Política de Segurança da Informação

Equipe Revisora

Alexandre Neinas - Coordenador Administrativo

Cleonir Debarba – Coordenador Mercado

Jonathas Bertoldi – Coordenador Promoção e Assistência à Saúde

Narcizo Bodanese - Gerente Geral

Responsável pela aprovação

Diretoria Executiva e **Conselho de Administração**

Assinado por:
Marco Aurelio Farinazzo
4D8C84854BEE4A6...
Dr. Marco Aurélio Farinazzo

Diretor Presidente

DocuSigned by:
DD7283EF791F4DE...
Dr. Rodrigo Otavio G. França

Diretor Vice Presidente

Assinado por:
Henrique Bertassoni Alves
9FC4301CECE548C...
Dr. Henrique Bertassoni Alves

Diretor Superintendente

Histórico de Versões

Data	Versão	Descrição	Autor
18/03/2024	1.0	Primeira versão da política de segurança da informação	Fábio Borin

DocuSigned by:
FABIO BORIN
D419DBC91E50405...

Fabio Borin

DPO

Sumário

Equipe Revisora 2

Diretoria Executiva ..... **Erro! Indicador não definido.**

Histórico de Versões 3

Apresentação 8

2 - Objetivo 9

3 - Abrangência e divulgação 9

4 - Conceitos e definições 10

5 - Estrutura Normativa da Segurança da Informação 13

5.1 Normas Básicas: 13

5.2 Normas Adicionais: 14

6 - Declaração de Comprometimento da Direção 14

7 Responsabilidades Mínimas pela Segurança da Informação 14

7.1 Supervisores (comitê) 14

7.2 Proteção e privacidade (DPO) 16

7.2.1 Gestão operacional 17

7.2.2 Gestão operacional Lei geral de proteção de dados – LGPD 18

7.3 Diretoria Executiva 19

7.4 Gestão de Negócios – Setor comercial 19

7.5 Gestão de Recursos Humanos/Controladoria 19

7.6 Gestão de recursos Financeiros 20

7.7 Gestão de Tecnologia da informação 21

7.8 Usuários Internos e Externos 22

7.9 Proprietário da Informação 24

8 - DIRETRIZES 24

8.1 Gestão de ativos 24

8.1.1 Responsabilidade pelos ativos 24

8.1.2 Classificação da informação 25

8.1.2.1 Reclassificação da informação 27
8.1.2.2 Armazenamento da informação 27
8.1.2.3 Descarte da informação e mídias 27
8.1.3 Leis Aplicáveis na Gestão de Ativos 27
8.1.4 Política de Backup 27
8.2 Segurança em Recursos Humanos 28
8.2.1 Antes da Contratação 28
8.2.2 Durante a Contratação 28
8.2.3 Encerramento e Mudança na Contratação 29
8.2.4 Termo de Confidencialidade e Sigilo 29
8.3 Controle de Acesso Lógico 29
8.3.1 Acesso à Rede, Sistema Operacional e Aplicações 29
8.3.2 Uso de Dispositivos Móveis 30
8.3.3 Trabalho Remoto 31
8.3.4 Política de *Logging* 31
8.4 Criptografia 31
8.4.1 Gestão de Chaves Criptográficas 31
8.5 Segurança Física e do Ambiente 32
8.5.1 Visitantes 32
8.5.2 Infraestrutura 32
8.6 Comunicação Segura 32
A organização deve determinar as comunicações internas e externas relevantes para o sistema de gestão de segurança da informação incluindo: 32
8.6.1 Rede e recursos de rede seguros 32
8.6.2 Transferência de Informações 33
8.7 Sistemas de informação 33
8.8 Fornecedores e terceirizados 34
8.8.1 Termo de Sigilo do Fornecedor 34

8.8.2 Segurança na contratação 34
8.8.3 *Cloud Computing* (Computação na Nuvem) 35
8.8.4 Gerenciamento de Serviços Terceirizados 35
8.8.5 Gestão de mudanças 36
8.8.6 Gestão de Incidentes de Segurança da Informação 36
8.9 Sistema de Gestão privacidade da informação (SGPI) 36
8.10 Orientações ao Usuário Final 38
8.10.1 Uso Aceitável dos Ativos 38
8.10.2 Mesa Limpa e Tela Limpa 38
8.10.3 Transferência de Informações 38
8.10.4 Acesso à Internet e a Redes Sociais 38
8.10.5 Conscientização de Segurança da Informação 39
8.10.6 Acesso ao Correio eletrônico e a Ferramentas de Colaboração 39
8.10.7 Proteção contra Códigos Maliciosos 40
8.11 Gestão de riscos 40
8.11.1 Definição de critérios de riscos 40
8.11.2 Análise, Avaliação e Tratamento de Riscos 40
8.11.4 Gestão de Continuidade de Negócios 41
8.12 Monitoramento e Auditoria 41
8.13 Gestão de Indicadores de Segurança 42
9 Penalidades/Processo Disciplinar 42
9.1 Violações 42
9.1.1. Não conformidade e ação corretiva 43
9.2 Sanções 43
10 Atualização 44
11 Aprovação 44
11.1 Política 44
11.2 Normas Técnicas e procedimentos 44

12 Referências Legais 44

Apresentação

As informações são um dos ativos mais valiosos da Unimed do Oeste do Paraná, dessa forma o uso, guarda ou qualquer outro tratamento com elas realizado deve estar amparado por medidas técnicas e administrativas, garantindo a gestão e minimizando a probabilidade de ocorrência de incidentes.

A crescente automatização das informações, deu ênfase a necessidade de proteger todas as categorias de dados contra roubos e danos, para isso as frentes de atuação da **prevenção, detecção e recuperação** deverão prevenir ataques, identificar possíveis ameaças em tempo hábil e eliminar/mitigar os riscos antes que comprometam a infraestrutura.

Os seguintes pontos devem ser atendidos afim de mitigar ou eliminar quaisquer riscos relacionados à segurança da informação:

Confidencialidade: Garantir que os dados sejam acessados somente por pessoas previamente autorizadas.

Integridade: Garantir que os dados sendo tratados não sofrerão nenhuma modificação indevida, acidental ou proposital durante o seu ciclo de vida.

Disponibilidade: Garantir que as pessoas previamente autorizadas (processo esse garantido pela confidencialidade) tenham acesso a informação sempre que necessitarem fazê-lo para um propósito legitimo.

Autenticidade: Garantir a identidade das pessoas envolvidas.

As diretrizes aqui apresentadas foram baseadas nas normas da família ABNT NBR ISO/IEC 27000 e NBR ISO/IEC 27701:2019, essa política servirá como guia para implementar e manter atualizadas as medidas e ações que devem ser aplicadas para que possamos atingir os 4 pontos acima descritos e assim alcançarmos a gestão da segurança da informação.

Através dessa política a Unimed do Oeste do Paraná formaliza acerca do compromisso com a proteção, privacidade, controle e monitoramento de todos os dados e/ou informações com as quais realiza algum dos seguintes tratamentos: coleta, produção, recepção, classificação, utilização,

acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

A adoção de sistemas de gestão e segurança da informação (SGSI) e gestão de privacidade da informação (SGPI) é uma decisão estratégica.

2 - Objetivo

O objetivo desta política de segurança da informação é estabelecer as diretrizes a serem seguidas por todos os públicos envolvidos com a Unimed do Oeste do Paraná no que diz respeito à adoção de normas, regulamentações, procedimentos, legislações e mecanismos relacionados, afim de proteger os dados e informações, os meios pelos quais serão transmitidas e toda a infraestrutura envolvida, construindo assim um alicerce para a proteção e privacidade dos dados e informações. Também especifica os requisitos e fornece as diretrizes para o estabelecimento, implementação, manutenção e melhoria contínua de um Sistema de Gestão de Privacidade da Informação (SGPI) na forma de uma extensão das normas da família ABNT NBR ISO/IEC 27000 para a gestão da privacidade.

Quando mencionando “segurança da informação” o termo deve ser estendido para a proteção de privacidade, caso esta seja potencialmente afetada pelo tratamento de dados pessoais. Na prática, onde tivermos “segurança da informação”, iremos considerar “segurança da informação e proteção da privacidade” (ABNT NBR ISO/IEC 27701).

3 - Abrangência e divulgação

Afim de definir os limites e a aplicabilidade desse SGSI e SGPI, fica definido que essa política será aplica aos seguintes grupos:

1 – Interno:

- Médico cooperado;
- Diretoria e conselhos;

- Gerência;
- Recursos próprios;
- Colaboradores.

2 – Externo:

- Prestadores de serviços ou parceiros de negócio;
- Profissionais e serviços terceirizados;
- Visitantes;
- Clientes/Beneficiários.

4 - Conceitos e definições

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.

5 - 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:

5.1 Normas Básicas:

- Acesso à Internet;
- Uso Seguro de Redes Sociais;
- Acesso ao Correio Eletrônico;
- Backup e Recuperação de Dados; “incluir destruição de fitas”
- Gestão de Ativos;
- Proteção de Código Maliciosos;
- Segurança física;
- Controle e perfis de acesso lógico;
- 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 Derivada LGPD (ND 015 Unimed do Brasil).

5.2 Normas Adicionais:

- Aquisição, Desenvolvimento e Manutenção de Sistemas/Aplicações;
- Gerenciamento de Incidentes;
- Gerenciamento de Riscos;
- Gerenciamento de Continuidade de Negócios;
- Gerenciamento de Mudanças;
- Gerenciamento do tempo de retenção dos dados pessoais (Tabela de temporalidade);
- Mapeamento de dados pessoais;
- Intercâmbio de Informações;
- Aquisição ou utilização de novos softwares ou aplicativos que não estejam na lista de ativos;
- Segurança em Terceirização e Prestação de Serviços; e
- Uso da Computação em Nuvem.

6 - Declaração de Comprometimento da Direção

Tendo ciência da importância da conscientização e da aplicação dessa política de segurança da informação a diretoria da Unimed do Oeste do Paraná assegura que todo o SGSI+SGPI é compatível com a direção estratégica da cooperativa, disponibilizando os recursos necessários afim de promover a melhoria contínua e dessa forma, documenta e torna pública para toda a cooperativa o seu comprometimento e empenho através dos canais de comunicação oficiais.

7 Responsabilidades Mínimas pela Segurança da Informação

7.1 Comitê gestor de segurança da informação - CGSI

Um grupo de supervisores/colaboradores deve ajudar a definir e apoiar as estratégias necessárias à implantação e manutenção do SGSI e SGPI.

Dentre as funções principais destacamos:

1. Propor ajustes, aprimoramentos e modificações na estrutura normativa do SGSI, submetendo à aprovação da Diretoria;
2. Redigir o texto das normas e procedimentos de Segurança da Informação, submetendo à aprovação da Diretoria;
3. Requisitar informações das demais áreas, através da diretoria, gerências, coordenações, e supervisões, com o intuito de verificar o cumprimento da Política, das Normas e Procedimentos de Segurança da Informação;
4. Receber, documentar e analisar casos de violação da Política e das Normas e Procedimentos de Segurança da Informação sempre que convocados;
5. Estabelecer mecanismos de registro e controle de eventos e incidentes de Segurança da Informação, bem como, de não conformidades com a Política, as Normas ou os Procedimentos de Segurança da Informação;
6. Notificar o encarregado pela privacidade dos dados quanto ocorrer casos de violação da Política e das Normas e Procedimentos de Segurança da Informação;
7. Receber sugestões dos gestores da informação para implantação de Normas e Procedimentos de Segurança da Informação;
8. Propor projetos e iniciativas relacionadas à melhoria da segurança da informação;
9. Acompanhar o andamento dos projetos e iniciativas relacionados à segurança da informação;
10. Monitorar sistematicamente, a gestão dos ativos da informação;
11. Tomar as devidas providências junto aos supervisores e seus subordinados quando ocorrerem não conformidades;
12. Cumprir e fazer cumprir esta Política, as Normas e os Procedimentos de Segurança da Informação;
13. Conhecer os procedimentos de segurança em vigência;
14. Garantir a segurança e a proteção da confidencialidade da informação clínica e de todos os dados pessoais dos beneficiários da Unimed do Oeste do Paraná que possam causar riscos ou danos, inclusive morais aos mesmos;
15. Orientar a atualização dos Planos de Continuidade dos Negócios, demandando junto às diversas áreas da empresa e validando-os em intervalos definidos; e

16. Orientar e organizar sistematicamente, a gestão de riscos relacionados à segurança da informação.

7.2 Proteção e privacidade (DPO)

Cabe a área de proteção e privacidade executar os seguintes controles e medidas sempre que relacionados a **infraestrutura de modo geral**, inclusive para a área de tecnologia da informação, com o intuito de implementar diretrizes da segurança da informação no âmbito da Unimed do Oeste do Paraná;

1. Planejar, coordenar e/ou executar políticas de segurança de controles de acesso lógico baseados na segregação de funções e no princípio do menor privilégio;
2. Interagir com outros setores da empresa de modo a fomentar a segurança da informação e auxiliar em todas as tarefas relacionadas à segurança, proteção e privacidade dos dados/informações;
3. Notificar incidentes de segurança da informação, as partes interessadas e a Autoridade nacional de proteção de dados quando o incidente envolver dados pessoais e/ou causar danos relevantes aos titulares de dados;
4. Indicar treinamentos relativos à segurança da informação e privacidade de dados;
5. Identificar, avaliar e tratar os riscos inerentes às atividades que envolvam tratamentos de riscos;
6. Tratar a ocorrência de não conformidades;
7. Estruturar e manter os controles internos da área de segurança da informação;
8. Providenciar a segregação de ambientes distintos físicos e lógicos, impedindo acessos indevidos de pessoas não habilitadas, garantindo a integridade de instalações e equipamentos;
9. Recomendar a equipe de desenvolvimento de sistemas um processo de melhores práticas e desenvolvimento seguro;
10. Planejar, coordenar e/ou executar o desenvolvimento dessa política de segurança da informação;
11. Planejar, coordenar e/ou executar o desenvolvimento da política de resposta a incidentes;

12. Planejar e aplicar um framework de configurações de segurança, tais como, mas não se limitando ao CIS, NIST; e
13. Planejar, coordenar e/ou executar outras atividades correlatas ou quando determinado pela Gerência e/ou diretoria.

7.2.1 Gestão operacional

Cabe a área de proteção e privacidade executar os seguintes controles e medidas:

1. Gerenciar a plataforma de prevenção, detecção e reação a incidentes de segurança;
2. Tratar incidentes lógicos de segurança da informação e manter um plano de resposta a incidentes;
3. Avaliar vulnerabilidades e implementar as correções cabíveis;
4. Implementar mecanismos de proteção (segurança lógica) nas plataformas tecnológicas (Banco de Dados, Sistema Operacional, Rede, armazenamento, etc.) sob a sua responsabilidade;
5. Planejar, coordenar e/ou executar os serviços de proteção (Antivírus, backup, firewall, dentre outros);
6. Implantar mecanismos de segurança lógica e física;
7. Implementar ferramentas para permitir gerenciamento e administração da segurança de rede;
8. Identificar, analisar e gerenciar fluxos de tráfego de rede;
9. Analisar o desempenho e capacidade de redes;
10. Verificar periodicamente se as instalações de hardware e software estão em conformidade às aquisições, podendo:
    - Auditar os equipamentos para verificação da existência de software não homologado pela empresa, bem como aqueles de natureza ilegal;
    - Auditar todos os equipamentos de rede para verificação de vulnerabilidades ou brechas de segurança;

- Observar a utilização de código de acesso, por usuário que não seja o proprietário do mesmo;
- Verificar se os recursos de hardware, equipamentos e periféricos, estão instalados e utilizados em conformidade com padrões da Cooperativa;
- Instalar e manter em condições de uso os recursos de informática disponíveis e homologados pela Cooperativa;
- Testar e indicar ferramentas/aplicativos disponíveis no mercado;
- Avaliar as necessidades das áreas referentes aos recursos tecnológicos

7.2.2 Gestão operacional Lei geral de proteção de dados – LGPD

1. Realizar a gestão e auxiliar no programa de adequação lei geral de proteção de dados – LGPD;
2. Planejar, coordenar e/ou executar o desenvolvimento do Sistema de Gestão da privacidade da informação;
3. Planejar, coordenar e/ou executar o desenvolvimento de guias para conscientização da LGPD;
4. Planejar, coordenar e/ou executar o desenvolvimento de guias/normas a serem seguidas pelos gestores durante adequação a LGPD;
5. Auxiliar os responsáveis a planejar, coordenar e/ou executar adequações a LGPD sempre que um novo processo/fluxo de dados for desenhado pela cooperativa;
6. Planejar, coordenar e/ou executar a implantação de indicadores que auxiliem a gerencia e diretoria na tomada de decisão, para todos os que processos envolvam dados pessoais;
7. Fiscalizar o cumprimento dessa política e as normas dela derivadas;
8. Planejar, coordenar e/ou executar quaisquer atribuições ao cargo atreladas pela autoridade nacional de proteção de dados.

7.3 Diretoria Executiva e gerência

Cabe à Diretoria Executiva:

1. Nomear o Representante da Direção para a Proteção de Dados (*DPO – Data Protection Officer*, ou Encarregado de Dados);
2. Aprovar a Política e as Normas de Segurança da Informação e suas revisões;
3. Aprovar a composição de comitê gestor da segurança da informação (CGSI);
4. Nomear os gestores da informação, conforme as indicações do CGSI; e
5. 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.

7.4 Gestão de Negócios – Setor comercial

Cabe:

1. Fornecer as diretrizes estratégicas do negócio para orientar as atividades de proteção e privacidade referentes a contratos com clientes/beneficiários;
2. Garantir a inclusão de cláusulas contratuais com requisitos relacionados à proteção e privacidade dos dados;
3. Reportar a ocorrência de incidentes e não conformidades de Segurança da Informação à área de proteção e privacidade dos Clientes/Empresas contratantes de planos de saúde; e
4. Garantir que todos os tratamentos de dados executados estejam adequados a lei geral de proteção de dados.

7.5 Gestão de pessoas

Cabe:

1. 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;
2. Em caso de demissões registrar através do software de *helpdesk* a solicitação de bloqueio imediato ou transferência do login para seu gestor;

3. Divulgar aos novos colaboradores a existência da Política de Segurança da Informação e a maneira de acessá-la;
4. Reforçar a importância de seguir a Política de Segurança da Informação;
5. Providenciar a assinatura do Termo de Sigilo ou NDA, Responsabilidade e confidencialidade;
6. Garantir a coleta/atualização do termo de consentimento junto aos colaboradores;
7. Indicar necessidade de capacitação em segurança, proteção e privacidade para os novos colaboradores e/ou seguir orientações do encarregado pela proteção e privacidade dados;
8. Incluir na entrevista de desligamento a importância da manutenção do sigilo das informações para as quais possuía acesso;
9. Reportar a ocorrência de incidentes e não conformidades de Segurança da Informação que envolvam os colaboradores;
10. Em caso de infração e não cumprimento da política de segurança da informação:
    - Registrar e formalizar, perante os responsáveis, as não conformidades de segurança, visando medidas disciplinares
11. Garantir que todos os tratamentos de dados executados estejam adequados a lei geral de proteção de dados.

7.6 Gestão de recursos Financeiros

Cabe:

1. Fornecer as diretrizes estratégicas e operacionais para as atividades de Segurança da Informação relacionadas ao uso correto em transações bancárias.
2. Implantar e monitorar mecanismos contra fraudes financeiras.
3. Avaliar e selecionar parceiros de negócios que possuam infraestrutura compatível com os padrões de segurança da informação, como criptografia, controle de acesso, gerenciamento de riscos, levando em consideração no mínimo os seguintes pontos:
    a. O controle, classificação e compartilhamento de informações privadas e/ou pessoais;
    b. A regulamentação do uso de tecnologias e serviços em nuvem, incluindo provedores internacionais;

c. A necessidade de um plano de resposta ágil transparente e que informe sobre incidentes que possam prejudicar a segurança dos dados;
d. A responsabilidade por eventuais vazamentos de informação;
e. Aplicação do questionário "Análise de Privacidade de Terceiros" disponibilizado pelo encarregado pela proteção de dados para sanar os pontos acima descritos, bem como todos os pontos considerados relevantes antes da contratação.

4. Informar e capacitar os colaboradores da área no uso das ferramentas relacionadas a movimentações bancárias, mantendo a segregação dos acessos por perfis e seguindo a política do menor privilégio;
5. Garantir que todos os tratamentos de dados executados estejam adequados a lei geral de proteção de dados.

7.7 Gestão de Tecnologia da informação

Cabe a área de Tecnologia da informação executar os seguintes controles e medidas sempre que relacionados aos softwares/ativos listados no inventário de softwares:

1. Gerenciar a plataforma de prevenção, detecção e reação a incidentes de segurança relacionados aos sistemas de gestão sob sua responsabilidade;
2. Tratar e/ou auxiliar em incidentes lógicos de segurança da informação que envolvam os sistemas de gestão/portais sob sua responsabilidade;
3. Receber, avaliar e corrigir vulnerabilidades reportadas, seja internamente ou através de equipes de suporte externas;
4. Implementar mecanismos de proteção (segurança lógica: perfis de acesso, política de senhas, criptografia, métodos de conexão a banco de dados, senhas de administração, uso seguro, dentre outros) nos sistemas sob sua responsabilidade conforme orientação e/ou buscar a adequação dos sistemas de acordo com as normas da cooperativa;
5. Planejar, coordenar e monitorar logs das ações executadas em sistemas sob sua responsabilidade de forma preditiva, identificando ações que possam ser a causa/fonte de risco de incidentes de segurança;

6. Planejar, coordenar e/ou executar a implementação de medidas de segurança nos códigos fonte dos sistemas desenvolvidos, considerando os princípios do *"Privacy by design"* e o *"Privacy by default"*;
7. Auditar e garantir a implantação de medidas de segurança no processo de desenvolvimento e uso de relatórios e painéis de *Business Intelligence* – BI;
8. Gerenciar serviços de alta disponibilidade para condicionadores de ar e fornecimento de energia para as salas de datacenters e microinformática.
9. Reportar de imediato à área de proteção e privacidade, quando houver, qualquer incidente de segurança da informação ou suspeitas iminentes;
10. Manter um inventário estruturado dos ativos de software associados a informação e aos recursos de hardware e processamento da informação, bem como, identificar o seu proprietário;
11. Fiscalizar periodicamente o cumprimento de regras de acesso aos recursos existentes nos sistemas;
12. Verificar se os recursos de hardware, equipamentos e periféricos, estão instalados e utilizados em conformidade com essa política e as normas derivadas;
13. Instalar e manter em condições de uso os recursos de informática disponíveis e homologados pela Cooperativa;
14. Treinar e orientar os usuários quanto à utilização dos recursos da rede;
15. Providenciar a instalação e garantir a manutenção da rede física;
16. Avaliar as necessidades das áreas referentes aos recursos tecnológicos seguindo o fluxo para análise de segurança da informação; e
17. Garantir que todos os tratamentos de dados executados estejam adequados a lei geral de proteção de dados.

7.8 Usuários Internos e Externos

Cabe aos colaboradores, estagiários, aprendizes, terceirizados e prestadores de serviços cumprir com as seguintes obrigações:

1. Tomar ciência da Política de Segurança da Informação e assinatura do Termo de Sigilo e Responsabilidade e cumpri-la;
2. Não divulgar suas credenciais de acessos;
3. Não instalar em hipótese alguma, qualquer software sem o parecer e/ou acompanhamento da Área de TI, nem mesmo executar programas portáteis (*MS Office, TeamViewer, Anydesk,* etc);
4. Desligar seu equipamento ao fim da jornada de trabalho;
5. Não executar *softwares* de acesso remoto sem autorização, tais como, mas não se limitando a, *teamviewer*, *anydesk*, google *remote desktop*;
6. Respeitar e preservar o grau de confidencialidade da informação, divulgando-a exclusivamente para as pessoas autorizadas a terem esse conhecimento;
7. Garantir a segurança e a proteção da confidencialidade da informação clínica e de todos os dados pessoais dos beneficiários da Unimed do Oeste do Paraná que possam causar riscos ou danos, inclusive morais aos mesmos;
8. Zelar continuamente pela proteção das informações em poder da Unimed do Oeste do Paraná ou de seus clientes, contra acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;
9. Sempre que convocados participar e seguir as orientações recebidas através de palestras, seminários e/ou treinamentos promovidos pela Unimed do Oeste do Paraná;
10. Assegurar que os recursos (computacionais ou não computacionais) colocados à sua disposição sejam utilizados apenas para as finalidades estatutárias da organização;
11. Garantir que os sistemas e informações sob sua responsabilidade estejam adequadamente protegidos;
12. Garantir a continuidade do processamento das informações críticas para os negócios;
13. Cumprir as leis e normas que regulamentam os aspectos de propriedade intelectual;
14. Atender às leis e resoluções normativas que regulamentam as atividades da Unimed do Oeste do Paraná e seu mercado de atuação;
15. Selecionar de maneira coerente os mecanismos de segurança da informação, balanceando fatores de risco, tecnologia e custo;

16. Comunicar imediatamente ao encarregado pela proteção e privacidade de dados qualquer descumprimento da Política de Segurança da Informação e/ou das Normas de Segurança da Informação; e
17. Garantir que todos os tratamentos de dados executados estejam adequados a lei geral de proteção de dados.

7.9 Proprietário da Informação

Cabe ao proprietário/responsável pela informação:

1. Determinar o nível de relevância e classificação correta das informações utilizadas nos ativos sob sua responsabilidade, de forma a subsidiar as decisões de classificação a serem aplicadas;
2. Garantir que todos os dados e informações sob sua responsabilidade respeitem as diretrizes dessa política e/ou normas derivadas;
3. Garantir que todos os tratamentos de dados executados estejam adequados a lei geral de proteção de dados; e
4. Comunicar imediatamente ao encarregado pela proteção e privacidade de dados qualquer descumprimento da Política de Segurança da Informação e/ou das Normas de Segurança da Informação.

8 - DIRETRIZES

8.1 Gestão de ativos

8.1.1 Responsabilidade pelos ativos

Deve ser determinada a competência necessária para as pessoas que realizam trabalhos em nome da cooperativa e que afetam o desempenho da segurança da informação. Devem ser executadas, quando aplicáveis, ações que visam capacitar e dar competência as pessoas.

Deve ser definido um proprietário e as responsabilidades para proteção dos ativos de informação, sendo por via de regra definido que cada supervisor ficará nomeado como proprietário das informações relacionados ao seu setor, tendo que gerenciá-la durante todo o ciclo de vida da

mesma, desde a criação, processamento, movimentação, compartilhamento, armazenamento até o descarte, seguindo as normas e diretrizes aqui definidas.

OBS: Os ativos da informação pertinentes aos setores são mapeados/atualizados sempre que houver mudanças ou a cada 12 meses e entregue por cada um dos supervisores ao DPO para que dentre outras tarefas a serem executadas a *política de privacidade* possa ser atualizada e publicada.

O proprietário deverá fazer cumprir com todas as regras impostas pela política de segurança da informação dentro dos limites a ele definidos, podendo inclusive delegar tarefas de segurança da informação a outro colaborador quando sob sua coordenação ou supervisão, reportar a área de proteção e privacidade sempre que incidentes ou conduta impropria seja detectada, ficando sob pena de ser responsabilizado pelas ações ilícitas em caso de imprudência, imperícia ou negligência, mesmo não sendo o responsável direto pela execução da ação que causou o dano/incidente.

ISO 27002, item 6.1.1 *"Convém que as pessoas indicadas sejam competentes e capazes de cumprir com as responsabilidades pela segurança da informação e a elas seja dada a oportunidade de manter-se atualizada com os desenvolvimentos."*

8.1.2 Classificação da informação

Toda informação tratada pela Unimed no papel de controladora, será classificada, devendo o proprietário/responsável pelo dado/informação executar essa ação seguindo as definições aqui descritas.

As classificações especificas para "dados pessoais" de acordo com a LGPD:

1. **Dado Pessoal**

   Informação relacionada a pessoa natural identificada ou identificável;

2. **Dado Pessoal Sensível**

   Já previamente determinado pela lei geral de proteção de dados e que compõe os seguintes grupos, quando vinculado a uma pessoa natural:

   i. Dado pessoal sobre origem racial ou étnica,

ii. Convicção religiosa,

iii. Opinião política,

iv. Filiação a sindicato ou a organização de caráter religioso, filosófico ou político,

v. Dado referente à saúde ou à vida sexual,

vi. Dado genético ou biométrico,

3. **Anomizado**

Dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;

4. **Pseudonimizado**

A pseudonimização é o tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro.

Além do que impõe a LGPD podemos ter o dado/informação classificada em:

1. **Confidencial**
    a. Dado/Informação que deve ser mantida somente sob o conhecimento da alta gestão e conselhos e/ou representam segredos comerciais mantidos pela cooperativa; O acesso não autorizado a estas informações pode causar danos financeiros, perdas de mercado, danos à imagem da Unimed do Oeste do Paraná ou vazamento não autorizado de informações estratégicas;
    Ex: Analise de viabilidade de novos negócios.
2. **Restrita**
    a. Restrita a um grupo de pessoas previamente determinada com o auxílio da gerência e coordenação; Informações de uso interno da cooperativa, mas que são sensíveis em caso de vazamento. Essas informações não devem sair do âmbito do grupo de pessoas previamente determinadas. Se isto ocorrer, podem causar constrangimento da cooperativa e prejuízos indiretos não desejáveis;

Ex: Registro eletrônico de saúde de beneficiários.

3. **Pública**
    a. Dados/Informação que pode ser divulgada em canais oficiais da cooperativa sem causar prejuízos de qualquer natureza a nenhuma das partes envolvidas;

    Ex: Política de privacidade.

8.1.2.1 Reclassificação da informação

A classificação das informações deve ser reavaliada anualmente pelo CGSI, se houver alteração a informação deverá ser reclassificada, devendo informar as partes interessadas.

8.1.2.2 Armazenamento da informação

- É recomendada a existência de uma tabela de temporalidade informando a expiração de cada documento categorizado;
- Informações sensíveis em meios físicos devem ser armazenadas em local controlado. Ex,: Cofres, armários com chave, salas com registro de acesso.

8.1.2.3 Descarte da informação e mídias

Recomenda-se que informações que perderam sua utilidade ou valor e/ou armazenadas em meios físicos e mídias sejam destruídas de forma que não seja possível recuperá-las e devem ser executadas por meio de procedimentos formais.

8.1.3 Leis Aplicáveis na Gestão de Ativos

Normas e procedimentos adicionais devem ser elaborados para atender aos requisitos legais da Lei de Acesso Informação - (LAI) Lei nº 12.527 de 18 de novembro de 2011, do Marco Civil da Internet - Lei nº 12.965 de 23 de abril 2014 e a Lei Geral de Proteção de Dados Pessoais (LGPD) - Lei nº 13.709 de 14 de agosto de 2018.

8.1.4 Política de Backup

Devem ser estabelecidas regras e procedimentos para as atividades de backup, armazenamento e recuperação de dados. A política de backup deve prever o local e a forma de armazenamento, o tempo de retenção, mecanismos de teste de recuperação dos dados, meios para o descarte seguro das mídias do backup, dentre outros.

Para uma rotina de backup eficiente deve existir um documento formal interno da cooperativa e acordado com as diversas áreas de negócio, contendo as seguintes informações:

- Devem ser definidos quais os dados que serão armazenados em backup (ex.: sistemas, base de dados, arquivos);
- Deve existir a definição dos responsáveis pela administração, execução e controle do backup onde estarão expressos os papéis de cada colaborador/área;
- Deve ser definida a frequência da operação de backup;
- Deve ser definido o tempo de retenção das cópias de segurança;
- Devem ser definidos os equipamentos e as tecnologias que serão utilizados para a realização do backup;
- Deve existir um local seguro para o armazenamento das cópias de segurança;
- Deve existir um processo sistemático de verificação da integridade e execução das cópias de segurança;
- Deve ser definido um processo para recuperação das informações.

8.2 Segurança em gestão de pessoas

8.2.1 Antes da Contratação

Prever no anúncio de vaga e em cláusula contratual, uma seleção criteriosa, especificando a obrigatoriedade da apresentação de cópias de certidões negativas de registros civis, criminais, e assinatura do termo de Sigilo, Responsabilidade e confidencialidade. Realizar avaliação de perfil com a finalidade de detectar incompatibilidades ao cargo proposto e suas atividades. Toda contratação deverá em seus termos de responsabilidade, contemplar a proteção ao dado/conhecimento sensível através de acordos de confidencialidade, inclusive com as prestadoras de serviços, devendo especificar também os direitos e deveres que o contratado terá referente às informações, assim como à segurança destas.

8.2.2 Durante a Contratação

Deverão ser definidos os requisitos de segurança necessários para exercer cargos e funções de natureza sensível na empresa, assim como, o grau de sensibilidade dos cargos e das funções existentes, no intuito de identificar formalmente aqueles que, em razão de suas atribuições, tarefas

e responsabilidades, possam acessar informações de conhecimento sensível ou Confidencial/Restrita. As credenciais de acesso, só deverão ser entregues ao(s) contratado(s) quando todos os documentos que descrevem as responsabilidades forem assinados. Caso a atividade a ser desenvolvida implique a custódia de ativos, estes, assim como as credenciais de acesso, só deverão ser fornecidos após a assinatura de toda documentação pertinente.

8.2.3 Encerramento e Mudança na Contratação

Estes processos deverão contemplar a comunicação com o(s) responsável(is) pelo gerenciamento das credenciais de acesso, objetivando que estas estejam em conformidade com os processos:

1. Normatizar procedimentos de desligamento, de forma a interromper o acesso e a vinculação da empresa ao colaborador desligado, bem como o procedimento de devolução de ativos sob custódia do(s) contratado(s);
2. Realizar a entrevista de desligamento objetivando detectar o grau de satisfação dos colaboradores com a empresa e lembrar a estes da permanência do sigilo de informações as quais tinham acesso durante o vínculo empregatício.

8.2.4 Termo de Confidencialidade e Sigilo ou NDA

O NDA é conhecido como acordo, ou termo de confidencialidade e tem o objetivo de formalizar a não divulgação de qualquer dado/informação que o colaborador venha ter acesso devido ao papel que desempenha ou ao ecossistema de operação da Unimed do Oeste do Paraná, independente do formato em que as informações se encontram, ou seja, texto, áudio, vídeo, imagens, falas e etc.

Todos os colaboradores da empresa devem assinar o Acordo/Termo de Confidencialidade independente da classificação dos dados/informações com as quais possui acesso, o acordo deve ainda ser claro e objetivo, informando suas punições em caso de não cumprimento.

8.3 Controle de Acesso Lógico

8.3.1 Acesso à Rede, Sistema Operacional e Aplicações

O acesso aos recursos computacionais deve ser individual, pessoal e intransferível.

O usuário é responsável pela guarda de sua senha e pelo acesso aos recursos computacionais realizados através da sua credencial de acesso.

O controle de acesso lógico deve ser composto de processos para autenticação, autorização e auditoria.

O acesso lógico à rede deve ser controlado de forma centralizada através de procedimentos formais vinculados a um perfil de usuário, no qual estará definido seu nível de autorização.

Todo serviço de rede não autorizado deve ser bloqueado ou desabilitado.

Todas as transações em rede devem, obrigatoriamente estarem protegidas através de mecanismos de segurança.

O acesso a sistemas e aplicações deve sempre ocorrer através de um procedimento seguro de acesso ao sistema (login), projetado para minimizar oportunidades de acessos não autorizados.

O acesso aos ativos deve estar estritamente vinculado à execução do trabalho do usuário, e deve ser concedido em conformidade ao princípio do privilégio mínimo.

8.3.2 Uso de Dispositivos Móveis

A política de uso de dispositivos móveis na empresa deve ser regulamentada através de normas e procedimento de segurança. Todo dispositivo móvel somente poderá ser utilizado para acessar à rede e/ou recursos computacionais, caso ofereça os requisitos mínimos de segurança, como:

- Ter permissão previamente assinada para uso do equipamento na rede da Unimed a qual deve conter:
    - Motivo do uso do equipamento que explique a impossibilidade de utilização dos equipamentos da cooperativa;
    - Data de início e fim da autorização;
    - Recursos que poderão ser acessados;
    - Local/Setor onde irá utilizar o equipamento;
    - Responsável pela autorização;
    - Dono/Responsável pelo equipamento;

- Autenticação através de usuário e senha
- Comprovação do uso de software antivírus que possua licença ativa, garantindo assim a atualização de vacinas contra códigos maliciosos (Vírus computacionais) ou uso de antivírus que comprovadamente dispense a atualização de vacinas devido ao uso de Inteligência artificial, análise comportamental e/ou outro meio.

8.3.3 Trabalho Remoto

Quando em instalações ou fazendo uso de meios alheios aos disponibilizados pela infraestrutura da Unimed do Oeste do Paraná, deve-se estabelecer norma e procedimento quanto a autorização, gestão, responsabilidades e controle dos acessos efetuados pelos colaboradores, clientes, parceiros externos ou empresa contratada, para uso da rede e seus ativos, sendo assim chamado de trabalho remoto.

8.3.4 Política de *Logging*

Adotar solução de análise e gestão de *LOGs* que permita a geração de relatórios e emissão automática de alertas de eventos que possam representar riscos para a segurança da infraestrutura tecnológica e dos sistemas de informação.

8.4 Criptografia

8.4.1 Gestão de Chaves Criptográficas

Definir um processo formal para proteger chaves criptográficas, contemplando requisitos referentes ao gerenciamento ao longo de todo o seu ciclo de vida incluindo a geração, a armazenagem, o arquivo, a recuperação, a distribuição, a retirada e a destruição das chaves considerando a geração de registro e auditoria das atividades relacionadas com o gerenciamento destas.

8.5 Segurança Física e do Ambiente

8.5.1 Visitantes

O acesso interno ao ambiente administrativo da Unimed deve ser controlado com registro de data e informação que identifique os visitantes, para auxilio caso ocorra algum incidente de segurança da informação/privacidade de dados, servindo como instrumento de auxilio nas investigações.

8.5.2 Infraestrutura

O acesso aos equipamentos internos, como, desktops ou servidores deve ser controlado e disponível somente a pessoas autorizadas, seja com auxílio de chaves, cartões ou credenciais de acesso aos recursos.

Câmeras de monitoramento devem registrar as entradas de pessoas no prédio principal e nas salas cujo recursos precisam ser protegidos de forma especial.

8.6 Comunicação Segura

A organização deve determinar as comunicações internas e externas relevantes para o sistema de gestão de segurança da informação incluindo:

a) O que comunicar;
b) Quando comunicar;
c) Quem comunicar;
d) Quem será comunicado; e
e) O processo pelo qual a comunicação será realizada.

8.6.1 Rede e recursos de rede seguros

É imprescindível a segregação física e lógica de todo trafego de rede, afim manter seguras as informações trocadas levando em consideração:

1. Cada setor deve estar logicamente separado dos demais;
2. A manutenção de ambientes de produção e homologação deve ser mantidos para que erros que possam ocorrer em novas implementações, ferramentas, upgrades, patch possam ser previamente testados e não comprometam a integridade dos dados;

3. Bancos de dados redundantes devem proteger os dados de acessos não autorizados, exceto quando o mesmo assumir a função principal devido a um incidente que tenha comprometido o funcionamento do banco de dados principal;
4. Bancos de dados de homologação devem proteger os dados dos titulares de dados com técnicas de anonimização ou pseudonimização sempre que possível; da mesma forma as restrições de perfis mantidas no banco de produção devem ser replicadas para bancos de dados de homologação.

8.6.2 Transferência de Informações

Devem ser definidas regras para que sempre que a troca de informações se faça necessária com órgão municipais, governamentais ou entidades externas a mesma ocorra de forma segura, técnicas de criptografia devem ser implementadas e automatização de procedimentos por parte de sistemas para evitar o erro humano e o comprometimento do processo, a gestão de logs para todas as transações é imprescindível.

8.7 Sistemas de informação

A contratação ou revisão de sistemas de informação utilizados pela cooperativa deve levar em consideração requisitos relacionados à segurança da informação afim de proteger os dados e processos de negócio.

Devem ser levados em consideração os 7 princípios do *privacy by design*:

1. Ser proativo e não reativo;
2. Privacidade e configuração como padrão;
3. Privacidade incorporada ao design;
4. Funcionalidade completa;
5. Segurança End-to-End – proteção completa no ciclo de vida da informação;
6. Transparência e visibilidade;
7. Respeito pela privacidade.

8.8 Fornecedores e terceirizados

8.8.1 Termo de Sigilo do Fornecedor

Deve ser garantido que a empresa contratada tenha termo/acordo de Confidencialidade coletado junto aos seus colaboradores que estarão diretamente ligados ao processamento dos dados com eles compartilhados. No caso dos prestadores de serviço, o sigilo deve ser também observado em cláusulas contratuais.

8.8.2 Segurança na contratação

Os contratos devem prever os requisitos de segurança pertinentes, regras de conduta internas e externas, responsabilidades das partes durante a execução do contrato e as penalidades aplicáveis em caso de não cumprimento de cláusulas relativas à segurança da informação.

Parcerias devem ser firmadas com assinaturas de contratos onde constam cláusulas especificas sobre à privacidade e à proteção de dados, sendo essas as cláusulas mínimas a serem inseridas:

- Agentes de tratamento: Definição de quem é controlador e operador, juntamente com as responsabilidades e funções de cada agente.
- Medidas de segurança: (Todos os agentes envolvidos devem garantir que adotam medidas técnicas e administrativas aptas a proteger os dados envolvidos de acessos não autorizados e de acidentes;
- Compartilhamento de dados: (Caso haja a necessidade de compartilhamento com terceiros alheios ao contrato, devem existir cláusulas que definam como esse compartilhamento se dará, se será com o consentimento prévio notificação) lembrando que a parte que realizar esse compartilhamento deverá garantir do terceiro os mesmos níveis de maturidade em relação à proteção dos dados e à privacidade dos dados;
- Direitos dos titulares: (Ambas as partes devem adotar meios internos a atender todos os direitos dos titulares de dados (Art. 18 LGPD), podendo esclarecer que nessas situações trabalharão de forma mutua);

- Incidentes: (As partes devem estabelecer os procedimentos a serem implementados em caso de incidente de dados pessoais, com planos de respostas e remediação estruturados);
- Auditoria: (A depender da natureza dos dados envolvidos podemos determinar que auditorias possam ser realizadas afim de determinar que as regas do contrato estão sendo seguidas);
- Penalidades e multas: (Independente das penalidades impostas pela LGPD, podem ser definidas penalidades ou multas a serem aplicadas em caso de descumprimento pelas partes acerca das disposições da proteção de dados definidas em contrato);
- Comunicações: (Para tornar a comunicação facilitada entre as partes deve ser informado no contrato os dados de contato do DPO);
- Retenção e exclusão dos dados: (Exceto casos em que haja a necessidade de retenção dos dados para fins de obrigação legal, findado o contrato deve ser definido o prazo e a forma com que os dados serão excluídos das bases de dados).

O diagnóstico inicial será realizado via questionário “Análise de Privacidade de Terceiros disponibilizado pelo encarregado pela proteção de dados e deve ter sido antes aprovado pela diretoria. Fica a cargo do supervisor da área realizar o envio do questionário para o destinatário correto.

8.8.3 *Cloud Computing* (Computação na Nuvem)

A contratação de serviço em nuvem deve atender aos requisitos da política de segurança da empresa e às normas e legislação brasileira quanto a confidencialidade e propriedade, localização dos dados armazenados, estes não podem sair do território nacional. A empresa contratada deve assegurar que segue os padrões das normas nacionais e internacionais de segurança em computação na nuvem, através de certificações emitidas por estas entidades.

8.8.4 Gerenciamento de Serviços Terceirizados

Estabelecer diretrizes para implementar e manter o nível apropriado de segurança da informação e de entrega de serviços nos acordos firmados entre a empresa e terceiros. Os contratos devem prever os requisitos de segurança pertinentes, regras de conduta internas e externas, responsabilidades das partes durante a execução do contrato, acordo de nível de serviço (SLA), e as

penalidades aplicáveis em caso de não cumprimento de cláusulas relativas à segurança da informação.

8.8.5 Gestão de mudanças

Um processo de gerenciamento de mudanças deve ser estabelecido e implementado a fim de garantir que modificações em recursos de Tecnologia da Informação sejam processadas, levando-se em consideração o grau de importância dos sistemas e processos de negócio envolvidos.

Convém que a segurança da informação e a privacidade dos titulares de dados seja considerada nesses projetos, independentemente do tipo.

8.8.6 Gestão de Incidentes de Segurança da Informação

Um processo de gerenciamento de incidentes deve ser estabelecido e implementado. Procedimentos de segurança devem ser elaborados para registro, classificação e tratamento de incidentes de segurança da informação.

8.9 Sistema de Gestão da privacidade da informação (SGPI)

Um programa de boas práticas e governança em proteção e privacidade de dados dever ser formulado conforme orienta o Art. 50 da lei 13709/2018 o qual prevê que:

"*Os controladores poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais. "*

O Sistema proposto de Gestão da privacidade da informação deve possuir uma metodologia consolidada em processos, fases, etapas, políticas, procedimentos e ferramentas técnicas, dentre elas teremos:

– Gestão de políticas de segurança da informação;
– Gestão de projetos;
– Gestão de bases de dados;
– Gestão dos contratos com subcontratantes;
– Gestão das avaliações de impacto (RIPD);

– Gestão dos consentimentos;
– Gestão da tabela de temporalidade;
– Gestão de reclamações e direitos dos titulares;
– Gestão de incidentes de proteção e privacidade;
– Gestão de acessos;
– Gestão dos tratamentos de dados pessoais;
– Gestão de riscos de proteção e privacidade

Afim de demonstrar comprometimento relação a proteção e privacidade dos titulares, todo o tratamento de dados realizado pela Unimed do Oeste do Paraná deverá seguir as regras previamente aprovadas e publicadas nas normas abaixo listadas, assim a segurança dos dados estará integrada no gerenciamento de projetos, assegurando que os riscos envolvidos estejam identificados e foram considerados, isto se aplica, de um modo geral, a qualquer projeto, independentemente do seu propósito, por exemplo, projeto que envolva um processo crítico da Unimed, um processo de TI, de gerenciamento de recursos próprios ou outro processo de apoio. Todas as normas que regem a adequação a LGPD foram desenvolvidas considerando os requisitos previstos na ABNT NBR ISO/IEC 27701:2019:

1. Etapas para adequação a LGPD;
2. Guia para avaliação de riscos e controles;
3. Guia para exclusão segura de dados e Tabela de temporalidade;
4. Guia para Tratamento e resposta a incidentes;
5. Template para criação do RIPD – Relatório de Impacto de dados.

Esses documentos/guias devem garantir que os princípios e os direitos dos titulares de dados previstos na lei geral de proteção de dados sejam adotados.

Para todos os dados/informações mapeados serão considerados, requisitos legais, necessidade de coleta de consentimento e todos os 10 princípios descritos no Artº 6 Capitulo I da LGPD:

1. **Finalidade** – Utilizar as informações unicamente para a finalidade a qual ela é coletada e que o titular tem o prévio conhecimento.
2. **Adequação** – Compatibilidade do tratamento com as finalidades informadas ao titular.
3. **Necessidade** - Data Minimization, serão coletados os dados mínimos necessários para atingir a finalidade que se deseja.

4. **Livre acesso** – Garantia aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais.
5. **Qualidade dos dados** – Deixando-os exatos e atualizados, seguindo a real necessidade no tratamento.
6. **Transparência** - Titular deve ter informações claras e acessíveis sobre o tratamento e seus responsáveis.
7. **Segurança** – Coibir situações acidentais ou ilícitas como invasão, destruição, perda, difusão. É dever da empresa inibir situações como ataques hackers, venda ou perda de informações.
8. **Prevenção** – Ainda sobre a segurança, a empresa deve prevenir de danos ao titular em virtude do tratamento de dados realizado por ela.
9. **Não Discriminação** – Impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos.
10. **Responsabilização** – Responsabilização do agente, obrigado a demonstrar a eficácia das medidas adotadas. Demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

8.10 Orientações ao Usuário Final

8.10.1 Uso Aceitável dos Ativos

Estabelecer as diretrizes e responsabilidades para o acesso aos recursos de Tecnologia da Informação disponibilizados pela cooperativa.

8.10.2 Mesa Limpa e Tela Limpa

Adotar procedimentos de “mesa limpa” ao final do expediente e instalação de armários com dispositivos de segurança para armazenamento de informações, exceto quando classificadas como “pública” e que possua mecanismos de recuperação aprovados e aplicados.

8.10.3 Transferência de Informações

Definir regras e procedimentos para acondicionamento, envio e recebimento de documentos sensíveis em meios físicos e em meios digitais.

8.10.4 Acesso à Internet e a Redes Sociais

Estabelecer as diretrizes de proteção relativas ao uso da Internet e de outras redes públicas de computadores, com o objetivo de reduzir o risco a que estão expostos os Ativos de Tecnologia

da Informação da cooperativa, todo acesso será disponibilizado de forma restrita ou controlada conforme a necessidade da cooperativa/função, afim de prevenir que ações prejudiciais sejam executadas, evitando perdas/fraudes financeiras, danos à imagem/reputacionais, parada de sistemas ou perda de produtividade.

Para que usos indevidos sejam inibidos deverá ser implantado um mecanismo de rastreio dos acessos à internet, afim de identificar qual foi o usuário e qual o recurso/local acessado.

Estabelecer diretrizes de proteção e conduta no uso das Redes Sociais indicando quais são os colaboradores autorizados a realizarem postagens nos canais oficiais da cooperativa, bem como fazer uso de canais particulares para fins de divulgação de conteúdos relacionados ao ambiente de trabalho ou a cooperativa.

A Unimed do Oeste do Paraná, como detentora de sua marca, não autoriza a divulgação da mesma, de sua imagem ou de informações de sua propriedade nas mídias e redes sociais salvo em caso de consentimento formal;

8.10.5 Conscientização de Segurança da Informação

- Desenvolver programas de capacitação específicos, visando à ampliação da cultura organizacional, quanto à importância da segurança da informação, e seu valor estratégico para a cooperativa.
- Desenvolver um programa de conscientização continuo que vise minimizar a ocorrência de falhas humanas;
- Desenvolver um programa de engajamento que nos leve a uma cultura organizacional consciente em relação a segurança da informação e comunicação.

8.10.6 Acesso ao Correio eletrônico e a Ferramentas de Colaboração

Estabelecer regras para utilização de correio eletrônico e ferramentas de colaboração providas pela empresa para execução das tarefas operacionais.

Devem ser definidos no mínimo os seguintes pontos:

- Quais documentos podem não ser compartilhados e qual a ferramenta que deve ser usada para tal ação;

- Para quais endereços de e-mail, números de telefone os documentos podem ser enviados; (somente os existentes em contrato, um novo endereço perante comprovação prévia da identidade do requerente);
- Quais setores podem realizar a disponibilização dos dados;
- Qual a conduta a ser seguida em caso de compartilhamento indevido;

Capacitações quanto ao comportamento dos colaboradores no uso das ferramentas em questão devem ser periodicamente realizados por uma equipe competente.

8.10.7 Proteção contra Códigos Maliciosos

Estabelecer regras para a proteção dos recursos de Tecnologia da Informação da empresa contra ação de códigos maliciosos e programas impróprios.

8.11 Gestão de riscos

Devido a interpretação estendida aplicada ao termo “segurança da informação” por orientação da ISO IEC 27701:2019 a gestão de riscos aqui tratada deverá integrar segurança da informação e a proteção da privacidade dos dados pessoais.

A gestão de riscos de proteção e privacidade será realizada de acordo com a norma:

1. Guia para avaliação de riscos e controles;

8.11.1 Definição de critérios de riscos

Estabelecer os critérios de aceitação de riscos e os critérios para o desempenho das avaliações dos riscos de segurança da informação.

8.11.2 Análise, Avaliação e Tratamento de Riscos

Estabelecer regras para implementar um processo de gerenciamento de riscos, com o inventário de ativos, Análise, Avaliação, Tratamentos de dados, Aceitação, Comunicação e Monitoramento dos Riscos.

Determinar as potenciais consequências quando da materialização dos riscos identificados, juntamente com a probabilidade realística da sua ocorrência.

Determinar quais controles necessariamente devem ser aplicados no intuito de eliminar ou minimizar a probabilidade de ocorrência dos riscos. Ao avaliar a aplicabilidade dos objetivos de controle e dos controles (ABNT NBR ISO/IEC 27001:2013, Anexo A) para o tratamento dos riscos, os objetivos de

controles e os controles devem ser considerados no contexto de ambos os riscos de segurança da informação, bem como os riscos relativos ao tratamento de DP, incluindo os riscos/danos que os titulares de DP possam sofrer.

8.11.4 Gestão de Continuidade de Negócios

Estabelecer regras e os princípios que regulamentam a Gestão da Continuidade do Negócio, através de um processo sistêmico para que se construa uma resiliência organizacional que seja capaz de responder efetivamente aos incidentes críticos de segurança e salvaguardar as atividades e a reputação da empresa.

8.12 Monitoramento e Auditoria

Estabelecer regras para criação de um programa de auditoria interna do processo de Gestão de Segurança da Informação, visando verificar o cumprimento dessa política e se os controles implementados estão atendendo eficazmente a conformidade dos requisitos. Deverá ser conduzida uma análise crítica dos resultados da auditoria, com o objetivo de determinar ações preventivas e corretivas para melhoria contínua do processo de Gestão de Segurança da Informação e privacidade. Um plano de ação deve ser elaborado com base no relatório gerado pela auditoria.

O resultado de auditoria deve ser caracterizado como informação sigilosa, quando esse puder comprometer a segurança dos processos de negócio da empresa.

Todo ativo de informação sob responsabilidade da Unimed do Oeste do Paraná é passível de auditoria em data e horários determinados pelo comitê, podendo esta, também, ocorrer sem aviso prévio.

Na realização de uma auditoria, durante a sua execução, deverão ser resguardados os direitos quanto à privacidade de dados pessoais, desde que estas não estejam dispostas em ambiente físico ou lógico de propriedade da Unimed do Oeste do Paraná ou de seus clientes.

Com o objetivo de detectar atividades anômalas de processamento da informação e violações da Política, das Normas ou dos Procedimentos de Segurança da Informação, a área de proteção e privacidade de dados poderá realizar monitoramento e controle proativos, mantendo a confidencialidade do processo e das informações obtidas, sendo que, as informações obtidas poderão servir como indício ou evidência em processo administrativo e/ou legal.

8.13 Gestão de Indicadores de Segurança

Indicadores e métricas devem ser definidos para os processos de segurança da informação, objetivando monitorar, através de uma análise crítica, o desempenho e eficácia dos controles implementados. Os indicadores deverão ser criados baseados nos objetivos estratégicos da empresa.

A análise crítica deve ser realizada em intervalos planejados ou quando mudanças significativas ocorrerem, para assegurar a sua contínua pertinência, adequação e eficácia e demonstrem apoio e comprometimento com a Segurança da Informação.

9 Penalidades/Processo Disciplinar

Nos casos em que houver violação desta Política ou das normas de segurança da informação, sanções administrativas e/ou legais poderão ser adotadas, podendo culminar com o desligamento e eventuais processos administrativos, cíveis e judiciais cabíveis.

9.1 Violações

São consideradas violações à política, às normas ou aos procedimentos de segurança da informação as seguintes situações, não se limitando às mesmas:

1. Quaisquer ações ou situações que possam expor a Unimed do Oeste do Paraná ou seus clientes à perda financeira, direta ou indiretamente, potenciais ou reais, comprometendo seus ativos de informação e/ou sua imagem;
2. Quaisquer ações ou situações que venham expor titulares de dados a alto risco, à garantia dos princípios gerais de proteção de dados pessoais previstos na LGPD e às liberdades civis ou seus direitos fundamentais;
3. Acessos não autorizados, situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão de qualquer dado ou informação sob responsabilidade da Unimed do Oeste do Paraná;
4. Utilização indevida de dados corporativos e divulgação não autorizada de informações, segredos comerciais ou outras informações sem a permissão expressa do responsável legal pela informação, sempre considerando sua classificação;
5. Uso de dados, informações, equipamentos, *software*, sistemas ou outros recursos tecnológicos, para propósitos ilícitos, que possam incluir a violação de leis, de regulamentos internos e externos, código de ética ou de exigências de organismos reguladores da área de atuação da Unimed do Oeste do Paraná;

6. A materialização de qualquer um dos riscos listados no “Guia análise riscos (segurança e privacidade)”; e
7. A não comunicação imediata à área de proteção e privacidade de quaisquer descumprimentos da política, de normas ou de procedimentos de Segurança da Informação, que porventura um colaborador, empregado, estagiário, aprendiz ou prestador de serviços tome conhecimento, presencie ou execute.

9.1.1. Não conformidade e ação corretiva

Todos os responsáveis quando acionados devido a uma não conformidade devem:

- De acordo com o plano de resposta a incidentes:
  - Tomar ações para controlar e corrigi-la;
  - Tratar com as consequências;
- Avaliar a necessidade de ações para eliminar as causas de não conformidade, para evitar sua repetição ou ocorrência, por um dos seguintes meios:
  - Analisar criticamente a não conformidade;
  - Determinar as causas da não conformidade; e
  - Determinar se não conformidades similares existem, ou podem potencialmente ocorrer;
- Manter a informação documentada como evidência e enviar cópia ao encarregado pela proteção de dados, da:
  - Natureza das não conformidades e todas as ações subsequentes tomadas; e
  - Resultado das ações corretivas aplicadas

As ações corretivas devem ser apropriadas aos efeitos das não conformidades encontradas.

9.2 Sanções

A violação à política, às normas ou aos procedimentos de segurança da informação ou a não aderência à Política de Segurança da Informação são consideradas faltas graves, podendo ser aplicadas penalidades previstas em normas internas de recursos humanos ou leis vigentes e resultar em:

- Suspensão do uso da ferramenta;
- Advertência verbal e escrita;
- Penalidades cíveis;
- Demissão por justa causa.

As penalidades não seguem ordem, as infrações podem ser analisadas e classificadas sem que outra tenha acontecido anteriormente.

10 Atualização

Deve-se estabelecer a periodicidade mínima para a revisão da Política de Segurança da Informação, bem como os demais documentos normativos gerados a partir dela, a fim de que não fiquem ultrapassados ou desatualizados. Não obstante, a política pode ser revisada tempestivamente, a qualquer momento que se fizer necessário.

11 Aprovação

Os documentos integrantes da estrutura normativa da Segurança da Informação deverão ser aprovados e revisados conforme critérios descritos abaixo:

11.1 Política

Nível de aprovação: Coordenação, Gerência, Diretoria e conselhos.

Periodicidade da revisão: Trienal.

11.2 Normas Técnicas e procedimentos

Nível de aprovação: Coordenação, Gerência, Diretoria e conselhos.

Periodicidade da revisão: Bienal.

12 Referências Legais

Correlacionam-se com a política, com as diretrizes e com as normas de Segurança da Informação as Leis abaixo relacionadas, mas não se limitando às mesmas:

- Lei Federal 12.737, de 30 de novembro de 2012 (Tipifica os Delitos Informáticos);
- Lei Federal 12.965, de 23 de abril de 2014 (Marco Civil);
- Decreto-Lei 2.848, de 7 de dezembro de 1940 (Institui o Código Penal);
- Lei Federal 10.406, de 10 de janeiro de 2002 (Institui o Código Civil);
- Constituição da república federativa do Brasil de 1988;
- Lei Federal 13.709, de 14 de agosto de 2018 (LGPD);
- Emenda constitucional 115, de 10 de fevereiro de 2022 (EC 115)