## Sumário



- - -

## Objetivo

Durante o curso de suas atividades, a UNIMED DE ARAÇATUBA – COOPERATIVA DE TRABALHO MÉDICO e suas filiais realiza o tratamento de informações e dos dados pessoais, sejam de seus cooperados, colaboradores, seus clientes, fornecedores, parceiros e terceiros, que nessa política serão denominados por usuário, a presente Política Interna de Segurança da Informação e Proteção de Dados Pessoais tem como objetivo apresentar as regras aplicáveis para o tratamento de dados pessoais, mais alto nível de segurança, confidencialidade, integridade, fidedignidade em atenção às disposições da Lei Federal nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais ou "LGPD"), alterada pela Lei Federal nº 13.853/2019, dentro dos processos de captação, produção, armazenamento, uso e disseminação de informações, bem como organizar todos os pontos necessários para a construção de um programa de privacidade que garanta a conformidade com a referida legislação.

Como parte da Unimed de Araçatuba, nossos colaboradores, gestores e administradores devem sempre, no exercício de suas atividades, garantir que as informações e os dados pessoais são tratados em conformidade com as leis vigentes no território nacional e com esta Política.

Caso você tenha alguma dúvida em relação às suas obrigações, direitos e deveres em relação as informações tratadas no decorrer da atividade, entre em contato com

nosso departamento de Tecnologia de Informações através do e-mail: Operadora: informatica@unimedaracatuba.com.br; Hospital: ti@unimedaracatuba.com.br.

Seguindo os mesmos parâmetros de obrigatoriedade, em caso de dúvida no tratamento de dados pessoais e suas proteções, entre em contato com nosso Encarregado de proteção de dados pessoais, através do e-mail dpo@unimedaracatuba.com.br.

Resumidamente, esta Política visa demonstrar o comprometimento da Unimed em:

- Proteger os direitos dos usuários;
- Adotar processos e regras que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais;
- Promover a transparência na forma em que a Unimed trata as informações e os dados pessoais; e
- Proteger a Unimed, bem como seus colaboradores, clientes, fornecedores, parceiros e terceiros de riscos envolvendo incidentes de segurança envolvendo dados pessoais.
- Garantindo assim:
    - Garantir confidencialidade, integridade, disponibilidade, autenticidade e qualidade da informação;
    - Proteger as informações de diversos tipos de ameaças externas ou internas, para garantir a continuidade dos negócios;
    - Otimizar mecanismos para segurança da informação;
    - Assegurar que as informações sejam prontamente, identificáveis e/ou recuperáveis, de acordo com sua aplicação;
    - Controlar informações geradas na organização;
    - Garantir adequada utilização da Tecnologia da Informação;
    - Evitar a perda parcial ou total das informações.

- - -

A Unimed considera que garantir o tratamento de dados pessoais realizado de forma legítima, correta e conforme é importantíssimo para o sucesso de suas atividades, bem como para resguardar sua imagem e credibilidade perante colaboradores, clientes, fornecedores e parceiros, bem como perante o público em geral e a A.N.P.D.

Havendo conflito entre as disposições desta Política e a legislação de proteção de dados aplicável, esta última prevalecerá.

## Abrangência

As diretrizes dessa política se aplicam a todos os associados cooperados, conselheiros, colaboradores, e demais pessoais, físicas ou jurídicas (todas as partes interessadas), que se relacionam com a Unimed de Araçatuba e Filiais.

## Siglas e definições

- **A.N.P.D.**
  Autoridade Nacional de Proteção de Dados;
- **C.F.M.**
  Conselho Federal de Medicina;
- **C.L.T.**
  Consolidação das Leis Trabalhistas;
- **C.I.D.**
  Comunicado de Incidente de Dados;
- **C.S.V.**
  *Comma-separated Values;*
- **D.P.O.**
  Data Protection Officer
- **L.G.P.D.**
  Lei Geral de Proteção de Dados;
- **G.E.D.**
  Gerenciamento Eletrônico de Documentos;
- **J.S.O.N.**
  *JavaScript Object Notation;*
- **S.I.P.O.C.**
  *Supplier/Input/Process/Output/Customer*
- **T.I.**
  Tecnologia da Informação.

## Diretrizes

- - -

## 1. Informação

É o resultado do processamento, manipulação e organização de dados. Ela pode ser impressa ou escrita em papel, armazenada eletronicamente, transmitida pelo correio ou por meio de correio eletrônico, mostrada em filmes ou falada em conversas. Genericamente, o conceito de informação está intimamente ligado às noções de restrição, comunicação, controle, dados, forma, instrução, conhecimento, significado, estímulo, padrão, percepção e representação de conhecimento.

### 1.1. Propriedade da informação

É garantido de que todas as informações produzidas, vinculadas aos dados pessoais, veiculas e armazenadas são de propriedade dos usuários, de uso restrito e exclusivo da UNIMED DE ARAÇATUBA E SUAS FILIAIS, com as devidas autorizações, podendo ser disponibilizada por meio de solicitação ao usuário.

A Segurança da informação pós rompimento de contrato é controlado de forma que garante que o fluxo de acesso entre rede e relacionamento com o cooperado seja limitado de acordo com as regras do contrato.

As informações pessoais dos beneficiários utilizadas pelos colaboradores também estão protegidas pelo termo de sigilo de uso, devidamente assinado no ato da contratação.

É contratualmente previsto a obrigatoriedade de manter o sigilo das informações relacionadas aos usuários, pelos provedores externos da Unimed que recebem e/ou obtém informações desses, para desta forma garantir a segurança e confidencialidade do seu trabalho.

### 1.2. Classificação do documento e da informação

Em toda atividade executada na instituição, existe o tratamento, manipulação e o armazenamento de informações, onde essa, em muitos casos, podem ser restritas, ou não, a todos os públicos. Dessa forma, existe a necessidade da existência de uma classificação interna da Unimed de Araçatuba, quanto os documentos que são gerados.

- - -

### 1.2.1. Pública

O documento deve ser classificado como pública, quando ela puder ser divulgada a todos, isto é, colaboradores, cooperados, terceirizados, clientes, fornecedores e público em geral, sem que isso provoque danos à imagem e a moral da instituição e impacto no negócio.

Por Exemplo:

- **Politicas Institucionais** (https://unimedaracatuba.coop.br/politicas-institucionais);
- **Notícias** (https://unimedaracatuba.coop.br/imprensa-e-comunicacao);
- **Relatório de Sustentabilidade** (https://unimedaracatuba.coop.br/relatorio-de-gestao-e-sustentabilidade);
- **Código de Conduta** (https://unimedaracatuba.coop.br/documentos/codigo_de_conduta_atual.pdf);
- **Demonstrações Contábeis:** (https://unimedaracatuba.coop.br/transparencia);
- **IDSS** (https://unimedaracatuba.coop.br/indice-de-desempenho-da-saude-suplementar)

### 1.2.2. Interna

O documento deve ser classificado como interna quando não for desejável que ela se torne conhecida por pessoas de fora da Unimed de Araçatuba e suas filiais. Por exemplo:

- Comunicações Internas (PSI);
- Procedimentos Internos (UNIMAKER e MV 2000I);
- Normas (Manuais Setoriais - Sigquali);
- Intranet da Unimed de Araçatuba.

Assim, caso haja vazamento e as informações se tornem de conhecimento público, seja esse vazamento de pequena ou grande escala, será iniciado o protocolo CID

(Comunicado de Incidente de Dados), informando o usuário, em todas as ocasiões e a autarquia, caso haja necessidade, pois, a característica da informação classificada como interna, à possibilidade da ocorrência de um grande prejuízo ao usuário/titular dos dados e em segundo plano à organização. Como são informações relevantes para o funcionamento dos negócios, precisam principalmente ter sua integridade protegida.

### 1.2.3. Confidencial

O documento deve ser classificado como confidencial, quanto se trata de caráter estratégico de negócios. Informações restritas dentro da organização e protegidas de acesso externo, onde qualquer perda da confidencialidade causará eventual comprometimento das operações, resultando em perdas financeiras, de competitividade, de imagem e risco de ações judiciais.

Por Exemplo:

- Ata de reunião da diretoria executiva e dos conselhos;
- Ata de reunião do Planejamento estratégico;
- Relatório de diagnóstico para o conselho de administração de Auditoria;
- Relatório dos Canais de Denúncias (Canal de Denúncia, Canal do Colaborador, Canais de Relacionamento com o Cooperado (Área Restrita)).

Entretanto, em se tratando, no decurso da sua utilização de informações confidenciais, seja no ambiente virtual e físico, sua disponibilização somente ocorrerá com prévia autorização, por exemplo, o “Livreto do Guia Médico”, onde o seu emprego de forma irregular ou vazamento pode acarretar para o usuário, maior interessado, e a Unimed de Araçatuba perdas e danos significativos.

### 1.2.4. Restrita

Os documentos conditos nos canais específicos para os públicos da Unimed de Araçatuba, como o Canal do Beneficiário, Canal do Cooperado e Rede Credenciada

devem ser classificadas como restrita quando acessos não autorizados a esses, mesmo que por membros da própria organização, levando o seu vazamento ensejar em sérios danos ao negócio, uma vez que são considerados restritos a cada um dos públicos, tendo em vista o seu conteúdo. Onde, por exemplo, cada beneficiário tem acesso as informações do seu plano de saúde de assistência suplementar, através de usuário e senha, garantindo assim a segurança das informações contidas nesse Canal.

Logo, a informação restrita precisa ser protegida contra acessos internos e externos. São tão quão importantes que as informações confidenciais e por isso devem receber um grau de proteção elevado, como "usuário e senha" para o acesso.

Fora os casos de acesso pelo próprio usuário, só devem ter acesso às informações restritas, colaboradores que necessitem dessas informações para a realização de suas atividades, independentemente do cargo ocupado.

Por exemplo:

- Canal do Colaborador;
- Central P.J.;
- Canal do Cooperado e Rede Credenciada;
- Formulário de Cadastro dos Colaboradores (Docuware);
- Contrato de Plano de Saúde Suplementar (Docuware);
- Documentos de Comitês (Sigquali);
- Notas Fiscais (Pasta setorial);
- Contas Médicas (Docuware e UNIMAKER);
- Processos Jurídicos no Geral (Projuris).

### 1.3. Nível de acesso a documento e informações

O acesso é restrito por departamento e definido em comum acordo com as áreas e o setor de T.I.

A liberação será pertinente conforme a atividade exercida no departamento e suas necessidades.

- - -

### 1.3.1. Acesso à Internet

Com relação ao acesso à internet, a permissão será realizada por perfil, conforme o definido entre o supervisor(a) do departamento e o T.I. e são classificados de 3 formas: negado total, uso mínimo e uso monitorado.

**a. Negado total**

Corresponde ao profissional que não necessita da internet para desempenhar suas atividades dentro da empresa;

**b. Uso mínimo**

Compreende ao profissional, que para desempenho de suas funções, necessitam de acesso a sites específicos;

**c. Uso monitorado**

Corresponde ao profissional que tem acesso totalmente liberado, sendo que neste caso é mantido o log de acesso.

### 1.3.2. Acesso aos sistemas

Para acesso aos sistemas, obrigatoriamente deve-se informar o usuário e senha, sendo que a partir disto, será liberado somente o acesso as opções predefinidas pelo supervisor(a) do departamento e classificadas conforme o anexo 2 (Classificação de acesso), aba 1 (Por Departamento) dessa política.

**a. Novo colaborador**

Para acesso aos sistemas internos e externos da instituição, o supervisor(a) imediato do colaborador realizará a solicitação junto ao departamento de tecnologia da informação, via e-mail, anexando o formulário, devidamente controlado pelo Departamento Pessoal, com o seu preenchimento, com os sistemas que o colaborador precisa ter acesso para a execução de suas atividades.

- - -

Para os acessos aos sistemas que não são de domínio do departamento de tecnologia da informação, como por exemplo, sistema da qualidade ou do atendimento, esse supervisor(a) realizará da mesma forma a solicitação para esse departamento responsável.

**b. Novo supervisor(a)/coordenador(a)**

Quando do desenvolvimento do colaborador esse troca de cargo para assumir a supervisão ou a coordenação de um departamento, o departamento pessoal informa o setor de tecnologia da informação para adequar o acesso aos sistemas internos e externos.

Também, quando isso ocorrer de forma temporária, por exemplo, cobrindo férias, o departamento pessoal fará da mesma forma, porém o setor de tecnologia da informação fará um cadastro que terá tempo determinado.

**c. Desligamento de colaborador**

Em caso de desligamento de colaborador, o departamento pessoal informará o departamento de tecnologia da informação o ocorrido e esse realizará a exclusão dos usuários pessoais deste. Quanto aos usuários setoriais (exemplo: ans@/dp.h@/financeiro@) esses serão remanejados para o supervisor(a) imediato responsável até que um novo colaborador assuma as responsabilidades hábeis a assumirem tais usuários.

### 1.3.3. Acesso a Rede(pastas)

Para o armazenamento dos documentos e registros do departamento, cada uma desse, possui uma pasta na rede monitorada da Unimed de Araçatuba, para realizar tais funções, somente o departamento tem acesso e pode realizar modificações no seu conteúdo. Em caso de corrompimento das informações, como possíveis exclusões da pasta, será acionado a contingência.

Quando houver a necessidade de mais de um departamento utilizar a mesma pasta, isso deve ser solicitado ao T.I. para que esse defina os acessos e permissões.

- - -

#### 1.3.4. Acesso aos Documentos

Posteriormente ao tratamento das informações pelos departamentos, esses são publicados ou arquivados de forma digital através de um sistema ou plataforma. Para que haja um controle sobre a manipulação, visualização e disseminação dessas informações conditas nos documentos, existe a restrição de acesso por usuários, onde esses são individualizados, sem permissão de divulgação desse acesso.

Esse controle é definido através do anexo 2 (Classificação de acesso), aba 2 (Por Colaborador), dessa política.

Para que haja um melhor entendimento, quanto aos documentos como prontuário médico, esse é arquivado pelo departamento de gerenciamento eletrônico de documentos. No tocante aos documentos de registro do departamento, como, Manual, SIPOC, Políticas e Matriz de Riscos, esses são arquivados no sistema da qualidade.

#### 1.3.5. Acesso aos registros

Cada departamento, através de sua **matriz de registros**, define a classificação dos seus registros, fazendo com que, os colaboradores do departamento tenham conhecimento das restrições advindas dessa classificação.

### 1.4. Gestão de continuidade de negócios

#### 1.4.1. Sistema Interno

Entende-se por gestão da continuidade do negócio o plano de contingência realizado com o objetivo de garantir a informação eficaz caso haja alguma falha no sistema.

Em caso de falha dos sistemas de informática, as atividades entre operadora e prestadores podem ser realizadas por meio guias físicas (papel), tanto para atendimento presencial na operadora quanto nos prestadores. Este processo é monitorado pela gestão de risco.

As remunerações dos prestadores e cobrança dos contratos será efetuada pela média histórica.

### 1.4.2. Plano de contingência de disponibilidade dos serviços de Tecnologia da Informação

Descrito no manual operacional do setor de Tecnologia da Informação da Operadora (OPS.MAN.TI-001).

### 1.4.3. Backup

- É obrigatório armazenar os arquivos inerentes a instituição no servidor de arquivos para garantir o *backup*.
- Para a realização do *backup* é utilizado o método 3/2/1 sendo 3 cópias, em 2 lugares diferentes e 1 mídia diferente. O *backup* é realizado com granularidade;
- A primeira cópia dos arquivos da operadora é mantida no servidor de *backup* que fica localizado fisicamente nas instalações do *datacenter* do Hospital Unimed, quanto aos arquivos do Hospital, esses são mantidos em ambiente diverso do principal em um cofre antichamas, em formato de "fita" gravadas no período noturno que é realizada de forma manual e evidenciada por meio de planilha;
- A segunda cópia dos arquivos da operadora é mantida no *datacenter* de uma empresa terceirizada e quanto aos arquivos do Hospital, esses são mantidos em um servidor de contingência localizado em ambiente diverso do servidor principal e do cofre antichamas, sendo realizado diariamente de forma automática;
- A terceira cópia dos arquivos da operadora é localizada em "nuvem" no provedor da empresa terceirizada e quanto aos arquivos do Hospital, esses são mantidos no servidor de *backup* que fica localizado fisicamente nas instalações do *datacenter* da operadora da Unimed com cofres antichamas;

### 1.4.4. Tentativa de Invasão

Quando identificado uma tentativa de invasão, é realizado o bloqueio do serviço e a criação de uma rota alternativa. Quando identificado o invasor toma-se a devidas medidas legais cabíveis.

## 1.5. Monitoramento de negócios de T.I.

- - -

Os processos de negócios da T.I. são monitorados por meio dos indicadores cadastrados no sistema da qualidade.

### 1.6. Processo de fraude/invasão e métodos de seguranças.

Caso ocorra uma invasão ou fraude, o caso será tratado individualmente. Ocorrendo um possível vazamento de dados é realizado o protocolo C.I.D., conforme 1.2.2.

Para o monitoramento mais preciso das tentativas de invasão, foi criado um indicador "ÍNDICE DE BLOQUEIO DE TENTATIVA DE INVASÃO".

Caso ocorra falha no processo de segurança que acarrete em perda de informação, será acionado o plano de contingência que é a recuperação do backup. Em caso de invasão, os servidores serão desligados provisoriamente.

### 1.7. Descarte

#### a. Equipamentos

Após a avaliação e verificação que o equipamento não tem mais utilidade, será retirado a placa de patrimônio e encaminhada para o setor de contabilidade para baixo do ativo imobilizado. Os equipamentos serão doados para entidades assistenciais

#### b. Material

Todos os materiais descartáveis que contém informações dos usuários, se não forem mais uteis ao processo que representa, são monitorados até o seu devido descarte, na instituição de coleta credenciada a época, pois o seu vazamento pode acarretar em perdas e danos ao usuário em todas as esferas.

## 2. Dados Pessoais

### 2.1. Segurança

Para garantir a segurança dos dados pessoais tratados no exercício de suas atividades e evitar a ocorrência de acessos indevidos ou não autorizados, perda, destruição ou qualquer outra ação que comprometa a integridade, disponibilidade ou confidencialidade dessas informações, a instituição manterá procedimentos e ferramentas implementadas, os quais seguem os mais altos padrões das normas técnicas de segurança da informação.

Para manter todos os dados pessoais tratados de forma sempre segura, o Comitê de Privacidade, o Encarregado (DPO) e o departamento de Tecnologia da Informação da instituição deverão trabalhar sempre em conjunto, criando ações e planejamentos para tanto, combatendo possíveis vazamentos e acessos indevidos.

A Unimed de Araçatuba possui protocolo específico para casos de ocorrência de incidentes de privacidade envolvendo dados pessoais, que pode ser encontrado no Incidentes de privacidade dessa Política.

Para garantir que as medidas de segurança implementadas pela instituição se mantenham sempre atualizadas e em consonância com as melhores práticas e ferramentas disponíveis atualmente no mercado, estes manuais e procedimentos passam por revisões periódicas, identificando e corrigindo eventuais falhas.

## 2.2. Coleta, uso, armazenamento e descarte de dados

Todas as atividades de tratamento de dados pessoais promovidas pela Unimed de Araçatuba deverão ocorrer em respeito a todos os pilares deste documento, estando sempre atribuídas a uma base legal específica.

Para melhor definir os fluxos de tratamento de dados, existe uma Diretriz de Tratamento de Dados (UA.DA.CPL-001), documento esse anexo a essa política.

### 2.2.1. Coleta de Dados Pessoais

O procedimento de coleta de dados pessoais deverá ser restrito àqueles essenciais para o cumprimento da finalidade primária determinada e informada ao titular dos dados, sempre observando a necessidade de manter atualizados os dados coletados.

Sempre que a coleta for feita em pontos ativos (onde os titulares fornecem seus próprios dados), os titulares dos dados pessoais deverão ser informados, antes da coleta, de todos os detalhes sobre a atividade de tratamento, nos termos do item 7.

Dados pessoais somente poderão ser coletados em pontos passivos (através de acesso a bases públicas/privadas de dados, por exemplo) se tais bases forem notoriamente fidedignas (atribuídas a órgãos ou entidades públicas e oficiais), se existir um contrato entre o provedor da base e a Unimed, ou mediante expressa autorização do Encarregado ou do Comitê de Privacidade.

Dados fornecidos por terceiros somente poderão ser recebidos mediante celebração de contrato que inclua a cláusula de privacidade robusta o suficiente, conforme orientações do departamento jurídico e do Encarregado, que deverão verificar a idoneidade de todos os terceiros que fornecem dados à instituição. Nestes casos, os dados pessoais deverão possuir uma descrição completa do seu ciclo de vida, antes da realização do compartilhamento à instituição, garantindo que, em nenhuma destas etapas, tenha ocorrido qualquer forma de tratamento ilícito ou inadequado.

### 2.2.2. Uso de Dados Pessoais

A utilização dos dados pessoais deverá estar limitada à expectativa que o titular dos dados possuía quando da realização da coleta das informações (inclusive se a coleta foi realizada por terceiros), sendo que, na eventual hipótese de necessidade de alteração da finalidade previamente informada ao titular, este deverá ser novamente informado sobre as intenções da instituição, avaliando a necessidade de qualquer adequação.

O mesmo dado jamais poderá ser utilizado para outra finalidade, exceto com a ciência / expectativa do titular e esses somente poderão ser tramitados via celular se esse for o celular corporativo do setor, conforme as diretrizes de utilização definidas na Diretriz De Privacidade E Proteção De Dados Pessoais – Celular Corporativo (UA.DA.CPL – 002).

### 2.2.3. Armazenamento de Dados Pessoais

O armazenamento de dados pessoais deverá ser realizado pelo tempo mínimo necessário para atendimento da finalidade pretendida e cumprimento de eventuais obrigações legais que regulam determinada atividade de tratamento, seguindo normas constitucionais e infraconstitucionais.

Sendo cumprida a finalidade e observados os prazos legais de necessária retenção da informação, os dados deverão ser descartados, o que por sua vez deverá seguir meios adequados, abaixo especificados:

- Documentos e dados em formato físico: O descarte deverá ser realizado pelo Setor GED (Gerenciador Eletrônico de Documentos, sendo proibido o uso direto de lixeiras) que envia os documentos a empresa de reciclagem devidamente contratada, onde em cada operação é realizada sobre vistoria de um colaborador, desde a retirada dos documentos no setor até a finalização do processo.
- Documentos e dados em formato eletrônico: Arquivados através do sistema do Setor GED, até o fim do prazo prescricional.

Alternativamente, para fins estatísticos e de pesquisa, dados pessoais poderão passar por procedimento de anonimização permanente, validado pelo Encarregado.

### 2.2.4. Tratamento de Dados Pessoais Sensíveis

A legislação de proteção de dados pessoais classifica alguns tipos de dados pessoais como dados sensíveis, dada a capacidade que possuem de gerar discriminação ao titular destas informações.

A LGPD classifica as seguintes informações como dados pessoais sensíveis: a origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de carácter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando relacionados a um indivíduo.

Em regra, a Unimed de Araçatuba não trata dados sensíveis para suas operações, utilizando-os apenas para finalidades especificas internas e com terceiros contratos e também junto ao departamento de recursos humanos. Não obstante e em todo caso, para que as atividades de tratamento de dados pessoais sensíveis sejam consideradas

lícitas e legítimas, se faz necessário o enquadramento destas atividades em uma das bases legais previstas pela LGPD.

Adicionalmente, dados sensíveis deverão receber a máxima prioridade na segurança, nos termos das políticas de segurança e classificação da informação vigentes.

### 2.2.5. Tratamento de Dados Pessoais de Crianças e Adolescentes

Da mesma forma, o tratamento de dados pessoais de "crianças" e "adolescentes" deve ser situação excepcionalíssima. Nestes casos remotos, ele somente deverá ser realizado:

- Visando o melhor interesse de tais indivíduos, ou seja, com a finalidade de beneficiá-los, ainda que de forma indireta.
- De forma clara e compreensível, de modo que informações destinadas a este público deverão ser prestadas de modo claro, acessível, consideradas as condições físico-motoras, perceptivas, sensoriais, intelectuais e mentais dos destinatários, com o uso de recursos audiovisuais, quando adequado.

Quando do tratamento dos dados de "crianças", deverá, necessariamente, haver a coleta do consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal, mantendo públicas as informações sobre o tipo de dados coletados, a forma de utilização e as garantias dos demais direitos dos titulares assegurados pela lei.

### 2.2.6. Qualidade dos dados cadastrais

Visando manter as informações de forma fidedigna e sempre em conformidade com as unidades públicas (ANS, Receita Federal) a Unimed de Araçatuba exerce de forma contínua e ininterrupta a validação e possíveis correções nos dados pessoais presentes no exercício das execuções das tarefas da instituição, fazendo assim com que os erros sejam minimizados e a atenção ao beneficiário seja precisa.

Essa política tem como definição essas práticas, trazendo a formalidade desse processo, controlando a qualidade que garantam a integridade, segurança e fidedignidade dos dados, abrangendo os processos de captação, produção, armazenamento, uso e disseminação de informações.

### 2.2.7. Criptografia dos dados

Os dados pessoais contidos no sistema interna são armazenados em servidores locais e são manuseados por meio de ferramentas que garantem a criptografia parcial, além de dificultar a identificação das informações contidas nos arquivos.

Para a compreensão, segue abaixo algumas das descrições das barreiras que são utilizadas como defesa para garantir a segurança das informações:

- Os servidores só poderão ser invadidos por meio de quebra de segurança do firewall;
- Para acesso aos arquivos de dados é necessário ter um conhecimento prévio de sua localização;
- Os dados deverão ser descriptografia;
- O dicionário de dados possui uma relação entre os dados descriptografados;

| |
|---|
| Obs: O dicionário de dados se encontra em outra localidade dentro do servidor que somente podem ser acessados pelos desenvolvedores; |

## 3. Aprimoramento de sistemas

No decurso das atividades estabelecidas internamente na Unimed de Araçatuba, para que haja melhoria nos processos, existe um ambiente sistêmico em paralelo (Segregado), para que essas melhorias sejam desenvolvidas, testadas e homologadas, sem que ocorra a interferência no ambiente laboral, havendo assim a garantia da estabilidade, segurança e qualidade dos sistemas de informação, evitando o risco de introduzir um sistema com falhas de software ou que ainda não foram testados ou homologados.

- - -

Essa execução é iniciada através da abertura de chamados ao departamento de Tecnologia da Informação pelas áreas solicitantes, uma vez que essas entendem a necessidade de melhoria nos sistemas. A abertura desses chamados está definida no manual do departamento de Tecnologia da Informação (OPS.MAN.TI-001).

## 4. Âmbito de Aplicação

Esta Política se aplica à Unimed de Araçatuba e a todas as empresas por ela controladas, bem como a todos os colaboradores que em algum momento possam ter contato com dados pessoais tratados pela, ou em nome da Unimed, em especial quando:

- A operação de tratamento tenha sido ou almeja ser realizada dentro território nacional Brasileiro;
- A atividade de tratamento objetivar a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados dentro do território nacional Brasileiro; e
- Os dados pessoais objetos do tratamento tenham sido coletados dentro do território nacional Brasileiro.

Políticas adicionais podem ser criadas em casos específicos, principalmente se exigido por lei ou regulamento.

## 5. Princípios norteadores da proteção da informação e dos dados pessoais

A Unimed de Araçatuba cuidará para que todas atividades de tratamento de dados pessoais estejam em conformidade com os 10 (dez) princípios trazidos pela legislação sobre privacidade e proteção de dados. São eles:

- **Princípio da boa-fé:** todas as operações de tratamento deverão ser pautadas em boas intenções, na moral e bons costumes aceitos pela sociedade.
- **Princípio da finalidade e adequação:** O tratamento de dados pessoais deve se limitar aos propósitos legítimos, específicos, explícitos e informados ao Titular, e somente deve ocorrer de formas compatíveis com estas finalidades. Dados

pessoais não poderão ser coletados/obtidos para uma finalidade, e depois utilizados para outra. Todos os usos de um dado devem ser compatíveis com o motivo original da coleta/obtenção.

- **Princípio da necessidade:** a coleta e utilização de dados pessoais deverá ser limitada ao mínimo necessário para o cumprimento das finalidades pretendidas e expostas ao titular, garantindo também, que tais informações sejam armazenadas pelo menor tempo possível/necessário.
- **Princípio do livre acesso e qualidade dos dados:** aos titulares deverá ser garantida a consulta facilitada e gratuita quanto a forma e duração do tratamento e integralidade de seus dados pessoais, estando assegurada a exatidão, clareza, relevância e atualização destes, conforme a DIRETRIZ DE PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS – QUALIDADE DOS DADOS CADASTRAIS (UA.DA.CPL-003) de controle da qualidade de dados, anexa a essa política.
- **Princípio da transparência:** serão garantidas aos titulares dos dados informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial.
- **Princípio da segurança e prevenção:** a segurança e confidencialidade dos dados pessoais devem ser garantidas por meio de medidas técnicas e organizacionais, abaixo exemplificadas, a fim de prevenir a ocorrência de incidentes de segurança envolvendo dados pessoais.
- **Princípio da não discriminação:** as atividades de tratamento de dados pessoais jamais poderão objetivar fins discriminatórios, ilícitos ou abusivos.
- **Princípio da responsabilização:** a Unimed de Araçatuba deverá armazenar registros de todas as atividades de tratamento de dados pessoais e as respectivas medidas tomadas para adequar tais atividades às normas relativas à privacidade e proteção de dados pessoais, comprovando a eficácia e eficiência de tais medidas.

## 6. Bases legais para o tratamento de dados pessoais

Para que uma atividade de tratamento promovida pela Unimed de Araçatuba seja considerada legítima e adequada à LGPD, ela deve estar acomodada em uma das hipóteses abaixo:

A Unimed de Araçatuba realiza atividades de tratamento visando o cumprimento de obrigações em leis ou em normas de órgãos reguladores atuantes em setores regulados (por exemplo, obrigações e licenças ambientais).

Nestes casos, é importante que os responsáveis pelo tratamento estejam cientes de qual a obrigação legal fundamenta o tratamento (lei, norma, regulação, decisão ou acordo judicial, etc.). Caso haja alguma alteração nestas regras, é possível que a atividade de tratamento também deva ser alterada.

Havendo dúvidas quanto à necessidade de se tratar dados para o cumprimento de obrigações legais ou regulatórias, é recomendado que o responsável pela atividade entre em contato com o Encarregado.

É importante que o tratamento realizado nestes casos esteja fundamentado em um contrato firmado (ou prestes a ser firmado) com o titular, e que seja essencial para que a Unimed cumpra com as obrigações estabelecidas neste contrato.

Em algumas hipóteses, contratos verbais também poderão ser considerados. Nestes casos, o Encarregado deve ser consultado para confirmar o enquadramento da atividade nesta base legal.

Alguns dados pessoais, ou documentos que contém dados pessoais, sejam de colaboradores, membros da Unimed, clientes, fornecedores ou demais terceiros, precisam ser armazenados para que a Unimed de Araçatuba possa garantir seus direitos de defesa, resposta, ou atuação junto a órgãos públicos, em processos judiciais ou administrativos.

É importante que a retenção dos dados não ultrapasse o período estabelecido nas normas, para fins jurídicos e administrativos, onde estabelece a guarda, por exemplo a Lei 13.787/2018 e a Lei 13.105/2015.

Dados pessoais podem ser utilizados para a realização de procedimentos de saúde, inclusive envolvendo serviços de saúde. Nestes casos, deve necessariamente haver o

envolvimento de um profissional de saúde, prestador de serviços de saúde, ou autoridade sanitária.

Esta base legal poderá ser utilizada para subsidiar o tratamento de dados, prezando pela preservação dos titulares, em caso de perigo ou iminência de perigo à sua vida ou incolumidade física.

A proteção do crédito pode fundamentar situações onde a Unimed trata dados pessoais, ou consulta dados pessoais visando decidir sobre a concessão de crédito ao funcionário e medidas de contratação com terceiros. Para a utilização desta base legal, é necessário que sejam observadas todas as leis aplicáveis à proteção ao crédito.

A prevenção à fraude pode ser aplicada somente a dados sensíveis, quando utilizados em procedimentos de identificação e autenticação de cadastro em sistemas eletrônicos. Nestes casos, é essencial que o titular seja exaustivamente cientificado das formas nas quais seus dados sensíveis são tratados para essa finalidade, através de avisos complementares de privacidade.

Esta hipótese excepcional somente pode ser utilizada para fundamentar interesses legítimos do controlador ou de terceiros, de modo que estes interesses não podem impactar de forma injusta ou desproporcional os direitos e liberdades dos titulares. É importante que as atividades baseadas nesta hipótese somente envolvam dados pessoais de titulares que já possuem alguma relação com a Unimed, sejam clientes, ex-clientes, colaboradores, etc.

O titular não pode “se assustar” com a atividade realizada sobre essa base legal. Ela deve, necessariamente, ocorrer dentro das legítimas expectativas dele. As atividades realizadas com base no interesse legítimo devem ser revisadas e avaliadas pelo Encarregado, que também deve aprovar o desenvolvimento de novos projetos que envolvam atividades deste tipo. A avaliação deve envolver a elaboração de Relatório de Impacto à Proteção de Dados, que deverá ser elaborado com o apoio do responsável pela atividade.

Em hipóteses excepcionais, a Unimed de Araçatuba coleta o consentimento do titular dos dados, o qual concede autorização mediante manifestação livre, espontânea,

inequívoca e para finalidades determinadas. Esta base legal deve ser utilizada apenas em último caso, uma vez que para tal, é necessário seguir todos.

## 7. Programa de privacidade Unimed de Araçatuba

Para que o programa de privacidade da Unimed de Araçatuba se mostre efetivo e produza resultados positivos, é importante que os pilares e procedimentos abaixo sejam constantemente observados durante as operações de tratamento de dados pessoais.

### 7.1. Gestão e Governança

#### 7.1.1. Responsáveis pelo Programa de Privacidade

A gestão e aplicação do programa de privacidade deverá ser conduzida pelos responsáveis abaixo.

Para facilitar o controle de conteúdo, datas de publicação e prazos para revisão, os documentos de governança relacionados à privacidade (incluindo esta política) devem ser controlados e gerenciados de forma centralizada pelo Comitê de Privacidade e pelo Encarregado de Proteção de Dados.

#### 7.1.2. Comitê de Privacidade

O Comitê de Privacidade deve se reunir quadrimestralmente, para apresentação e acompanhamento do programa de privacidade da Unimed de Araçatuba, e deve ser composto por um integrante da diretoria executiva, o Encarregado e integrantes de áreas-chave da Unimed de Araçatuba, capazes de deliberar e decidir sobre assuntos relacionados à privacidade e proteção de dados.

Adicionalmente, podem ser chamados, para deliberação de assuntos específicos representantes de áreas específicas envolvidas em atividades de tratamento de dados pessoais.

Os objetivos do comitê são, principalmente, garantir a comunicação do programa de privacidade, e discutir e tomar decisões sobre novas atividades de tratamento, com base nos riscos levantados através de Relatórios de Impacto à Proteção de Dados Pessoais.

- - -

Adicionalmente, o Comitê de Privacidade deverá sempre ser envolvido para tomar decisões a respeito de atividades de tratamento que envolvem riscos avaliados como altos. Caso o risco seja considerado muito alto, a decisão deverá ser escalada ao comitê de governança corporativa da Unimed de Araçatuba.

### 7.1.3. Encarregado de Proteção de Dados (DPO)

O Encarregado de Proteção de Dados (DPO) deve possuir conhecimentos jurídicos e técnicos relacionados à proteção de dados pessoais e experiência na área que sejam proporcionais ao nível de complexidade e sensibilidade das operações de tratamento de dados pessoais que a Unimed de Araçatuba realiza.

O Encarregado de Proteção de Dados deve gozar de um grau razoável de independência do restante da administração, de modo a lhe permitir assegurar os direitos dos titulares de dados cujos dados pessoais são tratados pela Unimed. Suas funções não devem incluir atividades ou responsabilidades que podem conflitar com a responsabilidade da Unimed de Araçatuba para com os titulares de dados pessoais.

A atuação do Encarregado de Proteção de Dados deve garantir a conformidade da Unimed de Araçatuba em relação às leis e demais normas de privacidade e proteção de dados aplicáveis aos seus negócios, através do programa de privacidade.

Suas principais atribuições envolvem:

- Gestão do programa de privacidade;
- Desenvolvimento, manutenção e revisão anual das normas e políticas de privacidade da organização, inclusive desta política;
- Fiscalização do cumprimento das normas e políticas de privacidade da organização;
- Monitoramento do nível de conformidade da organização, através de análises de diagnóstico semestrais, com a definição de planos de ação para melhorar o treinamento e a clareza das políticas de privacidade;
- Atuação como ponto de contato para Autoridade Nacional de Proteção de Dados - ANPD e os titulares dos dados;

- Recepção, junto ao Comitê de Privacidade, das eventuais requisições realizadas por titulares de dados pessoais, dando imediato atendimento a tais requerimentos, quando aplicável;
- Preparo dos Relatórios de Impacto à Proteção de Dados Pessoais, abaixo, com apuração e revisão dos riscos das atividades nele relatadas;
- Validação da nomeação de guardião de privacidade.

Cabe ao Encarregado a decisão, em casos de risco baixo a moderado, sobre as atividades de tratamento de dados pessoais conduzidas pela Unimed de Araçatuba. Caso o risco seja considerado alto, a decisão deverá ser escalada ao comitê executivo administrativo da Unimed.

Assim, o Encarregado deve auxiliar a esclarecer dúvidas e orientar demais membros da Unimed de Araçatuba, durante a execução de suas atividades, quando envolverem operações de tratamento de dados pessoais.

Por fim, como devidamente nomeado pela Diretoria Executiva, assume o cargo de Encarregado de Proteção de Dados o Colaborador Luiz Henrique dos Santos Matheus.

### *7.1.4.* Guardião da Privacidade

Os Guardiões da Privacidade são colaboradores nomeados para serem o ponto focal nas áreas de negócio da Unimed, a fim de facilitar o contato do Encarregado e do Comitê de Privacidade para com a área, e vice-versa.

Todas as decisões e comunicações do Encarregado e do Comitê de Privacidade direcionadas às áreas devem incluir os guardiões das respectivas áreas em cópia. Os guardiões não possuem poder decisório a respeito das operações de tratamento de dados pessoais.

As principais atribuições dos guardiões são:

- Distribuição e direcionamento das decisões e deliberações do Encarregado e do Comitê de Privacidade às suas respectivas áreas;

- Suporte na disseminação da cultura de privacidade, bem como na organização e condução de treinamentos sobre o programa de privacidade, voltados às suas respectivas áreas;
- Auxiliar na coleta de evidências sobre a aplicação e conformidade das regras do programa de privacidade em suas respectivas áreas;
- Auxiliar o Encarregado na elaboração de Relatórios de Impacto à Proteção de Dados referentes a atividades de suas respectivas áreas.

### 7.1.5. Registro de Operações de Tratamento de Dados Pessoais

A Unimed de Araçatuba manterá um registro de todas as suas operações de tratamento de dados pessoais, contendo, no mínimo, as seguintes informações sobre cada operação:

- Descrição do fluxo da informação em cada etapa de seu ciclo de vida (coleta, armazenamento, uso, compartilhamento – e neste caso, a finalidade para transferência – e descarte);
- Base legal para tratamento;
- Tipos de dados pessoais coletados;
- Finalidade para o qual o dado é tratado;
- Local lógico (nuvem, servidor, laptop etc.) e geográfico onde o dado é tratado;
- Período de retenção do dado;
- Área responsável pelo dado;
- Volume aproximado de registros existentes.

O Encarregado será responsável por manter o registro atualizado, bem como atribuir responsáveis para cada atividade registrada.

### 7.1.6. Tipos de Informações Geradas

| TIPO DE | SETOR GESTOR | UTILIZAÇÃO | LOCAL DE |
|---|---|---|---|

| INFORMAÇÃO | | | ARMAZENAMENTO |
|---|---|---|---|
| Dados pessoais colaboradores e médicos | Administração de pessoal; tecnologia da informação | Processo de admissão e demissão de colaboradores e cadastro no hospital | Data Center Hospital |
| Dados pessoais Pacientes / familiar | Same; GED; tecnologia da informação e segurança patrimonial | Prontuário de pacientes, cadastro no hospital e circulação de pessoas | Data Center Operadora<br>Data Center Hospital |
| Exames de imagem e diagnostico de pacientes | Imagem; tecnologia da informação; Same | Portuário de pacientes, atendimento clínico evolução clínica | Data Center Hospital<br>Data Center Pixeon |
| Dados de fornecedores e controle de estoque | Compras; almoxarifado; farmácia | Controle de fornecedores, produtos, estoque e compras | Data Center Hospital<br>Data Center Bionexo |
| Dados de faturamento e financias | Faturamento; custos; contabilidade e financeiro | Controle de financias do hospital | Data Center Hospital |

### 7.1.7. Utilização dos Dados Pessoais

Nas atividades da Unimed de Araçatuba e suas filiais que envolvem tramitação de dados pessoais, se faz necessária a padronização e a harmonização setorial quanto às respectivas intervenções, estabelecidas juntamente com o cooperados, beneficiários, colaboradores e terceiros.

Desse modo, todo e qualquer tratamento de dados pessoais, vinculados a pessoa, sejam sensíveis ou não, terá previsão de utilização adequada, a qual será definida pelos

documentos de apoio anexo a política de gestão de informações e proteção de dados pessoais, denominados de **Diretrizes de Tratamento de Dados Pessoais (UA.DA.CPL-001).**

### 7.2. Rede

#### 7.2.1. Cooperativa

O administrador de rede é o responsável pelo gerenciamento dos recursos da rede, integridade das informações e seus usuários, controles de acessos, cópias de segurança, otimização dos recursos, entre outros, conforme políticas internas do departamento de T.I.

- Não é permitido tentativas de obter acesso não autorizado, tais como tentativas de fraudar autenticação de usuário;
- A pasta "_Troca" localizada no drive M: do servidor deve ser utilizada para a transferência de arquivos entre estações de trabalho. Não deverá ser utilizada para armazenamento de arquivos sigilosos, por ser de domínio público da rede interna;
- Haverá exclusão periódica dos arquivos armazenados na pasta "_Troca" localizado no drive M: do servidor, de forma a liberar espaço em disco;
- É vedado qualquer tipo de alteração de layout das salas, trocar computadores e demais equipamentos de informática, sem aprovação e acompanhamento do departamento de T.I.;
- É vedado ao usuário compartilhar recursos do computador sem o acompanhamento do departamento de T.I.;
- É proibido utilizar os computadores, a rede corporativa, a Internet e outros recursos de T.I. para trabalhos particulares, em benefício próprio, de terceiros ou de quaisquer organizações alheias;
- O departamento de T.I. monitorará o desempenho computacional da rede por meio da verificação do seu uso adequado, bem como do inventário periódico dos softwares, aplicativos e programas instalados nas estações de trabalho, relatando

ao gerente do departamento, os desvios identificados, para que sejam tomadas as providências cabíveis;

- É proibido retirar das dependências da Unimed qualquer tipo de arquivo ou documento, seja digital ou físico, sem autorização prévia do gerente do departamento;
- O usuário que gravar qualquer arquivo que represente um documento da Unimed na unidade c: da estação de trabalho, deve estar ciente que não será realizado copias de segurança destes arquivos, pois o backup de segurança é realizado somente para os arquivos localizados nas unidades f: g: h: e m:
- Todo e qualquer arquivo gravado na unimed c: da estação de trabalho, será perdido na sua integra caso houver problemas na estação de trabalho que impeçam seu acesso, como por exemplo, problemas no disco rígido;
- Para todas as estações de trabalhos está disponível a possibilidade de monitoramento pelo departamento de T.I. por meio de acesso remota, onde é possível visualizar as atividades da sessão aberta pelo colaborador;
- Toda e qualquer navegação na internet assim como e-mails enviados e recebidos estão sendo monitorados constantemente pelo departamento de T.I. e podem ser auditado caso necessário.

### 7.2.2. Hospital

- Nossos processos utilizam dados pessoais de colaboradores, prestadores, fornecedores, terceiros; dados pessoais de pacientes e familiares; dados de faturamento da organização; controle de estoque entre outras informações digitais que são de cunho restritos e privados;
- Essas informações são alimentadas em nosso ERP MV2000i localizado em nosso data center, mas nem todos colaboradores tem acesso a todas informações, são designados acessos as informações conforme responsabilidade do cargo exercido;
- É feito backups diariamente para evitar perdas de informações, e também temos uma cópia replicada do nosso banco de dados na operadora de contingência;

- Nossa rede é controlada por um sistema de Firewall, que estabelece a política de segurança de navegação interna e externa da organização;
- Nossas máquinas são bloqueadas a entrada de pen-drives, CD-*ROM* de modo a evitar cópias indevidas de informações e entradas de malwares.

### 7.3. Mídias

- Quando uma determinada mídia for descartada, o conteúdo (dados) deverá ser excluído;
- Toda mídia deve ser guardada em ambiente seguro, de acordo com as especificações do fabricante;
- Não é permitida a retirada de mídias como fitas magnéticas da empresa. Caso seja necessário, deve existir prévia autorização do gerente do departamento, assim como mantido o registro dessa remoção como trilha de auditoria;
- A embalagem para transporte deve ser suficiente para proteger o conteúdo contra qualquer dano físico e deve ser feita de acordo com especificações dos fabricantes.

### 7.4. Arquivos e Backup

- O usuário é responsável por todos os arquivos que estejam armazenados em sua estação de trabalho;
- A utilização do serviço de armazenamento de arquivos na rede é de uso restrito aos interesses da empresa.
- É obrigatório armazenar os arquivos inerentes à empresa no servidor de arquivos para garantir o backup.
- Para a realização do backup é utilizado o método 3/2/1 sendo 3 cópias, em 2 lugares diferentes e 1 mídia diferente. O backup é realizado com granularidade;
- A primeira cópia dos arquivos da operadora é mantida no servidor de backup que fica localizado fisicamente nas instalações do datacenter do Hospital Unimed, quanto aos arquivos do Hospital, esses são mantidos em ambiente diverso do

principal em um cofre antichamas, em formato de "fita" gravadas no período noturno que é realizada de forma manual e evidenciada por meio de planilha;

- A segunda cópia dos arquivos da operadora é mantida no datacenter de uma empresa terceirizada e quanto aos arquivos do Hospital, esses são mantidos em um servidor de contingência localizado em ambiente diverso do servidor principal e do cofre antichamas, sendo realizado diariamente de forma automática;
- A terceira cópia dos arquivos da operadora é localizada em "nuvem" no provedor da empresa terceirizada e quanto aos arquivos do Hospital, esses são mantidos no servidor de backup que fica localizado fisicamente nas instalações do datacenter da operadora da Unimed;
- Caso o usuário necessite da restauração de arquivos que não estejam disponíveis na rede, deverá emitir solicitação pelo responsável da área;
- Como forma de evidenciar que o backup está sendo realizado de forma correta, foi criado um processo de teste de destore que é realizado semanalmente. Para registrar que o teste de destore foi realizado, foi criado uma planilha de monitoramento contendo a data de realização do destore, o colaborador que realizou, qual foi o arquivo restaurado, o status do processo e um campo de observação para relatar possíveis problemas.

### 7.5. Impressoras

- Não é permitido descartar impressões erradas na mesa das impressoras ou nas mesas próximas;
- Se você notar que o papel da impressora está no final, faça a gentileza de reabastecê-la. Isso evita que outras pessoas tenham seus pedidos de impressão prejudicados e evita acúmulo de trabalhos na fila de impressão;
- Evite a utilização de impressoras coloridas para a impressão de testes ou rascunhos. Se não for possível utilizar impressora laser, imprima em baixa qualidade (modo rascunho).

### 7.6. Estações de trabalhos

- É vedada a abertura de computadores para quaisquer tipos de reparos. Esta é uma tarefa exclusiva do departamento de T.I.;
- Não é permitida a instalação de quaisquer softwares e/ou pacotes aditivos aos softwares pré-instalados de quaisquer naturezas (licenciados ou não). Caso seja necessário, contatar o departamento de T.I.;
- Não é permitido o armazenamento de arquivos MP3, filmes, fotos e softwares com direitos autorais ou qualquer outro tipo de pirataria;
- Ao ausentar-se do seu local de trabalho, o usuário deverá bloquear a estação de trabalho por meio de senha e se possível fechar todos os programas e efetuar logout/logoff da rede, evitando acesso de pessoas não autorizadas;
- Não é permitido instalar ou utilizar nenhum tipo de jogo na estação de trabalho, ou qualquer outro tipo de atividade incompatível com o trabalho dentro da empresa;
- Não é permitido que se configure senhas de quaisquer tipos na inicialização do computador. Se necessário, entre em contato com o departamento de T.I., e solicite a adição das senhas. Essas devem ser de conhecimento do departamento de T.I.;
- Nos casos de travamento do computador ou sistema, entre em contato com o departamento de T.I. relatando o fato;

### 7.7. Senhas

- As senhas são individuais/pessoais e não devem ser compartilhadas nem mesmo com um membro da sua equipe ou da informática, mantendo assim a confidencialidade das mesmas. Caso desconfie que sua senha não está mais segura, entre em contato com o departamento de T.I. para mudá-la;
- Tudo que for executado com sua senha é de sua inteira responsabilidade, por isso tome todas as precauções para mantê-la secreta;
- Por questões de segurança se o usuário não estiver autenticado na rede, não será possível a utilização do sistema de gestão;

- - -

- Por precaução, memorize sua senha, nunca anote em papel e nunca mantenha gravada em arquivos.
- No momento da criação de sua senha, sugere-se que essa contenha no mínimo 10 caracteres, letra maiúsculas e minúsculas, número e caractere especial, por exemplo, *Unimed100%*.
- Para segurança dos sistemas internos, sugere-se que o usuário faça o controle de suas senhas e que essa seja atualizada a cada 6 meses, caso o sistema não tenha uma padronização diferente dessa definida.

### 7.8. Vírus e Códigos Malicioso

- Seu antivírus será atualizado automaticamente toda vez que o fornecedor gerar uma nova atualização do antivírus. Para isso, é indispensável que toda vez que o computador for ligado, o usuário acesse a rede por meio de login e senha;
- É vetada a utilização de disquetes, pen-drives, aparelhos mp3 ou CDs externos à Unimed, com exceção aos computadores com autorização do departamento de T.I. Se necessário, o usuário deverá emitir solicitação formal assinada pelo supervisor(a) do departamento ao departamento de T.I.
- Reporte atitudes suspeitas em seu sistema ao departamento de T.I., para que possíveis vírus possam ser identificados no menor espaço de tempo;
- Desconfie de softwares que você clica e não acontece “nada”;
- Caso seu computador estiver infectado por vírus, ou receba alguma nota alertando sobre vírus, reporte a situação para o Departamento de Tecnologia da Informação.

### 7.9. Energia

É terminantemente proibido utilizar “*benjamins*” ou “*T*” para ligar equipamentos de informática e demais equipamentos eletro/eletrônicos.

### 7.10. Custódia de *Software* e *Hardware*

Quaisquer *softwares* adquiridos pela Unimed de Araçatuba ficarão sob guarda e responsabilidade do Departamento de Tecnologia da Informação, bem como sua instalação e suporte

### 7.11. Material Inapropriado ou Ofensivo

É proibido acesso ou distribuição de materiais que possam ser considerados inapropriados, ofensivos, ou desrespeitosos a outros como:

- Material que contenha imagens ou descrições pornográficas;
- Material que defenda ou incite intolerância a outras pessoas (por exemplo, racismo);
- Material que defenda ou incite atividades ilegais;
- Material que ofenda credos, ritos ou religiões;
- Material que promova e ou incentive o trabalho escravo e/ou infantil;
- Material que propague ideias de degradação ao meio ambiente;
- Direitos Autorais (Copyright) e Lei de Propriedade Intelectual;
- As informações e softwares disponíveis em domínio público (incluindo a internet) estão sujeitas à proteção de Copyright ou outros direitos de propriedade intelectual. Portanto, não obtenha softwares, imagens, etc. (downloads) destas fontes para uso na Unimed, a não ser que haja uma permissão explícita e formal por parte do proprietário do material, e fica proibido o uso de qualquer foto, imagem ou desenho que possua uma marca registrada de terceiro, devido a questões legais.

### 7.12. *Internet*

- A Unimed de Araçatuba fornecerá acesso à Internet aos usuários autorizados, que receberão uma conta (login/senha) de acesso. Este acesso deverá ser utilizado exclusivamente como ferramenta de trabalho e usado com responsabilidade, tendo em vista os riscos envolvidos em segurança e produtividade;

- É proibido o uso de programas de mensagens instantâneas como Skype ou equivalentes. Caso tenha autorização para utilizar estes programas, deverão ser utilizados para uso exclusivo em serviço. Não realize envio de informações que caracterize atividade corporativa ou comercial;
- Caso haja necessidade, a Unimed de Araçatuba oferece um programa (PSI) e seu uso deve seguir as mesmas regras aplicadas ao Correio Eletrônico.

### 7.13. Correio Eletrônico

- A Unimed de Araçatuba disponibilizará o uso de seu servidor de Correio Eletrônico a todos os usuários autorizados, que receberão uma conta de correio eletrônico padronizada em um mesmo domínio da Internet da seguinte forma: usuario@unimedaracatuba.com.br;
- O serviço de Correio Eletrônico deve ser utilizado somente nas atividades profissionais, sendo restrito aos interesses da Unimed de Araçatuba;
- É proibido forjar quaisquer informações do cabeçalho do remetente, fazendo-se passar por outra pessoa;
- Não é permitida má utilização da linguagem em e-mails comerciais, tais como abreviações de palavras (Ex: “tbm”, “pq”, “vc”), gírias;
- Evite enviar anexos muito grandes, pois sobrecarregam o serviço de Correio Eletrônico. O departamento de T.I. restringe o tamanho destes anexos de acordo com a capacidade de utilização do serviço. Caso necessário o envio de arquivos maiores, contate o departamento de T.I.;
- É obrigatória a utilização de assinatura nos e-mails com o seguinte formato, não devendo conter mensagens pessoais nela inseridas:

| |
|---|
| Nome do Funcionário<br>Função<br>Tel.: (XX) XXXX-XXXX<br><logo unimed><br>http://www.unimedaracatuba.com.br |

- - -

Endereço Unimed Araçatuba

- Desconfie de mensagens recebidas de origem desconhecida ou em outros idiomas. Evite ao máximo abrir estas mensagens e exclua-as imediatamente;
- Não abra em nenhuma circunstância anexos de e-mails não confiáveis, não solicitados ou de cartões virtuais, pois eles podem conter vírus ou outros programas maliciosos;
- Da mesma forma, não clique em links para páginas ou arquivos na Internet por sugestão de e-mails recebidos. Órgãos como a Receita Federal, SERASA ou Bancos não enviam estas mensagens;
- Não envie como anexo qualquer software ou dados de propriedade da Unimed ou de seus clientes, sem expressa autorização da gerência responsável;
- Em caso de dúvida sobre alguma mensagem recebida, verifique a veracidade dos fatos com o seu autor ou solicite ajuda do Suporte de Informática;
- Lembre-se que o simples envio de um e-mail não garante o recebimento pelo destinatário. Quando for de suma importância, peça a resposta confirmando o recebimento do mesmo. Não confie nas respostas de confirmação automáticas, pois não são eficientes.

## 7.14. Sistemas Informatizados

- O acesso aos recursos informatizados, bem como o bloqueio destes;
- O acesso às informações que não são obtidas por meio de recursos disponíveis nos sistemas informatizados deverá ser solicitado ao departamento de Tecnologia da Informação, formalmente pelo supervisor(a) do departamento requisitante;
- Processos padronizados de identificação e avaliação das ameaças, impactos e vulnerabilidades da informação e dos sistemas são realizados periodicamente, promovendo:

    - Alertas de falhas nos sistemas;

- Registro dos acessos concedidos ou não, identificação da estação de trabalho, bem como a identificação do usuário;

- Há monitoramento dos principais recursos dos equipamentos, tais como, processadores, memória, área de armazenamento, dentre outros, a fim de garantir a disponibilidade da capacidade adequada de processamento e armazenamento das informações processadas;
- Para os sistemas próprios são armazenados os códigos fonte, bibliotecas, documentações e versões em produção. Para os sistemas desenvolvidos por terceiros são armazenadas as versões em produção;
- A aplicação de novas versões, dependendo do impacto das modificações, somente são realizadas em horários programados após a homologação das implementações pelo analista responsável, que se certifica por meio de testes realizados em ambiente próprio, que as modificações estão de acordo com o esperado e que tanto as informações quanto os sistemas não serão comprometidos com a mudança de versão, mantendo deste modo a integridade dos processos dos negócios envolvidos;
- Os acessos remotos no período de expediente da instituição, realizados pelos colaboradores, são permitidos quando autorizado pelo setor de departamento pessoal, tendo em vista as necessidades emergenciais como, por exemplo, problema predial, doença endêmica ou pandêmica, onde a solicitação é realizada ao setor de Tecnologia da Informação.
- Os sistemas e aplicações internas são desenvolvidos seguindo normas e padronizações do departamento de T.I.

## 7.15. Servidores

- O acesso à sala de servidores é restrito e a chave de acesso está resguardada pela equipe de T.I.;
- Ao acessar a sala do servidor, colaborador deve registrar sua entrada por meio de uma planilha que fica disponível dentro da sala. Esta planilha foi criada para

monitorar quem está acessando a sala do servidor, a data de acesso, o horário de entrada e o horário de saída;

- Existe uma planilha para cada sala de servidores.

### 7.16. Câmeras de segurança

- Existem câmeras de segurança para realizar o monitoramento das dependências da instituição, situadas em pontos estratégicos, com avisos de existência;
- A análise do funcionamento de cada câmera é realizada diariamente e evidenciada por meio de uma planilha através do departamento de tecnologia da informação. A planilha foi criada para monitorar o colaborador que está analisando a câmeras, a data de análise, o *status* geral das câmeras e um campo observação para descrever qual câmera que está com problema.
- Em decorrência de adversidades externas ou interna nos ambientes da Unimed de Araçatuba e de suas filiais, um terceiro interessado poderá ter acesso as imagens da câmera mediante solicitação formal ao departamento jurídico através de oficio do órgão público responsável pela investigação.

### 7.17. Padronização no processo de cadastro

- Regras de obrigatoriedade, validações, tamanho de campos e advertências criam um ambiente padronizado para os processos de cadastro evitando falhas e possíveis erros.

### 7.18. Penalidades

- O não cumprimento desta política, após as devidas averiguações, poderá ensejar as seguintes medidas:
  a. Advertência verbal;
  b. Advertência por escrito;
  c. Suspensão por tempo determinado;
  d. Demissão por justa causa, nos termos do artigo 482 da CLT;

- - -

e. Rescisão contratual do prestador de serviços, sem prejuízo do ingresso de eventuais ações judiciais pertinentes, no caso de colaboradores sem vínculo empregatício;

f. Além das medidas acima, poderá haver bloqueio e/ou encerramento do acesso ao sistema, rede, e-mail, Internet entre outros recursos de T.I.

### 7.19. Tabela de Temporalidade

A retenção dos dados não deve ultrapassar o período estabelecido na tabela de temporalidade documental, conforme anexo 1 (Tabela de Temporalidade - UA.TAB.CPL-001) e os programas de gestão de documentos presentes no sistema GED, por sua vez, deve estar sempre atualizada com os prazos legais e prescricionais aplicáveis para estabelecimento do período de retenção.

## 8. Transparência

Todas as operações envolvendo atividades de tratamento de dados e informações de titulares externos (terceiros/parceiros/clientes), deverão observar o Aviso de Privacidade, contidos no contrato com cláusula especifica.

Todas as operações envolvendo atividades de tratamento de dados pessoais de titulares internos (funcionários/colaboradores/ cooperados), deverão observar o Aviso Interno de Privacidade, contidos no contrato de trabalho e definidos em ata de reunião dos cooperados.

Além disso, caso a Unimed de Araçatuba promova atividade que envolve o tratamento de dados pessoais de formas que excepcionalmente não se enquadram no respectivo Aviso de Privacidade, e caso, em razão disso, o respectivo Aviso não contenha informações claras e suficientes sobre os pontos elencados abaixo, aplicáveis a esta atividade, será necessária a apresentação de aviso específico para complementação das informações fornecidas ao titular, devendo ser validado pelo Encarregado, setor responsável e Diretoria e disponibilizado antes que os dados pessoais sejam efetivamente tratados:

- Escopo da atividade;
- Quais os dados envolvidos na atividade;
- Finalidade da atividade de tratamento;
- Forma e duração do tratamento;
- Descrição da forma de coleta, utilização, armazenagem e descarte das informações;
- Informações sobre os agentes de tratamento envolvidos na atividade; e
- A eventual existência de decisões automatizadas incorporadas na atividade.

## 9. Consentimento

O consentimento somente poderá embasar atividades de tratamento de dados pessoais em casos excepcionais. Nestes casos, o Encarregado deverá ser consultado para confirmar quanto à exigência de consentimento para a atividade, e a impossibilidade de seu enquadramento em outras bases legais, bem como revisar a forma de coleta do consentimento se aplicável, que deverá observar os pontos a seguir:

- Manifestação livre: O titular deve fornecer o consentimento de maneira livre, sem que seja obrigado para tanto para, por exemplo, usufruir do serviço/produto relacionado.

Exemplo:

| Consentimento Forçado | Consentimento Livre |
|---|---|
| "Ao utilizar a plataforma, você consente com a utilização de seus dados pessoais para fins de *marketing*." | □ "Gostaria que meus dados pessoais sejam utilizados para o envio de comunicações de marketing pela Unimed." |

- Manifestação granular: O titular forneceu a sua autorização (consentimento) para que fosse realizado o tratamento em situações específicas e determinadas.

- - -

Exemplo:

| Consentimento Genérico | Consentimento Granular |
|---|---|
| □ "Gostaria que meus dados pessoais sejam utilizados para fins de *marketing*." | □ "Aceito que meus dados pessoais sejam utilizados para fins estatísticos, para melhorias da plataforma da Unimed.<br>□ Aceito que os dados estatísticos mencionados acima sejam utilizados para personalizar minha experiência na utilização da plataforma da Unimed. |

- Manifestação informada: O titular, teve acesso ao aviso de privacidade correspondente a atividade na qual foi sujeitado, antes do fornecimento de sua autorização, garantindo possuir plena ciência da finalidade e dos limites da atividade de tratamento realizada.
- Manifestação inequívoca: O titular forneceu os seus dados pessoais, sem qualquer dúvida ou questionamento quanto aos limites da atividade.

Ainda, para garantir que o consentimento foi coletado de maneira correta, possibilitando inclusive a demonstração deste fator tanto ao próprio titular como para a Autoridade Nacional de Dados Pessoais, bem como para garantir ao titular o direito à revogação do consentimento, a UNIMED realizará a documentação, o armazenamento e a gestão da autorização concedida, por meio de controle técnico e específico de gestão de consentimento.

## 10. Relatório de impacto à proteção de dados pessoais

Os relatórios de impacto à proteção de dados pessoais são documentos que contêm a descrição dos processos que envolvem o tratamento de dados pessoais que, por sua natureza, são passíveis de gerar riscos às liberdades civis e individuais dos

titulares dos dados pessoais. A elaboração deste documento será exigível em especial quando:

- Da realização de operações de tratamento de dados pessoais sensíveis; e
- Da realização e condução de operações que, por sua natureza, realizem o tratamento de dados críticos, passíveis de gerar altos riscos aos titulares de dados pessoais em caso de ocorrência de incidentes envolvendo tais informações;
- A operação de tratamento de dados pessoais estiver amparada na base legal do interesse legítimo.

Em caso de necessidade de elaboração deste documento, a obrigatoriedade primária de elaboração será do gestor da área responsável pela operação, tendo o Encarregado pela proteção de dados pessoais da Unimed de Araçatuba, o papel primordial de avaliar o documento preparado por este gestor e elaborar um parecer final sobre a atividade de tratamento.

Ainda, o Encarregado da Unimed de Araçatuba disponibilizará um modelo específico a ser seguido, o qual, dentre outras coisas, conterá:

- a descrição dos tipos de dados coletados;
- a metodologia utilizada para a coleta e para a garantia da segurança das informações; e
- na análise do controlador com relação a medidas salvaguardas e mecanismos de mitigação de risco adotados.

Para auxiliar os gestores de cada área da Unimed de Araçatuba a identificarem a necessidade de elaboração deste relatório, bem como auxiliá-los no momento de preparação deste documento, foi criado um guia prático sobre o tema, disponível na pasta eletrônica no Sigquali com a rastreabilidade **UA.FOR.CPL-008 CALCULO DO RISCO NO TRATAMENTO DOS DADOS PESSOAIS**.

- - -

Via de regra, tais documentos não deverão ser publicados ou disponibilizados, contudo, poderão ser objeto de requisição da Autoridade Nacional de Proteção de Dados Pessoais, a qualquer tempo.

## 11. Direitos dos titulares

Em toda atividade de tratamento de dado pessoal, a Unimed de Araçatuba deverá buscar garantir os direitos dos titulares abaixo. Em todos os casos, a identidade dos titulares requerentes deverá ser verificada, e o atendimento deverá ocorrer sob a orientação do Encarregado.

Com relação ao recebimento de requisições de exercício dos direitos dos titulares, a Unimed de Araçatuba possui um canal aberto e direcionado aos funcionários da empresa, disponível por meio do endereço eletrônico: dpo@unimedaracatuba.com.br. Ainda, caso estes direitos pretendam ser exercidos por clientes, parceiros ou terceiros que possuam dados pessoais sob o escopo de tratamento da Unimed de Araçatuba; a Unimed de Araçatuba possui um canal específico direcionado para tanto, disponível por meio do endereço eletrônico: dpo@unimedaracatuba.com.br.

Eventual decisão de recusa no atendimento às requisições de titulares deverá ser validada pelo Encarregado.

### 11.1. Direito à Informação e ao Acesso

Ao usuário titular, mediante sua expressa requisição, é garantido o direito de confirmação da existência de tratamento de seus dados pessoais. A Unimed utilizará meios eficazes, cuja gestão e operacionalização será supervisionada pelo Encarregado, para fornecer cópia dos dados pessoais, mediante requisição do titular, por meio eletrônico, seguro e idôneo para esse fim ou sob forma impressa.

Se em formato simplificado, o conjunto de dados deve ser entregue imediatamente.

Se exigido de forma completa, deverá ser fornecido no prazo de até 15 (quinze) dias úteis, contado da data do requerimento do titular contendo as informações que seguem:

- Inexistência de registro;
- Origem dos dados;
- Critérios utilizados;
- Finalidade do tratamento.

Para os casos em que o tratamento tiver como origem o consentimento do titular ou contrato celebrado com o titular, este poderá solicitar cópia eletrônica integral de seus dados pessoais em formato que permita a sua utilização subsequente, inclusive em outras operações de tratamento.

### 11.2. Direito a Retificação

O titular terá o direito de obter, a qualquer momento e mediante requisição, a correção de seus dados pessoais, quando incompletos, inexatos ou desatualizados.

### 11.3. Direito à exclusão, anonimização e bloqueio dos dados pessoais

O titular terá o direito de obter, a qualquer momento e mediante requisição, a eliminação, a anonimização ou o bloqueio de seus dados pessoais, quando as informações objeto de requisição se mostrarem excessivas, ou o tratamento dado pelo controlador estiver em desconformidade com as determinações da LGPD.

Em hipótese de ocorrência de requisições de eliminação de dados pessoais, a Unimed de Araçatuba, considerando que nenhum direito possui caráter absoluto, deverá verificar se o tratamento dos dados objeto de requisição se justifica em algumas das hipóteses abaixo, caso em que a solicitação e, por consequência, o direito do titular dos dados não deverá prevalecer:

- Cumprimento de obrigação legal ou regulatória;

- Estudo por órgão de pesquisa;
- Transferência a terceiro, desde que respeitados os requisitos de Tratamento de dados dispostos em lei; ou
- Uso exclusivo do controlador, vedado seu acesso por terceiros, e desde que os dados sejam mantidos anonimizados.

### 11.4. Direito à Oposição

É garantido ao titular o direito de, a qualquer momento e mediante requisição, opor-se ao tratamento de seus dados pessoais, quando a base legal que originou o tratamento não for o consentimento. Neste mesmo sentido, este direito só será garantido e exercível quando a Unimed deixar de observar e cumprir algumas das disposições trazidas na legislação que trata sobre o tema.

### 11.5. Direito à portabilidade

O titular tem direito de, a qualquer momento e mediante requisição, solicitar a portabilidade dos seus dados pessoais a outro fornecedor de serviço ou produto. Para tal, recomendamos que os dados pessoais do titular requerente sejam desvinculados de dados de outros titulares, e fornecidos em formato Interoperável, tal como .XLS, .CSV ou .JSON.

### 11.6. Direitos atrelados ao consentimento

O titular tem direito de, a qualquer momento e mediante requisição, solicitar informação sobre a possibilidade de não fornecer consentimento e as consequências de sua negativa, bem como de revogar o consentimento anteriormente fornecido.

## 12. Compartilhamento de dados pessoais com terceiros

Na hipótese da Unimed de Araçatuba objetivar a transferência ou o compartilhamento de dados pessoais para terceiros (“operadores”), para a prestação de

um serviço específico ou atendimento de uma demanda pontual, a instituição deverá, necessariamente:

- Celebrar instrumentos contratuais robustos: capazes de garantir a integridade e a confiabilidade das informações compartilhadas, bem como o respeito às normas específicas relativas à privacidade e proteção de dados pessoais, com a utilização do banco cláusulas-padrão, que deverá ser anualmente validado e revisado pelo Encarregado, e aplicado seguindo o Procedimento de Contratos da Unimed de Araçatuba (UA.PRS.JUR-001 – Versão 00), bem como a seguinte matriz:

| Modalidade de Contrato | Cláusula Aplicável |
|---|---|
| Contratos com fornecedores | Conforme avaliação do Departamento Jurídico com a validação do Encarregado |
| Minutas Padrão com Operadores de Dados Pessoais | Cláusula Padrão Completa, sem apêndice |
| Minutas Padrão com Controladores de Dados Pessoais | Cláusula Padrão Completa, com apêndice |
| Pedidos de Compra | Cláusula Padrão Simplificada |

### 12.1. Transferência internacional de dados pessoais

Na hipótese de transferência de dados pessoais para países estrangeiros, a Unimed de Araçatuba deverá adotar uma das salvaguardas a seguir, necessárias para garantir a integridade, a disponibilidade e a confidencialidade dos dados pessoais, conforme regulações da Autoridade Nacional de Proteção de Dados.

- Caso os dados pessoais sejam transferidos para países com níveis de proteção de dados pessoais considerado como adequado pela ANPD.
- Quando a Unimed de Araçatuba fornecer salvaguardas adequadas, no formato de:
  - Cláusulas contratuais específicas para determinada transferência;
  - Cláusulas-padrão contratuais;

- - -

- Normas corporativas globais; e
- Selos, certificados e códigos de conduta regularmente emitidos.

- Caso coletado o consentimento específico do titular de dados pessoais;
- Quando exigido por Lei para a tutela da saúde e demais circunstâncias específicas; ou
- Quando expressamente autorizado pela Autoridade Nacional de Dados Pessoais.

## 13. Responsabilidades

Para que a presente Política produza os efeitos pretendidos, é de grande importância que todos os colaboradores, gestores, diretores, funcionários, prestadores de serviços, dentre outros, observem as disposições contidas neste documento, levando em consideração que os atos de quaisquer colaboradores da Unimed de Araçatuba poderão repercutir para a Unimed como um todo, produzindo efeitos de magnitudes não previsíveis.

Assim, com o apoio dos responsáveis, para a garantia do cumprimento das normas de privacidade e proteção de dados pessoais, os pontos a seguir devem ser observados por todos, sem prejuízo dos demais pontos desta política:

- Os colaboradores possuem como dever primário o de garantir a integridade, disponibilidade e confidencialidade dos dados pessoais tratados no exercício de sua função;
- O tratamento dos dados pessoais deverá, necessariamente, observar as finalidades propostas, não permitido o tratamento incompatível ou excessivo ou para finalidades diversas, sem que haja a expressa autorização da Unimed de Araçatuba, o qual previamente validou esta nova finalidade com o titular das informações.
- O colaborador deverá se utilizar do mínimo de informações necessárias para o cumprimento das finalidades pretendidas e regular exercício de suas funções.
- Os dados pessoais tratados no exercício da função deverão necessariamente ser armazenados em local seguro e oficialmente aprovados pela Unimed de

Araçatuba, sendo vedado o armazenamento não autorizado em ambientes próprios, como *notebooks* ou área de trabalho de computadores.

- Os dados pessoais tratados no exercício da função não poderão ser apagados, deletados ou anonimizados, sem que haja comando direto da Unimed de Araçatuba para tanto.
- Os dados pessoais tratados no exercício da função, como regra, não poderão ser enviados para endereços de e-mail pessoal ou dispositivos remotos como pen drives.

Feitas as recomendações básicas necessárias, todos os colaboradores da Unimed de Araçatuba terão à disposição o atendimento do Encarregado de Proteção de Dados Pessoais da Unimed.

## 14. Treinamentos

Todos os membros da Unimed de Araçatuba e filiais que estejam envolvidos nas atividades de tratamento de dados pessoais, não importando o nível hierárquico que ocupe, deverá receber treinamentos periódicos, decididos pelo Comitê de Privacidade e organizado pelo Encarregado conjuntamente com o departamento de Treinamento e Desenvolvimento, especificamente sobre:

- Conceitos gerais de Privacidade e Proteção de Dados, incluindo a apresentação desta política e de materiais de estudo sobre os princípios da LGPD; e
- Conceitos específicos de Privacidade e Proteção de Dados, aplicados às atividades de cada área.

O treinamento dessa política necessariamente deverá fazer parte do processo de mentoria de todos os novos colaboradores e também suas diretrizes deverão ser compartilhadas no processo de integração de novos colaboradores da Unimed de Araçatuba e filiais.

## 15. Incidentes de privacidade

Incidentes de vazamento de dados podem ser definidos como qualquer falha na observância dos pontos descritos nesta política, que podem gerar risco ou danos aos titulares de dados pessoais.

A Unimed de Araçatuba manterá um canal público para recebimento de notícias de incidentes, que pode ser utilizado, também, pelos seus membros e colaboradores, essas comunicações serão recebidas pelo Encarregado (dpo@unimedaracatuba.com.br), que verificará o ocorrido e procederá à aplicação do Protocolo.

Esse protocolo consiste no Plano de Respostas a Incidentes que é a abertura de uma RNC (Relato de Não Conformidade) para o departamento, a fim de descobrir a fundo o ocorrido e ver as medidas contingência que foram adoradas e com isso a abertura do CID, afim de dar, na medida da necessidade e obrigatoriedade legal a transparência do ocorrido.

## Gestão de consequências

Colaboradores, fornecedores ou outros *stakeholders*, que observarem quaisquer desvios às diretrizes desta Norma, poderão relatar o fato ao Canal de Denúncia, localizado no site da Instituição (https://unimedaracatuba.coop.br/), podendo ou não se identificar.

Internamente, o descumprimento das diretrizes desta norma enseja a aplicação de medidas de responsabilização dos agentes que a descumprirem conforme a respectiva gravidade do descumprimento.

Situações excepcionais serão encaminhadas para a Diretoria Executiva e/ou demais órgãos de Governança.

## Indicadores - Efetividades

- **ÍNDICE DE BLOQUEIO DE TENTATIVA DE INVASÃO**
  - **Conceito**: Monitora as tentativas de invasão aos sistemas internos.
  - **Fórmula de Cálculo:** Número de tentativas bloqueadas / Total de tentativas de invasão) * 100.
  - Meta: 100%.
- **PERCENTUAL DE COMPLIANCE EM LGPD**
  - **Conceito:** Monitorar e analisar como está o desenvolvimento da aplicação da lei geral de proteção de dados da unimed.

- - -

- **Fórmula de Cálculo:** Quantidade de Chamadas não resolvidas que envolve LGPD/Quantidade de Chamadas que envolve LGPD * 100
- Meta: 100%.

- **PERCENTUAL DE RESOLUTIVIDADE – PROTOCOLO CID**
  - **Objetivo:** Monitorar e analisar como está o desenvolvimento da aplicação da lei geral de proteção de dados da unimed.
  - **Fórmula de Cálculo:** (Quantidade de protocolos CID concluído sem danos graves/Quantidade de protocolos CID Aberto) * 100

## Disposições finais

Sem prejuízo das disposições contidas nesta política, a Unimed de Araçatuba se reserva ao direito de revisá-la, na periodicidade que melhor entender, sempre respeitando o prazo máximo de 2 (dois) anos.

## Referências bibliográficas

- BRASIL. Lei Federal nº 12.965 de 23 de abril de 2014. Marco Civil da Internet. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acessado em: 10/03/2022;
- BRASIL. Lei Federal nº: 13.709 de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acessado em: 10/03/2022;
- BRASIL. Lei Federal nº: 12.551 de 15 de dezembro de 2011. Altera o art. 6º da Consolidação das Leis do Trabalho (CLT), aprovada pelo Decreto-Lei nº 5.452, de 1º de maio de 1943, para equiparar os efeitos jurídicos da subordinação exercida por meios telemáticos e informatizados à exercida por meios pessoais e diretos. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12551.htm. Acessado em: 10/03/2022;
- BRASIL. Lei Federal nº: 9.609, 19 de fevereiro de 1998. Dispõe sobre a proteção da propriedade intelectual de programa de computador, sua comercialização no País, e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9609.htm. Acessado em: 10/03/2022;
- BRASIL. Decreto Lei nº: 7.962 de 15 de março de 2013. Regulamenta a Lei nº 8.078, de 11 de setembro de 1990, para dispor sobre a contratação no comércio eletrônico. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/decreto/d7962.htm. Acessado em: 10/03/2022;
- BRASIL. Decreto Lei nº: 7.845 de 14 de novembro de 2012. Regulamenta procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo, e dispõe sobre o Núcleo de Segurança e

Credenciamento. Disponível em http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/decreto/d7845.htm. Acessado em: 10/03/2022;

- BRASIL. Lei Federal nº: 10.406 de 10 de janeiro de 2002. Institui o Código Civil. Disponível em http://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Acessado em: 10/03/2022;
- BRASIL. Constituição (1988). Constituição da República Federativa do Brasil. Brasília, DF: Senado Federal: Centro Gráfico, 1988. Acessado em: 10/03/2022;
- CONSELHO FEDERAL DE MEDICINA. Resolução CFM nº: 1.821 de 23 de novembro de 2007. Aprova as normas técnicas concernentes à digitalização e uso dos sistemas informatizados para a guarda e manuseio dos documentos dos prontuários dos pacientes, autorizando a eliminação do papel e a troca de informação identificada em saúde. Disponível em https://sistemas.cfm.org.br/normas/visualizar/resolucoes/BR/2007/1821. Acessado em: 10/03/2022;

## Controle de Alterações

| Data | Versão | Alteração |
|---|---|---|
| 01/09/2020 | 0 | 1° emissão. |
| 06/09/2021 | 1 | Atualização Lei Geral de Proteção de Dados. |
| 15/12/2021 | 2 | Atualização dos apontamentos da auditoria da RN 277 nos itens I.B.2.iii Armazenamento de dados pessoais e no item I.A.2.iii – Confidencial. |
| 10/02/2022 | 0 | - Alterada a rastreabilidade da política, pois essa política será de responsabilidade do setor de compliance e não mais do jurídico.<br>- Alteração no controle de alterações conforme apontamento da ISO 9001.<br>- Alteração da Rastreabilidade passando a política do departamento jurídico para o compliance.<br>- Inclusão da gestão de consequências na política.<br>Atualização dos apontamentos da Consultoria alterando e criando os seguintes itens:<br>- I.A.8.iii – Descrição do plano de contingência;<br>- I.A.8.iv – Extensão do item e remanejamento do conteúdo para o item I.A.2.iii e IV;<br>- V.B.5 – Exclusão das citações políticas extintas;<br>- V.B.15 – Alteração para inclusão da citação do item I.A.3 e adequação da realizada da Unimed;<br>- V.B.15.g – Melhorar a definição do acesso remoto;<br>- V.B.20 – Inclusão do item, contendo a definição da tabela de temporalidade<br>- IV.D – Inclusão da citação da diretriz de controle de qualidade de dados;<br>- Inclusão da Referência Bibliográfica;<br>- Alteração da renovação para 2 anos. |
| 10/03/2022 | 1 | - Revisão textual baseado no manual de redação do sistema unimed;<br>- Revisão baseado no modelo interno da Unimed de Araçatuba de política;<br>- Alteração da periodicidade do comitê de privacidade de bimestral para quadrimestral.<br>- Atualização do item I.A.2, I.A.3.ii e I.A.3.iii;<br>- Atualização do item VII.<br>- Higienização do conteúdo redundantes:<br>- V.B.3;<br>- V.B.4;<br>- V.B.5;<br>- V.B.7;<br>- V.B.13;<br>- V.B.14;<br>- V.B.15; |

- - -

| | | |
|---|---|---|
| | | - Exclusão:<br>- I.A.8<br>- Inclusão:<br>- I.A.3.iv<br>- I.A.4.i<br>- I.A.4.ii<br>- I.A.4.iii |
| 05/09/2024 | 02 | - Atualização do nome da política de Política Interna de Gestão de Informações e Proteção de Dados Pessoais para Política Institucional de Gestão das Informações e de Proteção e Privacidade dos Dados;<br>- Atualização do modelo do documento;<br>- Atualização do documento conforme o manual metodológico da Unimed de Araçatuba;<br>- Atualização item 7.16 e 7.18.<br>- Atualizações por conta do PNGPPD – Programa Nacional de Governança em Proteção e Privacidade de Dados<br>- item 7.1.3 – Encarregado<br>- item 7.4 - Arquivos<br>- item 7.7 - Senhas<br>- item 7.13 – Correio Eletrônico<br>- item 7.18 - Penalidade<br>- item 10 - Relatório de impacto à proteção de dados pessoais<br>- item 14 - Treinamentos |
| 06/11/2024 | 000 | Atualização do modelo do documento e mudança de local de repositório, passando a ser publicado no MV SOUL. |

| |
|---|
| **ELABORADO POR: Fabio Junio Pereira, Luiz Henrique dos Santos Matheus - Supervisor de Compliance, Assistente de Compliance.** |
| **ELABORADO EM:** 01/09/2020 |
| **REVISADO POR: Fabio Junio Pereira, Luiz Henrique dos Santos Matheus - Supervisor de Compliance, Assistente de Compliance.** |
| **VERIFICADO POR: BRENO PESSOA FILETI - Auxiliar da Qualidade** |
| **APROVADO POR: FLAVIO R GARBELINI DE OLIVEIRA, MARCIO RODRIGO DOMINGOS, RODRIGO PROTTE PEDRO, LUIS CESAR GABAS - Presidente, Vice Presidente, Superintendente, Diretor Técnico -** |
| **PUBLICADO POR: BRENO PESSOA FILETI - Papel: GE - QUALIDADE - Auxiliar da Qualidade** |

- - -