenção e melhoria contínua do Sistema de Gestão de Segurança da Informação (SGSI) e do Sistema de Gestão de Privacidade da Informação (SGPI), em conformidade com as normas da família ABNT NBR ISO/IEC 27000, ABNT NBR ISO/IEC 27701 e com a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018 – LGPD).

Adicionalmente, esta Política estabelece as bases para a adoção de controles, normas, procedimentos e mecanismos de governança necessários à prevenção, detecção, resposta e mitigação de incidentes de segurança da informação e de privacidade, bem como à gestão de riscos relacionados ao tratamento de informações.

A QUEM SE APLICA

Esta Política de Segurança da Informação aplica-se a todos os públicos que, de alguma forma, tenham acesso, tratem ou sejam responsáveis por ativos de informação da **Unimed Oeste do Paraná**, independentemente do meio ou local de acesso.

Estão incluídos no escopo desta Política:

I. **Público interno:**
   - » Diretoria e Conselhos;
   - » Gestores e lideranças;
   - » Colaboradores, estagiários e aprendizes;
   - » Áreas operacionais, administrativas e assistenciais.

II. **Público externo:**
   - » Prestadores de serviços, fornecedores e parceiros de negócio;
   - » Terceiros que realizem tratamento de dados em nome da organização, incluindo operadores de dados pessoais;
   - » Médicos cooperados;
   - » Clientes, beneficiários e demais titulares de dados, quando aplicável ao uso de recursos ou sistemas disponibilizados pela organização;
   - » Visitantes com acesso às dependências físicas ou recursos da organização.

Esta Política aplica-se a todos os ambientes e ativos de informação, incluindo, mas não se limitando a:

- Sistemas internos e externos;
- Infraestrutura tecnológica on-premise e em nuvem;
- Dispositivos corporativos e pessoais autorizados;
- Ambientes de trabalho remoto;
- Plataformas digitais, portais, APIs e serviços integrados.

DEFINIÇÕES E SIGLAS

Acordo de Confidencialidade – Cláusula ou instrumento contratual que contém responsabilidades, direitos e deveres dos empregados, prestadores e prospectores de serviços, tais como de leis de direito autorais ou de proteção de dados, bem como a extensão da responsabilidade para fora das dependências da organização e após a rescisão do vínculo contratual.

Análise de Risco – Processo que envolve a consideração detalhada das incertezas, dos eventos, das causas e das consequências, a fim de se determinar as probabilidades dos riscos e os impactos decorrentes se tornarem reais.

Ativo – Podemos definir o que é um ativo em segurança da informação como um recurso corporativo que possui valor para a companhia e que deve ser protegido a partir de práticas e políticas que garantam a sua integridade, confidencialidade, disponibilidade e autenticidade

Ativo Tecnológico – Equipamentos ou programas de computador que suportam o ambiente organizacional e de negócios da empresa.

Colaborador – Empregado ou pessoa que presta serviços à empresa, sejam através de Contrato Individual de Trabalho, ou por vínculo a um Contrato de Prestação de Serviço.

Responsável ou proprietário – Colaborador designado como dono/proprietário do ativo de segurança da informação.

Disponibilidade – Diz respeito à garantia de que a informação estará acessível às pessoas, processos automatizados, órgãos ou entidades no momento que for requerida. Logo a disponibilidade está relacionada à prestação continuada de um serviço, sem interrupções no fornecimento de informações.

Integridade – A integridade da informação está relacionada à sua fidedignidade. Assegurar a integridade da informação, portanto, significa garantir que a informação não foi modificada ou destruída de maneira não autorizada, quer de forma acidental ou intencional.

Confidencialidade – Implica em impedir o acesso não autorizado, quer acidental quer intencional, garantindo que apenas pessoas, sistemas, órgãos ou entidades devidamente autorizados e credenciados tenham acesso à informação.

Autenticidade – Mediante a autenticação é possível confirmar a identidade de quem presta a informação, garantindo que o emissor da informação seja de fato quem alega ser. Através da autenticação asseguramos a fidedignidade da fonte da informação.

Perímetro – Área física ou lógica da empresa onde são aplicadas proteções contra acessos indevidos.

Risco – É o efeito da incerteza nos objetivos.

Computação em nuvem (Cloud Computing) – Modelo de negócio que disponibiliza (compartilha) recursos computacionais e serviços sob demanda, os recursos são configuráveis pelo próprio cliente, de acordo com a sua necessidade, e cobrados apenas pelo que foi consumido. A computação na nuvem oferece escalabilidade e mecanismos de gestão dos serviços.

NDA – Acordo de não divulgação.

Conformidade – Aderência a um padrão previamente estabelecido e aceito como ideal.

Backup – Cópia de segurança gerada para possibilitar o acesso ou recuperação futura de dados existentes no Data Center. O termo também pode ser associado ao processo de geração da cópia de segurança, acepção que tem no restore seu complemento (vide restore).

Restore – É a ação de recuperar os dados armazenados em determinado dispositivo durante a rotina de backup, garantindo que todas as informações gravadas estejam intactas.

Dispositivos móveis – Qualquer equipamento ou acessório portátil, capaz de se conectar à internet e/ou armazenar dados, tais como: celular, smartphone, tablet, notebook, netbook, mp4, pendrive, CD/DVD, fita LTO e outros semelhantes.

Sistema de Gestão da Segurança da Informação (SGSI) – É um sistema de gestão corporativo voltado para a Segurança da Informação, que inclui toda a abordagem organizacional usada para proteger a informação empresarial e garantir os critérios de Confidencialidade, Integridade e Disponibilidade. O SGSI inclui estratégias, planos, políticas, medidas, controles, e diversos instrumentos usados para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar a segurança da informação.

Sistema de Gestão privacidade da informação (SGPI) – É uma metodologia voltada a estruturar um processo responsável pelo gerenciamento e por mitigar os riscos de proteção de dados e privacidade envolvidos em todo o Ciclo de Vida de Dados Pessoais tratados pela Unimed do Oeste do Paraná, considerando-se desde a coleta o processamento e a eliminação de dados pessoais.

NIST: O Instituto Nacional de Padrões e Tecnologia – foi fundado em 1901 e agora faz parte do Departamento de Comércio dos EUA. O NIST é um dos laboratórios de ciências físicas mais antigos do país. O Congresso criou a agência para eliminar um grande desafio à competitividade industrial dos EUA na altura – uma infraestrutura de medição de segunda categoria que estava aquém das capacidades do Reino Unido, da Alemanha e de outros rivais económicos.

CIS – O CIS Controls (ou Controles CIS) é uma publicação que apresenta boas práticas e recomendações para a área de Segurança da Informação. A iniciativa teve início nos anos 2000 com líderes empresariais e governamentais americanos e hoje é de responsabilidade da organização não governamental Center for Internet Security (CIS).

Logs – Em computação, log de dado é uma expressão utilizada para descrever o processo de registro de eventos relevantes em um sistema computacional. Esse registro pode ser utilizado para restabelecer o estado original de um sistema ou para que um administrador conheça o seu comportamento no passado. Um arquivo de log pode ser utilizado para auditoria e diagnóstico de problemas em sistemas computacionais.

Arquivo de log – Registro detalhado de todas as transações efetuadas durante a utilização de um aplicativo e necessário ao rastreamento do seu uso.

PAPÉIS E RESPONSABILIDADES

A segurança da informação e a privacidade dos dados são responsabilidades compartilhadas, sendo sustentadas por uma estrutura organizacional definida, na qual cada área possui atribuições específicas conforme seu papel na cooperativa.

COMITÊ EM PROTEÇÃO E PRIVACIDADE DE DADOS

O Comitê é composto por um grupo de colaboradores formalmente designados e aprovados pela Diretoria Executiva, com o objetivo de apoiar a governança, a implementação e a melhoria contínua do Sistema de Gestão de Segurança da Informação (SGSI) e do Sistema de Gestão de Privacidade da Informação (SGPI).

O comitê atua como instância consultiva e estratégica, contribuindo para o cumprimento dos requisitos legais, regulatórios e normativos aplicáveis, incluindo a Lei Geral de Proteção de Dados Pessoais (LGPD), bem como para o fortalecimento da cultura de segurança da informação na organização.

Compete ao comitê:

- Apoiar a definição, implementação e manutenção das estratégias de Segurança da Informação e Privacidade (SGSI e SGPI);
- Propor ajustes, aprimoramentos e modificações na estrutura normativa de segurança da informação, submetendo à aprovação da Diretoria;
- Revisar normas e procedimentos de segurança da informação e privacidade de dados;
- Solicitar informações às demais áreas para verificação do cumprimento da Política, normas e procedimentos;
- Receber, registrar e analisar casos de violação da política e normas derivadas;
- Estabelecer mecanismos de registro, controle e acompanhamento de incidentes e não conformidades;
- Notificar o encarregado de proteção de dados (DPO) em caso de incidentes envolvendo dados pessoais;
- Propor iniciativas e projetos de melhoria contínua em segurança da informação e privacidade de dados;
- Garantir a disseminação da Política e a formalização de ciência e responsabilidade pelos colaboradores;
- Atuar na gestão de riscos e apoiar a continuidade de negócios;
- Assegurar a proteção das informações clínicas e dados pessoais tratados pela cooperativa.

ÁREA DE PROTEÇÃO E PRIVACIDADE DE DADOS (PPD / DPO)

A área de Proteção e Privacidade de Dados atua como instância especializada responsável por gerenciar e administrar as atividades relacionadas à segurança da informação e à privacidade de dados pessoais no âmbito da cooperativa e recursos prórpios, contribuindo para a implementação, manutenção e melhoria contínua do Sistema de Gestão de Segurança da Informação (SGSI) e do Sistema de Gestão de Privacidade da Informação (SGPI).

Exerce papel central na definição, aplicação, monitoramento e evolução dos controles de segurança da informação, atuando tanto em nível estratégico quanto operacional, com o objetivo de garantir a efetividade das diretrizes de segurança da informação e a conformidade com a legislação vigente, em especial a Lei Geral de Proteção de Dados Pessoais (LGPD).

Compete à área de Proteção e Privacidade:

- Planejar, coordenar e executar políticas de segurança da informação, incluindo controles de acesso lógico baseados na segregação de funções e no princípio do menor privilégio;
- Interagir com os demais setores da organização, promovendo a cultura de segurança da informação e apoiando atividades relacionadas à proteção e privacidade dos dados;
- Notificar incidentes de segurança da informação às partes interessadas e à Autoridade Nacional de Proteção de Dados (ANPD), quando envolverem dados pessoais ou risco relevante aos titulares;
- Definir e indicar treinamentos relacionados à segurança da informação e privacidade de dados;
- Identificar, avaliar e tratar riscos relacionados à segurança da informação e privacidade;
- Tratar ocorrências de não conformidades relacionadas à segurança da informação;
- Estruturar, implementar e manter os controles internos de segurança da informação;
- Garantir a segregação de ambientes físicos e lógicos, prevenindo acessos indevidos e protegendo ativos;
- Recomendar à equipe de desenvolvimento a adoção de melhores práticas de desenvolvimento seguro;
- Planejar, coordenar e executar o desenvolvimento e a manutenção desta Política e das normas correlatas;
- Planejar, coordenar e executar o desenvolvimento da política de resposta a incidentes;
- Planejar e aplicar frameworks de segurança e boas práticas, tais como CIS, NIST, entre outros;
- Executar outras atividades correlatas ou determinadas pela Gerência ou Diretoria.

Gestão Operacional de Segurança da Informação

No âmbito operacional, a área de Proteção e Privacidade é responsável pela execução direta dos controles técnicos de segurança da informação nos ambientes tecnológicos da cooperativa.

Compete:

- Gerenciar e operar plataformas de prevenção, detecção e resposta a incidentes de segurança;
- Tratar incidentes de segurança da informação e manter atualizado o plano de resposta a incidentes;
- Avaliar vulnerabilidades e implementar as correções cabíveis;
- Implementar mecanismos de proteção (segurança lógica) nas plataformas tecnológicas, incluindo bancos de dados, sistemas operacionais, redes e armazenamento;
- Planejar, coordenar e executar serviços de proteção, tais como antivírus, backup, firewall e monitoramento;

- Implantar mecanismos de segurança lógica e física;
- Implementar e administrar ferramentas de segurança de rede;
- Identificar, analisar e gerenciar fluxos de tráfego de rede;
- Analisar o desempenho e a capacidade da infraestrutura de rede;
- Verificar periodicamente a conformidade das instalações de hardware e software com os padrões estabelecidos, incluindo:
  - » Auditoria de softwares instalados e identificação de softwares não homologados ou ilegais;
  - » Auditoria de equipamentos de rede para identificação de vulnerabilidades;
  - » Verificação de uso indevido de credenciais;
  - » Avaliação da conformidade de hardware, equipamentos e periféricos;
- Instalar e manter em condições adequadas os recursos tecnológicos homologados;
- Testar e indicar ferramentas e soluções tecnológicas;
- Avaliar as necessidades das áreas referentes aos recursos tecnológicos sob a ótica de segurança da informação.

Gestão Operacional de Privacidade e Proteção de Dados (LGPD)

No contexto da proteção de dados pessoais, a área de Proteção e Privacidade é responsável pela condução, execução e monitoramento das atividades relacionadas à governança e adequação à LGPD.

Compete:

- Realizar a gestão e apoiar o programa de adequação à LGPD;
- Planejar, coordenar e executar o desenvolvimento do Sistema de Gestão de Privacidade da Informação (SGPI);
- Planejar, coordenar e executar ações de conscientização em proteção de dados;
- Planejar, coordenar e executar o desenvolvimento de guias, normas e orientações para adequação à LGPD;
- Apoiar os responsáveis na adequação de novos processos e fluxos de dados pessoais;
- Planejar, coordenar e implementar indicadores relacionados ao tratamento de dados pessoais, apoiando a tomada de decisão da gerência e diretoria;
- Fiscalizar o cumprimento desta Política e das normas dela derivadas;
- Planejar, coordenar e executar atividades relacionadas às atribuições do Encarregado de Dados, conforme diretrizes da ANPD.

DIRETORIA EXECUTIVA

A Diretoria Executiva é responsável por assegurar o direcionamento estratégico da segurança da informação e da proteção de dados pessoais na Unimed Oeste do Paraná.

Compete:

- Aprovar esta Política e suas revisões;
- Nomear o Encarregado pelo Tratamento de Dados Pessoais (DPO);
- Aprovar a composição de comitê em proteção e privacidade de dados;
- Designar responsáveis pela gestão da informação;
- Acompanhar e deliberar acerca de incidentes de segurança da informação e/ou privacidade de dados relevantes;
- Assegurar o alinhamento do SGSI e do SGPI com a estratégia da organização;
- Garantir a disponibilização de recursos necessários à segurança da informação e proteção de dados; e
- Receber, por intermédio do DPO, relatórios de violações da política e das normas de segurança da informação e/ou violações da política de privacidade, quando aplicável.

GESTÃO DE NEGÓCIOS – GERÊNCIA COMERCIAL

O setor de cadastro é responsável por assegurar que as relações com clientes, beneficiários e parceiros sob sua gestão estejam alinhadas às diretrizes de segurança da informação e proteção de dados pessoais.

Compete:

- Assegurar nos contratos sob sua responsabilidade a inclusão de cláusulas contratuais relacionadas à segurança da informação e proteção de dados;
- Assegurar a conformidade com a LGPD nas atividades sob sua responsabilidade;
- Reportar incidentes e não conformidades relacionadas à segurança da informação;
- Apoiar a definição de diretrizes relacionadas ao tratamento de dados de clientes e beneficiários.

DEPARTAMENTO PESSOAL

A área de departamento pessoal é responsável por assegurar que os processos relacionados a colaboradores estejam alinhados às diretrizes de segurança da informação e privacidade de dados.

Compete:

- Gerenciar processos de admissão, movimentação e desligamento com impacto nos acessos;
    1. Garantir a ciência desta Política e a formalização de termos de sigilo e responsabilidade e termo de uso de imagem;
    2. Providenciar a assinatura do Termo de Sigilo ou NDA, Responsabilidade e confidencialidade;
    3. Promover ações de treinamento e conscientização;
    4. Apoiar a aplicação de medidas disciplinares em caso de descumprimento;
    5. Assegurar a conformidade com a LGPD no tratamento de dados pessoais de colaboradores sob sua responsabilidade.

6. Informar através do software de helpdesk aos responsáveis pelo gerenciamento das credenciais sobre as mudanças nos acessos dos colaboradores em caso contratações, alterações de função/setor ou demissões;
7. Em caso de demissões registrar através do software de helpdesk a solicitação de bloqueio imediato ou transferência do login para seu gestor;
8. Garantir a coleta/atualização do termo de consentimento junto aos colaboradores sempre que necessário;

GESTÃO DE RECURSOS FINANCEIROS

A área financeira é responsável por assegurar a segurança das informações e transações sob sua responsabilidade.

Compete:

- Garantir a adoção de controles de segurança em transações financeiras;
- Implementar mecanismos de prevenção a fraudes;
- Garantir que os fornecedores sejam avaliados sob critérios de segurança da informação e privacidade de dados;
- Assegurar a conformidade com a LGPD.

GESTÃO DE TECNOLOGIA DA INFORMAÇÃO

A área de Tecnologia da Informação é responsável por apoiar a implementação e manutenção dos controles de segurança da informação nos sistemas e ambientes sob sua responsabilidade, conforme diretrizes estabelecidas pela área de Proteção e Privacidade.

Compete:

- Apoiar a implementação de controles de segurança nos sistemas e aplicações;
- Assegurar que acessos a sistemas e ambientes tecnológicos sejam concedidos, revisados e revogados conforme princípios de necessidade e menor privilégio;
- Tratar vulnerabilidades e incidentes relacionados aos sistemas de gestão e/ou aplicações;
- Gerenciar registros (logs), trilhas de auditoria e mecanismos de monitoramento, assegurando sua integridade, retenção e disponibilidade para análise;
- Garantir a segurança no desenvolvimento, aquisição, manutenção e uso de sistemas, observando princípios de segurança e privacidade desde a concepção;
- Garantir a segurança no desenvolvimento e uso de sistemas;
- Manter inventário atualizado dos ativos tecnológicos;
- Reportar incidentes de segurança à área de Proteção e Privacidade;
- Garantir a gestão segura do ciclo de vida de scripts, incluindo sua implementação, execução controlada e monitoramento, conforme normas internas estabelecidas;

- Implementar e manter processo formal de gestão de mudanças, garantindo que alterações em ambientes tecnológicos sejam realizadas de forma controlada, rastreável e com análise de riscos;
- Garantir a identificação, análise e tratamento de problemas de TI, visando a continuidade dos serviços e a melhoria contínua dos ambientes tecnológicos;
- Cumprir e fazer cumprir as normas internas de segurança da informação e privacidade de dados aplicáveis;
- Assegurar que os sistemas, aplicações estejam aderentes às diretrizes de segurança da informação e privacidade de dados da organização.

USUÁRIOS INTERNOS E EXTERNOS

Todos os usuários são responsáveis por utilizar os ativos de informação de forma segura e em conformidade com esta Política.

Compete:

- Cumprir esta Política e normas associadas;
- Proteger suas credenciais de acesso;
- Utilizar os recursos de forma adequada e segura;
- Reportar incidentes e não conformidades;
- Zelar pela confidencialidade, integridade e disponibilidade das informações;
- Participar das ações de conscientização quando aplicável;
- Atuar em conformidade com a LGPD.

PROPRIETÁRIO DA INFORMAÇÃO

O Proprietário da Informação é responsável por garantir a governança das informações sob sua responsabilidade, assegurando sua classificação, proteção, uso adequado e conformidade com requisitos legais, regulatórios e normativos.

Compete:

- Classificar e rotular as informações conforme critérios definidos pela organização;
- Definir, aprovar e revisar regras de acesso, uso e compartilhamento das informações, assegurando a aplicação do princípio do menor privilégio;
- Garantir que controles de segurança proporcionais ao nível de classificação da informação sejam aplicados;
- Assegurar a proteção das informações durante todo o seu ciclo de vida, incluindo criação, armazenamento, uso, compartilhamento, retenção e descarte;
- Garantir que o tratamento de dados pessoais esteja em conformidade com a LGPD e diretrizes internas de proteção e privacidade;

- Apoiar a gestão de riscos relacionados às informações, incluindo sua identificação, avaliação e tratamento;
- Apoiar a resposta a incidentes de segurança da informação, incluindo a análise de impacto e definição de ações corretivas;
- Assegurar que as informações sob sua responsabilidade estejam devidamente inventariadas e sob controle;
- Atuar em conjunto com as áreas de Tecnologia da Informação e Proteção e Privacidade na definição e implementação de controles.

PRINCÍPIOS E DIRETRIZES

A segurança da informação e a proteção de dados pessoais na **Unimed Oeste do Paraná são** orientadas por princípios e diretrizes que estabelecem a forma como a organização deve proteger seus ativos de informação e conduzir o tratamento de dados pessoais. Esses princípios e diretrizes devem ser observados por todas as áreas, colaboradores e terceiros, servindo como base para a definição de normas, procedimentos e controles de segurança da informação e privacidade.

ESTRUTURA NORMATIVA DA SEGURANÇA DA INFORMAÇÃO

Todas as normas serão gerenciadas através da ferramenta de qualidade, nela será possível armazenar, visualizar e imprimir todas as seguintes normas:

Normas Básicas:

- Acesso à Internet;
- Uso Seguro de Redes Sociais;
- Acesso ao Correio Eletrônico;
- Backup e Recuperação de Dados;
- Gestão de Ativos;
- Proteção de Código Maliciosos;
- Segurança física;
- Norma de Gestão e perfis de acesso;
- Uso de dispositivos móveis;
- Uso de acesso remoto por colaboradores e uso de acesso remoto por terceiros para prestação de serviços;
- Troca de informações com empresas/entidades terceiras;
- Prazos e métodos de descarte seguro de dados (formato digital ou físico);
- Uso do sistema de monitoramento/segurança (alarme e DVRs);
- Acesso a sistemas de monitoramento Remoto;

- Norma de Proteção de Dados Pessoais;
- Classificação das informações;
- Gestão de Vulnerabilidades;
- Gestão de Registros–logs de auditoria;
- Norma de mesa e tela limpa;
- Norma Derivada LGPD (ND 015 Unimed do Brasil).

Normas Adicionais:

- Aquisição, Desenvolvimento e Manutenção de Sistemas/Aplicações;
- Gerenciamento de Riscos;
- Gerenciamento de Continuidade de Negócios;
- Gerenciamento de Mudanças de TI;
- Gerenciamento de problemas de TI;
- Gerenciamento do tempo de retenção dos dados pessoais (Tabela de temporalidade);
- Norma de resposta a incidentes de Privacidade;
- Política de Tratamento e Resposta a Incidentes;
- Segurança em Terceirização e Prestação de Serviços;
- Uso da Computação em Nuvem.

DECLARAÇÃO DE COMPROMETIMENTO DA DIREÇÃO

A Diretoria da **Unimed Oeste do Paraná**, ciente da importância da segurança da informação e da proteção da privacidade para a sustentabilidade do negócio, assegura que o Sistema de Gestão de Segurança da Informação (SGSI) e o Sistema de Gestão de Privacidade da Informação (SGPI) estejam alinhados à direção estratégica da organização.

Para tanto, compromete-se a disponibilizar os recursos necessários para sua implementação, manutenção e melhoria contínua, bem como a promover a disseminação desta Política e o fortalecimento da cultura de segurança e privacidade em todos os níveis da organização.

PRINCÍPIOS DE SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE

A segurança da informação e a proteção de dados pessoais na Unimed Oeste do Paraná devem observar os seguintes princípios:

Confidencialidade: garantir que as informações sejam acessadas apenas por pessoas devidamente autorizadas;

Integridade: assegurar que as informações sejam mantidas íntegras, completas e protegidas contra alterações indevidas ou não autorizadas;

Disponibilidade: garantir que as informações estejam acessíveis e disponíveis sempre que necessário, de forma segura e oportuna;

Autenticidade: assegurar a veracidade da identidade de usuários, sistemas e processos envolvidos no tratamento da informação;

Responsabilização (*Accountability*): garantir que todas as ações relacionadas ao tratamento da informação sejam passíveis de identificação, registro e responsabilização;

Finalidade: assegurar que o tratamento de dados pessoais seja realizado para propósitos legítimos, específicos e informados ao titular;

Necessidade e Minimização: limitar o tratamento de dados pessoais ao mínimo necessário para a realização de suas finalidades;

Segurança desde a concepção e por padrão (*Privacy by Design e by Default*): assegurar que a segurança da informação e a proteção de dados pessoais sejam consideradas desde a concepção de processos, sistemas e serviços, bem como configuradas como padrão

DIRETRIZES GERAIS DE SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE

A segurança da informação e a privacidade dos dados pessoais devem ser aplicadas de forma integrada e transversal em toda a Unimed Oeste do Paraná, observando as seguintes diretrizes:

- Todas as áreas da organização são responsáveis pela proteção das informações sob sua gestão, devendo observar esta Política e as normas dela derivadas;
- Os ativos de informação devem possuir responsáveis formalmente definidos, responsáveis por sua gestão e proteção ao longo de todo o seu ciclo de vida;
- As informações devem ser classificadas e tratadas de acordo com seu nível de sensibilidade e criticidade;
- O tratamento de dados pessoais deve observar os princípios e requisitos estabelecidos na legislação vigente, especialmente a LGPD;
- Os controles de segurança da informação devem ser aplicados de forma proporcional aos riscos identificados;
- A segurança da informação deve ser considerada na definição, contratação, desenvolvimento e operação de processos, sistemas e serviços;
- A organização deve adotar medidas técnicas e administrativas para proteção contra acessos não autorizados, perdas, vazamentos ou qualquer forma de tratamento inadequado da informação;
- Incidentes de segurança da informação e privacidade devem ser reportados, tratados e registrados conforme diretrizes estabelecidas;
- A organização deve promover ações periódicas de conscientização e capacitação em segurança da informação e proteção de dados pessoais, no mínimo anuais, contemplando boas práticas, riscos e responsabilidades dos usuários;

- Todos os contratos firmados pela organização devem observar as diretrizes de segurança da informação e proteção de dados pessoais, conforme sua aplicabilidade;
- A segurança da informação deve ser considerada na gestão de mudanças, novos projetos e iniciativas organizacionais;
- Devem ser estabelecidos mecanismos de monitoramento, auditoria e melhoria contínua dos controles de segurança da informação e privacidade.

DIRETRIZES PARA GESTÃO DE ATIVOS

Os ativos de informação da Unimed Oeste do Paraná devem ser identificados, classificados, protegidos e gerenciados ao longo de todo o seu ciclo de vida, desde a sua criação até o descarte.

Devem ser observadas as seguintes diretrizes:

- Todos os ativos de informação devem possuir um responsável formalmente designado, responsável por sua gestão e proteção;
- O responsável pelo ativo deve garantir o cumprimento das diretrizes desta Política e das normas associadas, podendo delegar atividades sob sua supervisão, quando cabível e previamente autorizado;
- Os ativos de informação devem ser gerenciados ao longo de todo o seu ciclo de vida, incluindo criação, processamento, armazenamento, compartilhamento e descarte;
- Os ativos devem ser identificados, mapeados e mantidos atualizados periodicamente ou sempre que houver mudanças relevantes;
- As informações devem ser protegidas de acordo com sua criticidade e sensibilidade;
- Devem ser adotadas medidas para prevenir acessos não autorizados, perda, alteração indevida ou uso inadequado das informações;
- Os responsáveis pelos ativos devem reportar à área de Proteção e Privacidade incidentes, desvios ou condutas inadequadas relacionadas às informações sob sua gestão;
- A organização deve assegurar que as pessoas envolvidas no tratamento da informação possuam a competência necessária para o desempenho de suas funções, promovendo ações de capacitação quando aplicável;
- Devem ser observados os requisitos legais e regulatórios aplicáveis à gestão dos ativos de informação.

DIRETRIZES PARA CLASSIFICAÇÃO DA INFORMAÇÃO

As informações da Unimed Oeste do Paraná devem ser classificadas de acordo com seu nível de sensibilidade, criticidade e requisitos legais, de forma a garantir a adoção de controles adequados para sua proteção.

Devem ser observadas as seguintes diretrizes:

- Todas as informações devem ser classificadas pelo responsável ou proprietário da informação, conforme critérios definidos pela organização;

- A classificação da informação deve considerar, no mínimo, requisitos legais, impacto para o negócio e riscos associados ao seu tratamento;
- Os dados pessoais devem ser classificados conforme sua natureza, observando as disposições da Lei Geral de Proteção de Dados Pessoais (LGPD), incluindo dados pessoais e dados pessoais sensíveis;
- Devem ser adotadas medidas diferenciadas de proteção conforme o nível de classificação da informação;
- As informações devem ser tratadas de forma adequada ao seu nível de classificação durante todo o seu ciclo de vida;
- A classificação das informações deve ser revisada periodicamente ou sempre que houver alterações relevantes em seu contexto ou finalidade;
- O acesso às informações deve ser concedido de acordo com sua classificação, observando o princípio do menor privilégio;
- Devem ser definidos critérios para armazenamento, retenção e descarte seguro das informações, conforme sua classificação e requisitos legais aplicáveis;
- Informações classificadas como sensíveis devem possuir controles adicionais de proteção, incluindo restrições de acesso e mecanismos de segurança apropriados.

DIRETRIZES PARA CONTROLE DE ACESSO

O acesso aos ativos de informação, sistemas, redes e recursos tecnológicos da Unimed Oeste do Paraná deve ser controlado de forma a garantir que apenas usuários autorizados tenham acesso às informações necessárias para o desempenho de suas funções

Gestão de Acessos Lógicos

- O controle de acesso deve ser baseado em processos formais de identificação, autenticação e autorização de usuários;
- Devem existir critérios formais para criação, alteração e revogação de acessos;
- O ciclo de vida dos acessos deve ser gerenciado, contemplando concessão, revisão periódica (mínimo anual), alteração e revogação;
- Os acessos devem ser concedidos com base no princípio do menor privilégio e necessidade de acesso;
- Deve existir definição de prazos para atendimento das solicitações de acesso;
- A gestão de acessos deve abranger todos os sistemas, aplicações e recursos tecnológicos da organização;
- Os processos devem ser formalizados e aprovados pela Diretoria Executiva.

Acesso à Rede, Sistemas e Aplicações

- O acesso deve ser individual, pessoal e intransferível;
- O usuário é responsável pelo uso de suas credenciais;
- O acesso à rede deve ser controlado de forma centralizada;

- Serviços e acessos não autorizados devem ser bloqueados;
- O acesso deve ocorrer por meio de mecanismos seguros de autenticação;
- As transações devem ser protegidas contra interceptação e uso indevido.

Autenticação e Gestão de Credenciais (senhas)

- Devem ser definidos critérios de complexidade de senhas conforme norma específica;
- Deve haver bloqueio de contas após tentativas inválidas;
- Deve existir periodicidade de troca de senha conforme criticidade;
- O uso de autenticação multifator (MFA) deve ser obrigatório para:
- Acessos privilegiados
- Acessos remotos
- Sistemas que tratem dados pessoais

Controle de Acesso por Perfis e Segregação de Funções

- O controle de acesso deve ser baseado em perfis, funções ou papéis;
- Deve ser aplicada segregação de funções para reduzir riscos de fraude ou uso indevido;
- Perfis de acesso devem ser revisados periodicamente.

Dispositivos Móveis

O uso de dispositivos móveis para acesso à rede e aos recursos computacionais da Unimed Oeste do Paraná deve ser controlado e regulamentado por meio de normas e procedimentos específicos de segurança da informação.

Devem ser observadas as seguintes diretrizes:

- O uso de dispositivos móveis corporativos ou pessoais (BYOD) deve ser previamente autorizado, mediante processo formal de aprovação;
- A autorização para uso de dispositivos pessoais deve conter, no mínimo:
  - » Justificativa do uso, incluindo a impossibilidade de utilização de equipamento corporativo;
  - » Período de autorização (data de início e término);
  - » Recursos e sistemas que poderão ser acessados;
  - » Local ou área de utilização;
  - » Identificação do responsável pela autorização;
  - » Identificação do responsável pelo dispositivo;
- O acesso deve ser realizado mediante mecanismos seguros de autenticação, sendo obrigatória a utilização de credenciais individuais;
- Os dispositivos devem possuir controles mínimos de segurança, incluindo:
  - » Proteção contra códigos maliciosos (antivírus, EDR ou tecnologia equivalente);
  - » Atualizações de segurança aplicadas;
  - » Mecanismos de bloqueio de tela e proteção por senha ou biometria;

- A organização poderá restringir, bloquear ou revogar o acesso de dispositivos que não atendam aos requisitos de segurança estabelecidos;
- O uso de dispositivos móveis deve observar as diretrizes de proteção de dados pessoais, confidencialidade e uso aceitável dos ativos de informação;
- Os critérios técnicos e operacionais para uso de dispositivos móveis devem ser definidos em norma específica.

Acesso Remoto

O acesso remoto aos ativos de informação, sistemas e recursos tecnológicos da Unimed Oeste do Paraná deve ser controlado e realizado de forma segura, quando efetuado fora das instalações ou por meio de infraestrutura não pertencente à cooperativa.

Devem ser observadas as seguintes diretrizes:

- O acesso remoto deve ser previamente autorizado por meio de processo formal, considerando a necessidade de negócio e o perfil de acesso do usuário;
- Devem ser estabelecidas regras claras quanto às responsabilidades dos usuários internos, terceiros, parceiros e prestadores de serviço que utilizarem acesso remoto;
- O acesso remoto deve utilizar mecanismos seguros de conexão, incluindo, quando aplicável:
  - » Redes privadas virtuais (VPN);
  - » Criptografia de comunicação;
  - » Autenticação multifator (MFA);
- O acesso deve respeitar o princípio do menor privilégio, sendo limitado aos recursos estritamente necessários para a execução das atividades;
- Os acessos remotos devem ser registrados e monitorados, garantindo rastreabilidade das ações realizadas;
- Dispositivos utilizados para acesso remoto devem atender aos requisitos mínimos de segurança definidos pela organização;
- A organização poderá restringir, suspender ou bloquear acessos remotos que apresentem riscos à segurança da informação ou não estejam em conformidade com as diretrizes estabelecidas;
- Os critérios técnicos e operacionais para acesso remoto devem ser definidos em norma específica.

DIRETRIZES PARA SEGURANÇA EM PESSOAS

A segurança da informação e a proteção de dados pessoais devem ser consideradas em todo o ciclo de vida do vínculo dos colaboradores, terceiros e demais usuários com a Unimed Oeste do Paraná, desde o processo de seleção até o encerramento de suas atividades.

Devem ser observadas as seguintes diretrizes:

Antes da Contratação

- Devem ser adotados critérios de seleção compatíveis com as responsabilidades do cargo, especialmente para funções que envolvam acesso a informações sensíveis;
- O processo de contratação deve prever a avaliação de perfil do candidato, considerando aspectos de segurança da informação e aderência às atividades a serem desempenhadas;
- Devem ser formalizadas, em contrato ou documentos equivalentes, as responsabilidades relacionadas à segurança da informação e proteção de dados;
- Deve ser obrigatória a assinatura de Termo de Confidencialidade, Sigilo e Responsabilidade por todos os colaboradores e terceiros;
- Quando aplicável, devem ser realizados procedimentos adicionais de verificação, conforme requisitos legais e o nível de criticidade da função.

Durante a contratação

Devem ser definidos e documentados os requisitos de segurança da informação aplicáveis a cada função ou perfil de acesso;

- O acesso a sistemas, informações e ativos deve ser concedido somente após a formalização das responsabilidades e obrigações do usuário;
- Os acessos devem ser compatíveis com o nível de sensibilidade das informações e com as atribuições do usuário;
- A organização deve promover ações contínuas de conscientização e capacitação em segurança da informação e proteção de dados pessoais;
- Os colaboradores e terceiros devem utilizar os ativos de informação de forma adequada, ética e em conformidade com as políticas e normas internas;
- Devem ser estabelecidos mecanismos para reporte de incidentes, comportamentos inadequados ou violações de segurança.

Movimentação Interna e Encerramento do Vínculo

- Processos de movimentação interna devem contemplar a revisão e ajuste dos acessos conforme a nova função exercida;
- O desligamento de colaboradores ou encerramento de contratos deve assegurar a revogação tempestiva de acessos a sistemas, redes e informações;
- Deve ser garantida a devolução de ativos de informação sob responsabilidade do usuário;
- Devem ser observados procedimentos formais de desligamento, incluindo comunicação às áreas responsáveis pela gestão de acessos;
- Deve ser reforçada a manutenção do dever de confidencialidade das informações após o encerramento do vínculo com a organização.

Confidencialidade e Responsabilidade (NDA)

- Todos os colaboradores, terceiros e demais usuários devem assinar Termo de Confidencialidade e Sigilo, independentemente do nível de acesso às informações;
- O termo deve abranger a proteção de informações em qualquer formato, incluindo dados digitais, documentos físicos, comunicações verbais e outros meios;
- Devem ser claramente estabelecidas as responsabilidades e penalidades em caso de uso indevido ou divulgação não autorizada de informações;
- O dever de confidencialidade deve permanecer válido mesmo após o encerramento do vínculo com a organização.

SEGURANÇA OPERACIONAL

A segurança operacional estabelece diretrizes para garantir que os processos, sistemas e recursos tecnológicos da Unimed Oeste do Paraná sejam operados de forma segura, controlada e resiliente, prevenindo falhas, acessos indevidos, perdas de dados e interrupções nos serviços.

Devem ser adotadas práticas formais para gestão, monitoramento e controle das operações, assegurando a integridade, disponibilidade e confidencialidade das informações ao longo de todo o seu ciclo de vida.

Gestão Operacional de Segurança

A organização deve estabelecer e manter processos operacionais que garantam a execução segura das atividades tecnológicas, incluindo:

- Implementação e manutenção de controles de segurança lógica nos ambientes tecnológicos;
- Adoção de mecanismos de proteção contra ameaças cibernéticas;
- Gestão segura da infraestrutura de tecnologia da informação;
- Monitoramento contínuo dos ambientes e serviços;
- Aplicação de boas práticas de *hardening* e configuração segura.

Proteção contra Códigos Maliciosos

Devem ser implementados mecanismos de proteção contra códigos maliciosos e ameaças cibernéticas, baseados em tecnologias de prevenção, detecção e resposta, incluindo:

- Uso de soluções de proteção de endpoint e rede, capazes de prevenir, detectar e responder a ameaças, incluindo malware, ransomware e comportamentos suspeitos;
- Adoção de tecnologias baseadas em análise comportamental, inteligência artificial e/ou assinaturas, conforme aplicável;
- Monitoramento contínuo de eventos de segurança e atividades suspeitas nos ambientes tecnológicos;
- Capacidade de resposta a incidentes, incluindo bloqueio, isolamento e remediação de ativos comprometidos;
- Atualização contínua dos mecanismos de proteção e das capacidades de detecção;

- Restrição da execução de arquivos, aplicações e códigos não autorizados, conforme políticas de segurança definidas.

Gestão de Vulnerabilidades

Devem ser estabelecidos processos contínuos para identificação, avaliação e tratamento de vulnerabilidades, incluindo:

- Realização periódica de varreduras de vulnerabilidades;
- Aplicação de correções e atualizações de segurança (patches);
- Priorização baseada em risco;
- Monitoramento de exposições e falhas conhecidas;
- Integração com o inventário de ativos de informação;
- Definição de prazos para tratamento conforme criticidade;
- Execução conforme norma específica de gerenciamento de vulnerabilidades.

Gestão de Logs e Monitoramento

Devem ser implementados mecanismos para registro, monitoramento, análise e tratamento de eventos de segurança da informação, garantindo a rastreabilidade, detecção de incidentes e suporte à auditoria.

Devem ser observadas as seguintes diretrizes:

- Registro de logs de acesso, autenticação e atividades relevantes contendo informações suficientes para rastreabilidade;
- Proteção contra alteração ou exclusão indevida de logs;
- Deve ser garantida a sincronização de horário dos sistemas (NTP ou equivalente), assegurando a integridade temporal dos registros;
- Deve ser realizado monitoramento contínuo dos eventos de segurança, com identificação de atividades suspeitas, anômalas ou não autorizadas;
- Devem ser implementados mecanismos de geração de alertas para eventos críticos ou comportamentos fora do padrão;
- O acesso aos logs deve ser restrito e controlado, garantindo a confidencialidade das informações registradas;
- Correlação de eventos para identificação de incidentes de segurança;
- Manutenção dos logs conforme requisitos legais e normativos;
- Execução conforme norma específica de gestão de registros/logs de auditoria.

Backup e Recuperação de Dados

Devem ser estabelecidos processos formais para backup e recuperação de dados, incluindo:

- Definição dos dados a serem protegidos;
- Frequência de execução dos backups;
- Definição de responsáveis;
- Armazenamento seguro e segregado das cópias;

- Testes periódicos de restauração;
- Definição de tempo de retenção;
- Definição de objetivos de recuperação (RTO e RPO);
- Procedimentos de descarte seguro das mídias;
- Execução conforme norma específica de backup e recuperação de dados.

Gestão de Mudanças Operacionais (GMUD)

A Gestão de Mudanças Operacionais, também denominada GMUD (Gestão de Mudanças de Tecnologia da Informação), estabelece diretrizes para que alterações em sistemas, infraestrutura e serviços tecnológicos sejam realizadas de forma controlada, segura e rastreável.

- Nenhuma mudança deve ser realizada sem registro e aprovação adequada;
- As mudanças devem ser avaliadas quanto a risco, impacto e criticidade;
- Deve existir planejamento formal, incluindo plano de execução e reversão;
- As mudanças devem ser classificadas (padrão, normal e emergencial);
- Mudanças críticas devem ser aprovadas pelas instâncias competentes;
- Mudanças emergenciais devem ser justificadas e revisadas posteriormente;
- Deve ser realizada revisão pós-implementação;
- Todas as mudanças devem possuir evidências registradas;
- O processo deve seguir norma específica de gestão de mudanças.

Segregação de Ambientes

Devem ser mantidos ambientes segregados, incluindo:

- Separação entre produção, homologação e desenvolvimento;
- Restrição de acesso entre ambientes;
- Proteção de dados em ambientes de teste por anonimização ou pseudonimização;
- Replicação de controles de segurança entre ambientes.

Auditoria Técnica e Conformidade Operacional

Devem ser realizadas verificações periódicas nos ambientes tecnológicos, com o objetivo de assegurar a conformidade operacional, a segurança dos ativos de informação e a aderência às normas internas e requisitos aplicáveis.

- Devem ser observadas as seguintes diretrizes:
- Os ambientes tecnológicos devem ser avaliados quanto à conformidade com padrões de segurança, configurações e requisitos estabelecidos pela organização;
- Devem ser identificadas e tratadas não conformidades técnicas que possam comprometer a segurança da informação;
- Devem ser realizadas avaliações periódicas de segurança, incluindo análise de vulnerabilidades e aderência a padrões definidos;
- O uso dos recursos tecnológicos deve ser monitorado quanto à conformidade com as diretrizes institucionais;

- Os critérios, métodos e ferramentas utilizados devem ser definidos em procedimento ou norma específica.

CRIPTOGRAFIA

A criptografia deve ser utilizada como mecanismo de proteção para assegurar a confidencialidade, integridade e autenticidade das informações, especialmente aquelas classificadas como confidenciais, restritas ou que contenham dados pessoais.

Diretrizes

Devem ser adotados mecanismos criptográficos adequados para proteção de informações em trânsito e em repouso, conforme a criticidade dos dados;

- O uso de criptografia deve ser aplicado de forma proporcional aos riscos identificados e à classificação da informação;
- Devem ser utilizados algoritmos, protocolos e padrões reconhecidos pelo mercado e considerados seguros;
- Deve ser estabelecido processo formal para gestão do ciclo de vida das chaves criptográficas, incluindo geração, armazenamento, distribuição, uso, rotação e descarte;
- O acesso às chaves criptográficas deve ser restrito a pessoas autorizadas, com controle e rastreabilidade;
- Devem ser adotadas medidas para proteção de chaves contra acesso não autorizado, perda ou comprometimento;
- A criptografia deve ser aplicada em processos de comunicação, armazenamento, backup e transferência de informações sensíveis;
- Devem ser consideradas técnicas de anonimização e pseudonimização sempre que aplicável ao tratamento de dados pessoais;
- A implementação de controles criptográficos deve estar alinhada aos requisitos legais, regulatórios e às normas internas da cooperativa.

Gestão de Chaves Criptográficas

A gestão de chaves criptográficas deve ser realizada de forma segura e controlada, garantindo a proteção dos mecanismos utilizados para cifrar e decifrar informações.

Devem ser observadas as seguintes diretrizes:

- Deve ser estabelecido processo formal para gestão do ciclo de vida das chaves criptográficas, incluindo geração, distribuição, armazenamento, uso, rotação e descarte;
- O acesso às chaves criptográficas deve ser restrito a usuários autorizados, com controle, rastreabilidade e segregação de funções quando aplicável;
- As chaves devem ser protegidas contra acesso não autorizado, perda, divulgação ou comprometimento;
- Devem ser definidos critérios para periodicidade de rotação de chaves, conforme criticidade da informação;

- Devem ser utilizados mecanismos seguros para armazenamento e proteção de chaves criptográficas;
- A revogação ou substituição de chaves deve ser realizada sempre que houver suspeita ou confirmação de comprometimento;

SEGURANÇA FÍSICA E DO AMBIENTE

A segurança física e do ambiente deve garantir a proteção das instalações, equipamentos, ativos de informação e pessoas contra acessos não autorizados, danos, interferências e outras ameaças que possam comprometer a segurança da informação e a privacidade dos dados.

Diretrizes:

- O acesso às instalações físicas deve ser controlado por meio de processo formal, garantindo que apenas pessoas autorizadas tenham acesso às áreas administrativas e técnicas;
- Devem ser estabelecidos critérios formais para concessão, revisão e revogação de acessos físicos, considerando colaboradores, terceiros e visitantes;
- O acesso físico deve ser registrado, monitorado e mantido para fins de rastreabilidade e auditoria";
- Visitantes e prestadores de serviço devem ser identificados, registrados e acompanhados durante sua permanência nas dependências da cooperativa e recursos próprios;
- Devem ser implementados mecanismos de controle físico, tais como crachás, chaves, catracas, biometria, recepção ou outros meios equivalentes;
- Áreas que contenham ativos críticos de informação devem possuir controles adicionais de restrição e monitoramento;
- Devem ser utilizados mecanismos de vigilância e monitoramento, como sistemas de CFTV, quando aplicável;
- Equipamentos e ativos devem ser protegidos contra acesso indevido, danos físicos, furtos e interferências;
- Devem ser adotadas medidas para proteção contra ameaças ambientais, como incêndios, falhas elétricas e desastres;
- O uso de identificação funcional (crachá) deve ser obrigatório nas dependências da cooperativa;
- O processo de controle de acesso físico deve ser formalizado em norma específica, aprovada pela Diretoria Executiva;
- Os controles estabelecidos devem ser aplicados de forma contínua e passíveis de verificação.

COMUNICAÇÕES E REDES

As comunicações e redes devem ser protegidas de forma a garantir a segurança das informações trafegadas, prevenindo acessos não autorizados, vazamentos, interceptações ou alterações indevidas durante a transmissão e processamento dos dados.

Diretrizes

- As redes e os ambientes tecnológicos devem ser configurados e operados de forma segura, com controles adequados para proteção das informações;
- O uso da internet corporativa deve observar as diretrizes estabelecidas em norma específica, contemplando requisitos de segurança, monitoramento, controle de acesso e uso aceitável;
- Deve ser garantida a segregação lógica e, quando aplicável, física dos ambientes e redes, de modo a reduzir riscos de acesso indevido ou propagação de incidentes;
- Ambientes de produção, homologação e desenvolvimento devem ser segregados, garantindo que testes ou alterações não impactem sistemas produtivos;
- O tráfego de rede deve ser monitorado e analisado, permitindo a identificação de atividades suspeitas ou não autorizadas;
- Devem ser adotados mecanismos de proteção para comunicações, incluindo criptografia, autenticação e controle de acesso;
- A transferência de informações, internas ou externas, deve ocorrer de forma segura, utilizando mecanismos que garantam confidencialidade, integridade e rastreabilidade;
- Devem ser estabelecidas regras para troca de informações com terceiros, considerando requisitos de segurança da informação e a privacidade dos dados pessoais;
- Serviços, aplicações e portas de rede não autorizados devem ser restritos ou bloqueados;
- O acesso às redes deve ser controlado com base em necessidade de negócio e perfil de acesso;
- Devem ser adotadas medidas para proteção contra interceptação, alteração ou perda de dados durante a transmissão;
- Devem ser adotadas medidas para garantir a disponibilidade e continuidade dos serviços de comunicação;
- A comunicação deve observar requisitos legais, regulatórios e normativos aplicáveis;
- A execução dos controles deve seguir normas específicas relacionadas à segurança de redes e comunicação.

SISTEMAS E DESENVOLVIMENTO

Os sistemas de informação devem ser concebidos, adquiridos, desenvolvidos e mantidos de forma segura, garantindo a proteção das informações e dos dados pessoais ao longo de todo o seu ciclo de vida.

Diretrizes

- A segurança da informação e a proteção de dados pessoais devem ser consideradas desde a concepção de sistemas, aplicações, APIs e processos (***security by design e privacy by design***);
- Requisitos de segurança devem ser definidos previamente à contratação, desenvolvimento ou aquisição de sistemas;
- Ambientes de desenvolvimento, homologação e produção devem ser segregados;

- Dados pessoais utilizados em ambientes de testes devem ser anonimizados ou pseudonimizados sempre que possível;
- O acesso a sistemas e ambientes deve ser controlado conforme perfis e níveis de privilégio definidos;
- Devem ser adotados mecanismos de autenticação segura para acesso a sistemas e aplicações;
- Alterações em sistemas devem seguir processo formal de gestão de mudanças;
- Devem ser realizados testes antes da entrada em produção, incluindo testes de segurança quando aplicável;
- Sistemas devem possuir mecanismos de registro de logs e trilhas de auditoria;
- Vulnerabilidades identificadas devem ser tratadas de forma tempestiva;
- A contratação de sistemas deve considerar requisitos de segurança da informação e proteção de dados pessoais;
- O ciclo de vida dos sistemas deve contemplar atualização, manutenção e descontinuação segura.

TERCEIROS

A relação com terceiros deve garantir que os requisitos de segurança da informação e proteção de dados pessoais sejam devidamente estabelecidos, avaliados e monitorados.

Diretrizes

- Terceiros que tenham acesso a informações, sistemas ou dados pessoais devem atender aos requisitos de segurança da informação e privacidade estabelecidos pela organização;
- A contratação de terceiros deve prever cláusulas contratuais específicas sobre segurança da informação e proteção de dados pessoais;
- Deve ser realizada avaliação prévia de segurança e privacidade dos terceiros antes da contratação;
- O compartilhamento de informações com terceiros deve ocorrer de forma controlada e segura;
- Terceiros devem atuar em conformidade com as diretrizes da organização e com a legislação vigente;
- Devem ser estabelecidos controles para acesso de terceiros aos ambientes e sistemas;
- Incidentes envolvendo terceiros devem ser comunicados e tratados conforme diretrizes estabelecidas;
- Deve ser garantida a rastreabilidade das atividades realizadas por terceiros;
- A organização deve prever mecanismos de auditoria e monitoramento dos serviços prestados por terceiros;
- Ao término da relação contratual, devem ser definidos procedimentos para devolução ou descarte seguro das informações;
- Serviços em nuvem devem atender aos requisitos de segurança, privacidade e legislação aplicável.

GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE

A organização deve manter processo formal, estruturado e integrado para gestão de incidentes de segurança da informação e de proteção de dados pessoais, abrangendo identificação, registro, classificação, tratamento, resposta e melhoria contínua.

Diretrizes

Governança e Processo:

- Deve ser mantido processo formal para gestão de incidentes de segurança da informação e privacidade;
- A gestão de incidentes deve considerar abordagem integrada entre segurança da informação e privacidade de dados pessoais;
- Devem ser definidos e formalizados papéis e responsabilidades para atuação no processo de gestão de incidentes, conforme estrutura de governança da organização;

Identificação e Registro

- A organização deve assegurar que incidentes sejam identificados, reportados e devidamente registrados;
- Todos os colaboradores e terceiros devem comunicar imediatamente incidentes ou suspeitas de incidentes;

Classificação e Avaliação

- Incidentes devem ser registrados e classificados conforme critérios definidos;
- Deve ser avaliada a ocorrência de risco ou dano relevante aos titulares, conforme legislação aplicável;

Tratamento e Resposta

- A organização deve assegurar a adoção de medidas para contenção, mitigação e recuperação dos incidentes;
- Devem ser implementadas ações corretivas e preventivas;
- Devem ser mantidos registros e evidências dos incidentes e das ações realizadas;
- Deve ser realizada análise de causa raiz e definição de ações corretivas e preventivas;

Comunicação e Escalonamento

- Deve existir fluxo formal de comunicação e escalonamento;
- Incidentes com dados pessoais devem ser tratados conforme requisitos da Lei Geral de Proteção de Dados e diretrizes da Autoridade Nacional de Proteção de Dados, incluindo comunicação aos órgãos competentes e titulares quando aplicável;
- As informações relacionadas a incidentes devem ser tratadas de forma confidencial e controlada, respeitando níveis de classificação da informação e restrições de acesso;

Monitoramento e Melhoria Contínua

- O processo deve ser monitorado e continuamente aprimorado;
- Devem ser realizadas análises pós-incidente e revisões periódicas;
- A organização deve manter plano de resposta a incidentes atualizado;
- Devem ser realizados testes periódicos do processo de resposta a incidentes;
- O processo de gestão de incidentes deve estar integrado à gestão de riscos e à melhoria contínua;

CONTINUIDADE DE NEGÓCIOS

A organização deve assegurar a continuidade de seus processos críticos de negócio, por meio do estabelecimento de diretrizes que garantam a resiliência organizacional e a manutenção ou recuperação das operações em níveis aceitáveis, diante de situações de interrupção.

Diretrizes

- A continuidade de negócios deve ser estruturada por meio de normas e procedimentos específicos, alinhados à estratégia da organização;
- Devem ser identificados os processos críticos e os recursos necessários para sua continuidade;
- Devem ser estabelecidas estratégias para garantir a continuidade ou recuperação das operações em situações de interrupção;
- Devem ser definidos e mantidos planos de continuidade de negócios, contemplando responsabilidades, priorização e estratégias de recuperação;
- A organização deve assegurar que os planos de continuidade sejam testados e avaliados periodicamente;
- Os planos devem ser revisados e atualizados sempre que houver mudanças relevantes no ambiente, nos processos ou na infraestrutura;
- Devem ser estabelecidos fluxos de comunicação para situações de indisponibilidade ou crise, considerando as partes interessadas internas e externas;
- A continuidade de negócios deve estar integrada à gestão de riscos;
- A organização deve promover a melhoria contínua dos processos de continuidade com base em testes, eventos e avaliações realizadas.

MONITORAMENTO, AUDITORIA E MELHORIA CONTÍNUA

A organização deve estabelecer e manter processos de monitoramento, auditoria e melhoria contínua do Sistema de Gestão de Segurança da Informação e Privacidade, visando assegurar a eficácia dos controles implementados e a conformidade com esta Política, normas internas e requisitos legais e regulatórios.

Devem ser observadas as seguintes diretrizes:

- Devem ser realizados monitoramentos e avaliações periódicas dos controles de segurança da informação e privacidade;
- Deve ser estabelecido programa de auditoria interna para verificação da conformidade com esta Política e normas relacionadas;
- Os resultados das auditorias devem ser analisados criticamente, visando a identificação de não conformidades e oportunidades de melhoria;
- Devem ser definidas e acompanhadas ações corretivas e de melhoria contínua;
- Informações de auditoria devem ser tratadas de forma controlada e, quando aplicável, classificadas quanto ao seu nível de sensibilidade;
- Ativos de informação e processos organizacionais podem ser submetidos a auditorias, conforme diretrizes institucionais;
- As atividades de monitoramento e auditoria devem observar os requisitos de proteção e privacidade de dados;
- Os critérios, procedimentos e responsabilidades devem ser definidos em normas ou processos específicos.

GESTÃO DE PRIVACIDADE DA INFORMAÇÃO (SGPI)

A Unimed Oeste do Paraná deve estabelecer, implementar e manter um Sistema de Gestão de Privacidade da Informação (SGPI), com o objetivo de assegurar a proteção de dados pessoais, a conformidade com a legislação vigente, especialmente a Lei nº 13.709/2018 (LGPD), e a adoção de boas práticas de governança em privacidade.

O SGPI deve ser integrado ao Sistema de Gestão de Segurança da Informação (SGSI), considerando a proteção dos dados pessoais ao longo de todo o seu ciclo de vida.

Devem ser observadas as seguintes diretrizes:

- O tratamento de dados pessoais deve observar os princípios estabelecidos na LGPD, incluindo finalidade, adequação, necessidade, transparência, segurança, prevenção e responsabilização;
- Devem ser implementadas práticas de governança em privacidade, conforme previsto no Art. 50 da LGPD, incluindo mecanismos de supervisão, mitigação de riscos, monitoramento e prestação de contas;
- O tratamento de dados pessoais deve ocorrer apenas para finalidades legítimas, específicas e informadas ao titular, sendo vedado o uso para finalidades incompatíveis;
- O tratamento de dados pessoais deve ocorrer observando as bases legais aplicáveis ao tratamento, conforme legislação vigente;
- Devem ser adotadas medidas técnicas e administrativas aptas a proteger os dados pessoais contra acessos não autorizados, perdas, vazamentos ou qualquer forma de tratamento inadequado ou ilícito;

- O SGPI deve contemplar a gestão estruturada dos processos relacionados à privacidade, incluindo:
  - » Gestão de inventário e mapeamento de dados pessoais (ROPA);
  - » Gestão de riscos em proteção e privacidade de dados;
  - » Gestão de contratos e terceiros que realizem tratamento de dados;
  - » Gestão de avaliações de impacto à proteção de dados pessoais (RIPD), quando aplicável;
  - » Gestão de consentimento e bases legais de tratamento;
  - » Gestão de retenção e descarte de dados pessoais;
  - » Gestão de direitos dos titulares;
  - » Gestão de incidentes de segurança da informação e privacidade;
  - » Gestão de acessos a dados pessoais.
- A proteção de dados pessoais deve ser considerada desde a concepção de novos projetos, sistemas e processos (*privacy by design e by default*);
- Os processos de privacidade devem estar formalizados em normas, procedimentos e guias específicos, devidamente aprovados e mantidos atualizados;
- O SGPI deve ser continuamente monitorado, avaliado e aprimorado, visando garantir sua eficácia e aderência aos requisitos legais, regulatórios e normativos;
- A organização deve ser capaz de demonstrar, a qualquer tempo, a adoção de medidas eficazes para assegurar a conformidade com a legislação de proteção de dados pessoais.

GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE

A gestão de riscos deve ser realizada de forma contínua, estruturada e integrada, considerando os riscos relacionados à segurança da informação e à privacidade de dados pessoais, em conformidade com as diretrizes da ABNT NBR ISO/IEC 27001, ISO/IEC 27701 e legislação aplicável.

Devem ser observadas as seguintes diretrizes:

Categoria	Diretriz
Estrutura e abordagem	A gestão de riscos deve seguir metodologia formal, definida em norma ou guia específico, contemplando identificação, análise, avaliação, tratamento, aceitação, comunicação e monitoramento de riscos.
	Devem ser considerados riscos à confidencialidade, integridade, disponibilidade das informações e aos direitos e liberdades dos titulares de dados pessoais.
	A gestão de riscos deve estar integrada aos processos organizacionais, incluindo projetos, operações, contratos e iniciativas que envolvam tratamento de dados pessoais.
Critérios e avaliação de riscos	Devem ser estabelecidos critérios formais para avaliação de riscos, incluindo probabilidade, impacto e níveis de risco aceitáveis.
	A avaliação deve considerar, quando aplicável, volume e sensibilidade dos dados tratados.
	A avaliação deve considerar, quando aplicável, impacto aos titulares de dados.
	A avaliação deve considerar, quando aplicável, requisitos legais, regulatórios e contratuais.
	Devem ser identificados riscos inerentes e riscos residuais após aplicação de controles.
Tratamento de riscos	Devem ser definidos e implementados controles adequados para tratamento dos riscos identificados.
	O tratamento de riscos deve considerar mitigação, eliminação, transferência ou aceitação do risco.
	Os controles adotados devem considerar, quando aplicável, os controles do Anexo A da ABNT NBR ISO/IEC 27001.
	Riscos que envolvam dados pessoais devem considerar medidas específicas de proteção à privacidade.
	Quando aplicável, deve ser realizada a elaboração de Relatório de Impacto à Proteção de Dados (RIPD).

Aceitação de riscos	Devem ser definidos critérios formais para aceitação de riscos.
	Devem ser definidos níveis de alçada e responsabilidades para aprovação de riscos.
	Riscos não tratados ou residuais devem ser formalmente aceitos pelos responsáveis competentes.
Monitoramento e revisão	Os riscos devem ser monitorados continuamente.
	Os riscos devem ser revisados periodicamente.
	Os riscos devem ser revisados sempre que houver mudanças relevantes em processos, sistemas ou tecnologias.
	Os riscos devem ser revisados em caso de incidentes de segurança ou privacidade.
	A eficácia dos controles implementados deve ser avaliada regularmente.
Integração com segurança e privacidade	A gestão de riscos deve estar integrada à gestão de incidentes de segurança da informação e privacidade.
	A gestão de riscos deve estar integrada à continuidade de negócios.
	A gestão de riscos deve estar integrada à gestão de fornecedores e terceiros.
	Riscos relacionados ao tratamento de dados pessoais devem observar os princípios da LGPD.
Papéis e responsabilidades	Devem ser definidos papéis e responsabilidades para execução da gestão de riscos.
	Devem ser definidos papéis e responsabilidades para acompanhamento da gestão de riscos.
	Devem ser definidos papéis e responsabilidades para aprovação dos riscos.
	Os gestores são responsáveis pela identificação e tratamento dos riscos de seus processos.
	A área de proteção e privacidade de dados deve atuar na avaliação de riscos relacionados a dados pessoais.
Normatização complementar	Os critérios, metodologias, ferramentas e procedimentos detalhados devem ser definidos em norma ou guia específico.

A organização deve manter uma Declaração de Aplicabilidade (Statement of Applicability – SoA), contendo os controles de segurança da informação adotados, sua aplicabilidade e justificativa, conforme os requisitos da ABNT NBR ISO/IEC 27001;

DIRETRIZES PARA USO ACEITÁVEL E COMPORTAMENTO DO USUÁRIO

O uso dos ativos de informação da Unimed Oeste do Paraná deve ser realizado de forma segura, responsável e em conformidade com esta Política, com as normas internas e com a legislação vigente, especialmente no que se refere à segurança da informação e à privacidade de dados pessoais.

Devem ser observadas as seguintes diretrizes:

Mesa Limpa e Tela Limpa

- Devem ser adotadas práticas de mesa limpa e tela limpa, visando reduzir a exposição indevida de informações em ambientes físicos e digitais;
- Informações devem ser protegidas contra acesso não autorizado quando não estiverem em uso;
- A organização deve promover ações periódicas de conscientização sobre práticas seguras de manuseio de informações;
- Os critérios e procedimentos detalhados devem ser definidos em norma específica.

Uso da Internet e Redes Sociais

- O uso da internet deve estar alinhado às atividades profissionais e às diretrizes institucionais;
- O uso de redes sociais deve observar princípios de ética, responsabilidade e não comprometer a imagem, reputação ou segurança da informação da cooperativa;
- Os critérios, restrições e controles técnicos devem ser definidos em norma específica.

Conscientização em Segurança da Informação e Privacidade

- A organização deve estabelecer e manter um programa contínuo de conscientização em segurança da informação e privacidade;
- O programa deve promover a cultura de proteção e privacidade de dados, considerando riscos e responsabilidades dos usuários;
- As ações devem ser realizadas de forma periódica e compatíveis com o nível de risco identificado;
- A participação dos colaboradores e demais partes aplicáveis devem ser asseguradas;

Uso do Correio Eletrônico e Ferramentas de Colaboração

- O uso do correio eletrônico e das ferramentas de colaboração deve estar alinhado às finalidades institucionais;
- O compartilhamento de informações deve observar a classificação da informação e os princípios de necessidade e minimização;

- Devem ser utilizadas, ferramentas corporativas aprovadas;
- Os critérios de uso, controle e segurança devem ser definidos em norma específica.

PENALIDADES / PROCESSO DISCIPLINAR

Nos casos em que houver violação desta Política, das normas de segurança da informação, privacidade ou demais procedimentos institucionais, poderão ser aplicadas sanções administrativas, disciplinares e/ou legais, conforme a gravidade da ocorrência, podendo culminar com o desligamento do infrator e a adoção de medidas administrativas, cíveis e judiciais cabíveis.

A aplicação de penalidades deverá observar os princípios da proporcionalidade, razoabilidade e devido processo, garantindo a adequada apuração dos fatos.

VIOLAÇÕES

São consideradas violações à Política, às normas ou aos procedimentos de segurança da informação e privacidade, incluindo, mas não se limitando:

- Quaisquer ações ou situações que possam expor a Unimed Oeste do Paraná ou seus clientes à perda financeira, direta ou indireta, potencial ou real, comprometendo seus ativos de informação, dados pessoais e/ou sua imagem institucional;
- Quaisquer ações ou situações que venham expor titulares de dados a risco relevante, violando os princípios de proteção de dados pessoais previstos na Lei nº 13.709/2018 (LGPD), bem como seus direitos e liberdades fundamentais;
- Acessos não autorizados, ou situações acidentais ou ilícitas que resultem em destruição, perda, alteração, comunicação, vazamento ou difusão indevida de dados ou informações sob responsabilidade da cooperativa;
- Utilização indevida de dados corporativos, bem como divulgação não autorizada de informações, segredos comerciais ou quaisquer informações classificadas, sem a devida autorização do responsável pela informação;
- Uso de dados, informações, equipamentos, softwares, sistemas ou outros recursos tecnológicos para fins ilícitos ou em desacordo com legislações, normas internas, código de conduta ou exigências regulatórias aplicáveis;
- A materialização de riscos identificados no "MANUAL DE RISCOS E CONTROLES RELACIONADOS A SEGURANÇA E PRIVACIDADE NO TRATAMENTO DE DADOS PESSOAIS" sem a devida comunicação, tratamento ou mitigação adequada;
- A omissão na comunicação imediata à área de proteção e privacidade de dados sobre qualquer incidente, violação, suspeita de descumprimento ou fragilidade de segurança da informação, independentemente de dolo ou culpa.

NÃO CONFORMIDADE E AÇÃO CORRETIVA

Todos os responsáveis, quando acionados em decorrência de uma não conformidade, devem:

- Atuar de forma imediata, conforme o plano de resposta a incidentes, para:
  - » Conter, controlar e corrigir a não conformidade;
  - » Tratar os impactos e consequências decorrentes;
- Avaliar a necessidade de ações corretivas para eliminar a causa raiz da não conformidade, prevenindo sua recorrência, por meio de:
  - » Análise crítica da ocorrência;
  - » Identificação da causa raiz;
  - » Avaliação de recorrência ou potencial de ocorrência em outros processos;
- Registrar e manter evidências documentadas da não conformidade, incluindo:
  - » Descrição da ocorrência;
  - » Ações adotadas;
  - » Responsáveis envolvidos;
  - » Resultados obtidos;
- Encaminhar as evidências e registros ao Encarregado de Proteção de Dados (DPO) e/ou área responsável pela governança de segurança da informação;

As ações corretivas devem ser proporcionais à criticidade e aos impactos da não conformidade identificada.

SANÇÕES

A violação desta Política, das normas ou dos procedimentos de segurança da informação e privacidade, bem como a não conformidade com seus requisitos, será considerada falta grave, sujeita à aplicação de medidas disciplinares, conforme normas internas e legislação vigente.

As sanções poderão incluir, sem limitação:

- Suspensão ou restrição de acessos a sistemas, recursos tecnológicos ou informações;
- Advertência verbal ou formal;
- Suspensão disciplinar;
- Aplicação de penalidades cíveis ou administrativas;
- Demissão por justa causa;
- Adoção de medidas judiciais cabíveis.

As penalidades não seguem ordem sequencial obrigatória, podendo ser aplicadas de acordo com a gravidade da infração, reincidência, impacto causado e nível de responsabilidade do envolvido.

ATUALIZAÇÃO E REVISÃO DA POLÍTICA

A Política de Segurança da Informação e Privacidade, bem como os documentos normativos a ela associados, devem ser mantidos atualizados, refletindo de forma contínua o ambiente organizacional, os riscos, as tecnologias utilizadas e os requisitos legais e regulatórios aplicáveis.

Devem ser observadas as seguintes diretrizes:

- A Política e os demais documentos normativos devem ser revisados, no mínimo, a cada dois anos, ou sempre que houver necessidade decorrente de mudanças relevantes;
- A revisão deve considerar, entre outros aspectos:
  - » alterações no ambiente tecnológico;
  - » mudanças organizacionais ou de processos;
  - » novos requisitos legais, regulatórios ou normativos;
  - » ocorrência de incidentes de segurança ou privacidade;
  - » resultados de auditorias e avaliações internas ou externas;
- As revisões devem ser formalmente registradas, mantendo histórico de versões, alterações realizadas e responsáveis;
- As atualizações devem ser submetidas à aprovação das instâncias competentes, conforme a governança estabelecida;
- A organização deve assegurar que as versões vigentes dos documentos estejam disponíveis aos públicos aplicáveis;
- Os documentos desatualizados devem ser devidamente controlados, evitando seu uso indevido;
- A atualização da Política deve estar alinhada ao processo de melhoria contínua do Sistema de Gestão de Segurança da Informação e Privacidade;

DISPOSIÇÕES FINAIS

Esta Política de Segurança da Informação e Privacidade entra em vigor na data de sua aprovação conselho de administração, devendo ser observada por todos os colaboradores, terceiros, parceiros e demais partes que tenham acesso às informações, sistemas ou ativos da Unimed Oeste do Paraná.

O descumprimento das diretrizes estabelecidas nesta Política e nas normas dela derivadas estará sujeito às penalidades previstas nos normativos internos e na legislação vigente.

A presente Política deve ser interpretada em conjunto com as normas, procedimentos e demais documentos institucionais relacionados à segurança da informação e à proteção de dados pessoais.

A responsabilidade pela manutenção, revisão e atualização desta Política é da área de Proteção e Privacidade de Dados, em conjunto com as áreas competentes, devendo sua aprovação seguir a governança estabelecida pela organização.

Esta Política deve ser amplamente divulgada aos públicos aplicáveis, de forma a garantir o conhecimento e o cumprimento de suas diretrizes.

Os casos omissos ou situações não previstas nesta Política devem ser analisados pelas áreas responsáveis pela área de proteção e privacidade de dados, podendo ser submetidos à deliberação do Comitê de Governança em Proteção e Privacidade de Dados, quando aplicável.

REFERÊNCIAS LEGAIS E NORMATIVAS

Esta Política de Segurança da Informação e Privacidade está alinhada com a legislação vigente, normas técnicas e boas práticas aplicáveis, não se limitando aos instrumentos abaixo:

- Constituição da República Federativa do Brasil de 1988;
- Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD);
- Emenda Constitucional nº 115, de 10 de fevereiro de 2022 (Proteção de Dados como Direito Fundamental);
- Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet);
- Lei nº 12.737, de 30 de novembro de 2012 (Crimes Informáticos);
- Lei nº 10.406, de 10 de janeiro de 2002 (Código Civil);
- Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal);
- ABNT NBR ISO/IEC 27001 – Sistema de Gestão de Segurança da Informação;
- ABNT NBR ISO/IEC 27002 – Código de práticas para controles de segurança da informação;
- ABNT NBR ISO/IEC 27701 – Sistema de Gestão de Privacidade da Informação.

2ª versão | Aprovada pelo conselho em 16/04/2026

Unimed
Oeste do Paraná

somos coop

ANS - nº 305227

www.unimedmedianeira.coop.br

@unimedoestepr