POLÍTICA GERAL DE PROTEÇÃO DE DADOS PESSOAIS

Versão 1.0

1. Introdução

1.1. A Unimed Araxá tem como missão proporcionar aos seus usuários a segurança e a certeza de que receberão por parte dos médicos cooperados, funcionários, hospitais e laboratórios credenciados um atendimento humanizado, diferenciado e que prime pela qualidade, tratando o cliente com toda presteza e solucionando seus problemas com eficiência.

1.2. A Unimed Araxá entende que a privacidade é um direito fundamental da pessoa natural.

1.3. A Unimed Araxá compreende que, em seus processos de negócio os dados pessoais percorrem todo um ciclo de vida, que contém as etapas de coleta, processamento, análise, compartilhamento, armazenamento, reutilização e eliminação, sendo estes vulneráveis a fatores externos e internos que podem comprometer a proteção destes respectivos dados pessoais e afetar negativamente a privacidade dos seus titulares.

1.4. Dessa forma, a Unimed Araxá estabelece sua POLÍTICA GERAL DE PROTEÇÃO DE DADOS PESSOAIS (PGPDP), como parte integrante do seu sistema de gestão corporativo, compatível com os requisitos da legislação brasileira, além de boas práticas e normas internacionalmente aceitas, com o objetivo de garantir níveis adequados de proteção para os dados pessoais tratados pela organização.

2. Propósito

2.1. A Política de Proteção de Dados é uma política interna, que tem por propósito estabelecer diretrizes de Proteção de Dados que permitam a Unimed Araxá realizar o tratamento de dados pessoais, em conformidade com a legislação brasileira.

2.2. Orientar quanto à adoção de controles técnicos e administrativos para atendimento dos requisitos para Proteção de Dados Pessoais, conforme a legislação vigente.

2.3. Resguardar os titulares dos dados pessoais que são tratados pela Unimed Araxá garantindo direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

2.4. Prevenir possíveis causas de violações de dados pessoais e incidentes de segurança da informação relacionados ao tratamento de dados pessoais.

2.5. Minimizar os riscos de perdas financeiras, de participação no mercado, da confiança de clientes ou de qualquer outro impacto negativo no negócio da Unimed Araxá como resultado de violações de dados.

3. Escopo

3.1. Esta política se aplica a qualquer operação de tratamento de dados pessoais realizada pela Unimed Araxá independentemente do meio ou do país onde estejam localizados os dados, desde que:

3.1.1. A operação de tratamento seja realizada em território nacional brasileiro.

3.1.2. Tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional.

3.1.3. Os dados pessoais, objeto do tratamento, tenham sido coletados no território nacional.

4. Diretrizes

4.1. O objetivo da Proteção de Dados na Unimed Araxá é garantir a gestão sistemática e efetiva de todos os aspectos relacionados à proteção de dados pessoais e dos direitos dos seus titulares, provendo suporte as operações críticas do negócio e minimizando riscos identificados e seus eventuais impactos a organização.

4.2. Os Conselhos, órgãos executivos e o Comitê Gestor de Proteção de Dados Pessoais estão comprometidos com uma gestão efetiva da Proteção de Dados Pessoais na Unimed Araxá. Desta forma, adotam todas medidas cabíveis para garantir que esta política seja adequadamente comunicada, entendida e seguida em todos os níveis da organização. Revisões periódicas serão realizadas para garantir sua contínua pertinência e adequação as necessidades da Unimed Araxá.

4.3. A Unimed Araxá declara que preenche os requisitos dispostos no artigo 3º, da Lei n. 13.709/2018, sobre a aplicação territorial, no qual a lei informa que se aplica a empresas que realizam: a coleta e processamento de dados pessoais de pessoas

localizadas no Brasil; oferecem serviços ao mercado consumidor brasileiro; e tem estabelecimento no Brasil.

4.4. A Unimed Araxá observa as regras relacionadas a transferência internacional de dados pessoais conforme artigos 33 e 34 da Lei n. 13.709/2018 e preza por relacionar comercialmente com empresas que buscam estar em conformidade com as regras da Lei Geral de Proteção de Dados.

4.5. A Unimed Araxá se compromete a seguir a diretriz de que os dados pessoais só devem ser coletados para finalidades especificas e não irá coletar dados que não sejam necessários, adequados ou relevantes para o propósito ou finalidades a serem atendidos.

4.6. A Política de Proteção de Dados sempre obedecerá a diretriz de que o titular dos dados precisa sempre ser informado sobre os dados pessoais que estão sendo coletados e para que finalidade e sempre serão respeitadas as regras do consentimento expostos nesta política.

4.7. É política da Unimed Araxá:

4.7.1. Garantir ao titular a escolha de permitir ou não o tratamento de seus dados pessoais, excetuando-se casos onde a lei aplicável permitir especificamente o processamento de dados pessoais sem o consentimento do titular, observando-se o princípio da transparência.

4.7.2. Garantir que o objetivo do tratamento de dados pessoais esteja em conformidade com a legislação vigente e de acordo com uma base legal permitida.

4.7.3. Comunicar, de forma clara e adequadamente adaptada às circunstâncias, o tratamento de dados pessoais ao titular, antes do momento em que os dados são coletados ou usados pela primeira vez para um novo propósito.

4.7.4. Sempre que necessário, fornecer ao titular explicações suficientes sobre o tratamento de seus dados pessoais, conforme previsto na legislação vigente.

4.7.5. Limitar a coleta de dados pessoais estritamente ao que é permitido de acordo com a legislação vigente, e os objetivos especificados na coleta do consentimento do titular dos dados pessoais, minimizando, onde possível, a coleta dos referidos dados pessoais.

4.7.6. Limitar o uso, retenção, divulgação e transferência de dados pessoais ao necessário para cumprir com objetivos específicos, explícitos e legítimos.

4.7.7. Reter dados pessoais apenas pelo tempo necessário para cumprir os propósitos declarados e, posteriormente, destruí-los, bloqueá-los ou anonimizá-los com segurança.

4.7.8. Bloquear o acesso a dados pessoais e não realizar mais nenhum tratamento quando os propósitos declarados expirarem, mas a retenção dos dados pessoais for exigida pela legislação vigente.

4.7.9. Garantir a precisão e qualidade dos dados pessoais tratados, excetuando-se casos onde exista uma base legal para manter dados desatualizados.

4.7.10. Fornecer aos titulares dos dados pessoais tratados, informações claras e facilmente acessíveis sobre as políticas, procedimentos e práticas com relação ao tratamento de dados pessoais realizado pela organização, incluindo quais dados são efetivamente tratados, a finalidade desse tratamento e informações sobre como entrar em contato para obter maiores detalhes.

4.7.11. Notificar titulares quando ocorrerem alterações significativas no tratamento dos seus dados pessoais.

4.7.12. Garantir que titulares tenham a possibilidade de acessar e revisar seus dados pessoais, desde que sua identidade seja autenticada com um nível apropriado de garantia, e que não exista nenhuma restrição legal a esse acesso ou a revisão dos dados pessoais.

4.7.13. Garantir a rastreabilidade e prestação de contas durante todo o tratamento de dados pessoais, incluindo quando dados pessoais forem compartilhados com terceiros.

4.7.14. Tratar integralmente violações de dados, garantindo que sejam adequadamente registradas, classificadas, investigadas, corrigidas e documentadas.

4.7.15. Garantir que, na ocorrência de uma violação de dados, todas as partes interessadas serão notificadas, conforme requisitos e prazos previstos na legislação vigente.

4.7.16. Documentar e comunicar, conforme apropriado, todas as políticas, procedimentos e práticas relacionadas à privacidade e proteção de dados.

4.7.17. Garantir a existência de um responsável por documentar, implementar e comunicar políticas, procedimentos e práticas relacionadas à privacidade e proteção de dados.

4.7.18. Adotar controles de segurança da informação, tanto técnicos quanto administrativos, suficientes para garantir níveis de proteção adequados para dados pessoais.

4.7.19. Disponibilizar políticas, normas e procedimentos para proteção de dados pessoais a todas as partes interessadas e autorizadas, tais como: empregados, terceiros contratados e, onde pertinente, clientes.

4.7.20. Garantir a educação e conscientização de empregados, terceiros contratados e, onde pertinente, parceiros e clientes, sobre as práticas de proteção de dados pessoais adotadas pela Unimed Araxá.

4.7.21. Melhorar continuamente a Gestão de Proteção de Dados Pessoais através da definição e revisão sistemática de objetivos de privacidade e proteção de dados pessoais em todos os níveis da organização.

4.7.22. Garantir a não discriminação no tratamento de dados pessoais, impossibilitando que estes sejam usados para fins discriminatórios, ilícitos ou abusivos.

4.7.23. Garantir a conformidade integral com leis e regulamentações de proteção de dados pessoais.

4.7.24. **Observações importantes sobre consentimento e tratamento**

4.7.25. Todos os setores Unimed Araxá devem sempre observar e analisar os seguintes pontos importantes sobre o consentimento, conforme artigo 8º, da Lei n. 13.709/2018, e tratamento de dados pessoais.

4.7.26. Devem sempre observar a adequação legal.

4.7.27. O consentimento deve ser por escrito ou outro meio que demonstre a manifestação da vontade do titular.

4.7.28. A Unimed Araxá sempre ficará com o ônus da prova de consentimento.

4.7.29. Não é permitido tratar dados mediante o vício do consentimento.

4.7.30. O consentimento vale para finalidades especificas e não pode ser utilizado de forma genérica.

4.7.31. O consentimento pode ser revogado pelo titular dos dados.

4.7.32. Se a finalidade, forma e duração mudarem, é obrigatório informar o titular dos dados.

4.7.33. O tratamento de dados pessoais de crianças/adolescentes requer consentimento de pais ou responsáveis, conforme artigo 14, § 1º, da Lei n. 13.709/2018;

4.7.34. O consentimento deve ser armazenado no mesmo sistema ou em algum outro que possa ser de fácil acesso, conforme artigo 5º, inciso XII e artigo 8º, § 1º, ambos da Lei n. 13.709/2018.

4.7.35. Em qualquer momento os titulares dos dados podem revogar os acessos, mediante as bases legais ou outras que subsidie as demais atividades, conforme artigo 8º, § 2º e artigo 18, ambos da Lei n. 13.709/2018.

5. Papéis e Responsabilidades

5.1. Comitê Gestor de Proteção de Dados Pessoais – CGPD

5.1.1. Fica constituído o Comitê Gestor de Proteção de Dados Pessoais (CGPD), responsável pela avaliação dos mecanismos de tratamento e proteção de dados existentes e pela proposição de ações voltadas ao seu aperfeiçoamento, com vistas ao cumprimento das disposições da Lei n. 13.709/2018.

5.1.2. É responsabilidade do CGPD:

5.1.2.1. Avaliar os mecanismos de tratamento e proteção de dados existentes e propor políticas, estratégias e metas para a conformidade com as disposições da Lei n. 13.709/2018.

5.1.2.2. Formular princípios e diretrizes para a gestão de dados pessoais e propor sua regulamentação.

5.1.2.3. Supervisionar a execução dos planos, dos projetos e das ações aprovados para viabilizar a implantação das diretrizes previstas na Lei n. 13.709/2018.

5.1.2.4. Prestar orientações sobre o tratamento e a proteção de dados pessoais de acordo com as diretrizes estabelecidas na Lei n. 13.709/2018 e nas normas internas.

5.1.2.5. Promover o intercâmbio de informações sobre a proteção de dados pessoais com outros órgãos, bem como outros setores da Unimed.

5.1.2.6. Promover alinhamento e conformidade das atividades por eles realizadas com aquelas exercidas pelo Encarregado de Proteção de Dados, de forma que suas atividades sejam complementares.

5.1.2.7. Contribuir para a tomada de decisões acerca da Lei n. 13.709/2018 de forma centralizada, a fim de evitar eventuais conflitos de interesses.

5.1.2.8. Supervisionar o correto cumprimento das políticas de privacidade implantadas.

5.1.2.9. Conscientizar os agentes internos envolvidos com tratamento de dados pessoais acerca das políticas de privacidade.

5.2. Encarregado de Proteção de Dados

5.2.1. É responsabilidade do Encarregado de Proteção de Dados:

5.2.1.1. Aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências.

5.2.1.2. Receber comunicações da autoridade nacional e adotar providências.

5.2.1.3. Orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais, quando solicitado.

5.2.1.4. Executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares, quando solicitado.

5.2.1.5. Informar e aconselhar o controlador ou o operador, bem como os colaboradores que tratem dados pessoais a respeito das suas obrigações, quando solicitado.

5.2.1.6. Monitorar a conformidade com a Lei n. 13.709/2018, outras normas aplicáveis e com as políticas corporativas, incluindo a repartição de responsabilidades, a sensibilização e formação das pessoas que

operam dados pessoais e as auditorias correspondentes, quando solicitado.

5.2.1.7. Aconselhar, quando solicitado, acerca da avaliação de impacto sobre a proteção de dados e monitorar a sua realização.

5.2.1.8. Cooperar com as Autoridades.

5.2.1.9. Ser o ponto de contato com as Autoridades sobre questões relacionadas ao tratamento de dados.

5.3. Segurança da Informação

5.3.1. É responsabilidade do time de Segurança da Informação:

5.3.1.1. Garantir que políticas, normas e procedimentos de Segurança da Informação sejam ajustados e constantemente atualizados de forma a atender os requisitos da Política Geral de Proteção de Dados Pessoais.

5.3.1.2. Estabelecer, manter e atualizar processos de gerenciamento de riscos a fim de minimizar os efeitos dos riscos nos processos operacionais, como também a novos projetos relacionados a Tecnologia da Informação, devendo também ser estendido para as demais áreas do negócio e seus respectivos processos.

5.3.1.3. Adotar medidas de segurança, tanto técnicas quanto administrativas, aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito, conforme padrões mínimos recomendados pela autoridade nacional de proteção de dados pessoais.

5.3.1.4. Adoção de medidas físicas afim de detectar e prevenir quaisquer invasões aos ativos tecnológicos da empresa que realizam o tratamento de dados pessoais.

5.3.1.5. Criar e atualizar constantemente procedimentos e devidos escalonamentos para lidar com incidentes de segurança da informação, realizando o mais rápido possível o tratamento de incidentes que envolvam dados pessoais, garantindo sua detecção, contenção, eliminação e recuperação. Todos os incidentes também devem ser

registrados em um sistema informatizado, para fins de controle, auditoria e melhoria contínua dos processos.

5.3.1.6. Realizar constantemente treinamentos de conscientização para os funcionários e partes externas, demonstrando a responsabilidade de cada um nas notificações de ocorrências de qualquer evento de segurança da informação o mais rápido possível.

5.3.1.7. Apoiar o Encarregado de Proteção de Dados pessoais na comunicação à autoridade nacional e ao titular dos dados pessoais em casos de ocorrência de incidente de segurança que possam acarretar risco ou dano relevante aos titulares.

5.4. Colaboradores

5.4.1. É responsabilidade dos Colaboradores:

5.4.1.1. Ler, compreender e cumprir integralmente os termos da Política Geral de Proteção de Dados Pessoais, bem como as demais normas e procedimentos de proteção de dados pessoais aplicáveis.

5.4.1.2. Garantir que os dados pessoais sejam tratados e processados de acordo com esta política e com os princípios de proteção de dados estabelecidos na Lei 13.709/2018.

5.4.1.3. Encaminhar quaisquer dúvidas e/ou pedidos de esclarecimento sobre a Política Geral de Proteção de Dados Pessoais, suas normas e procedimentos ao Encarregado de Proteção de Dados ou, quando pertinente, ao Comitê Gestor de Proteção de Dados Pessoais.

5.4.1.4. Comunicar ao Encarregado de Proteção de Dados pelo Tratamento de Dados Pessoais qualquer evento que viole esta Política ou coloque/possa vir a colocar em risco Dados Pessoais tratados pela Unimed Araxá

5.4.1.5. Assinar o Termo de Uso de Sistemas de Informação da Unimed Araxá formalizando a ciência e o aceite integral das disposições da Política Geral de Proteção de Dados Pessoais, bem como as demais normas e procedimentos de segurança, assumindo responsabilidade pelo seu cumprimento.

5.4.1.6. Direcionar questionamentos sobre o armazenamento seguro de dados ao Encarregado de Proteção de Dados (DPO).

5.4.1.7. Compreender que o armazenamento dos dados pessoais pode decorrer pela permanência do contrato em vigor e deve estar explicita a supressão após o término do interesse entre as partes.

5.4.1.8. Quando os dados são armazenados em papel, manter em um local seguro, onde pessoas não autorizadas não possam vê-los.

5.4.1.9. Essas diretrizes de armazenamento também se aplicam a dados que geralmente são armazenados eletronicamente, mas que foram impressos por algum motivo.

5.4.1.10. Quando não for necessário, o papel ou os arquivos devem ser mantidos em uma gaveta trancada ou em um arquivo.

5.4.1.11. Os funcionários devem garantir que o papel e as impressões não sejam deixados onde pessoas não autorizadas possam vê-los, como por exemplo em uma impressora.

5.4.1.12. As impressões de dados devem ser trituradas e descartadas com segurança quando não forem mais necessárias.

5.4.1.13. Quando os dados são armazenados eletronicamente, eles devem ser protegidos contra acesso não autorizado, exclusão acidental e tentativas maliciosas de hackers.

5.4.1.14. Os dados devem ser protegidos por senhas fortes, alteradas regularmente e nunca compartilhadas entre os funcionários.

5.4.1.15. Se os dados forem armazenados em mídia removível (como um CD ou DVD), eles deverão ser mantidos trancados com segurança quando não estiverem sendo utilizados.

5.4.1.16. Os dados só devem ser armazenados em drives e designados servidores, e só deve ser carregado para um serviço de Computação em Nuvem aprovado, nesse caso OneDrive for Business da Microsoft ou Amazon S3.

5.4.1.17. Os servidores que contêm dados pessoais devem estar localizados em espaço físico apropriado, com permissão de acesso somente para os profissionais de tecnologia da informação.

5.4.1.18. Os backups dos dados devem ser feitos com frequência e devem ser testados regularmente, de acordo com os procedimentos padrão de backup da empresa.

5.4.1.19. Os dados nunca devem ser salvos diretamente em laptops ou outros dispositivos móveis, como tablets ou smartphones.

5.4.1.20. Todos os servidores e computadores que contêm dados devem ser protegidos por um software de segurança aprovado e um firewall.

5.4.1.21. Responder pela inobservância da Política Geral de Proteção de Dados Pessoais, normas e procedimentos relacionados ao tratamento de Dados Pessoais, conforme definido no item sanções e punições.

6. Minimização dos dados

6.1. A Unimed Araxá orienta ao usuário da informação que os dados pessoais devem ser coletados apenas para finalidades especificas com observância na possibilidade da minimização dos dados pessoais, adequação, relevância e limitação ao que é necessário em relação aos propósitos para os quais são processados. Caso não seja possível, deve ser justificado formalmente ao Encarregado de Proteção de Dados.

7. Sanções e Punições

7.1. As violações, mesmo que por mera omissão ou tentativa não consumada, desta política, bem como demais normas e procedimentos de proteção de dados pessoais, serão passíveis de penalidades que incluem advertência verbal, advertência por escrito, suspensão não remunerada e a demissão por justa causa.

7.2. A aplicação de sanções e punições será realizada conforme a análise do Comitê Gestor de Proteção de Dados Pessoais, devendo-se considerar a gravidade da infração, efeito alcançado, recorrência e as hipóteses previstas no artigo 482 da Consolidação das Leis do Trabalho, podendo o CGPD, no uso do poder disciplinar que lhe é atribuído, aplicar a pena que entender cabível quando tipificada a falta grave.

7.3. No caso de terceiros contratados ou prestadores de serviço, o CGPD deve analisar a ocorrência e deliberar sobre a efetivação das sanções e punições conforme termos previstos em contrato.

7.4. Para o caso de violações que impliquem em atividades ilegais, ou que possam incorrer em riscos aos titulares de dados pessoais, ou danos a Unimed Araxá, o infrator será responsabilizado pelos prejuízos, cabendo aplicação das medidas judiciais pertinentes sem prejuízo aos termos descritos nos itens 7.1, 7.2 e 7.3 desta política.

7.5. No caso de uma violação de segurança que leve à destruição acidental ou ilegal, perda, alteração, divulgação não autorizada ou acesso a dados pessoais, a Unimed Araxá deverá prontamente avaliar o risco para os direitos e liberdades dos titulares de dados e, se apropriado, informar essa violação à autoridade competente.

7.6. A aplicação das sanções acima mencionadas não impede a adoção de outras providências que a Unimed Araxá entender cabíveis, seja no âmbito civil ou penal.

8. Casos Omissos

8.1. Os casos omissos serão avaliados pelo Comitê Gestor de Proteção de Dados Pessoais para posterior deliberação.

8.2. As diretrizes estabelecidas nesta política e nas demais normas e procedimentos de proteção de dados pessoais, não se esgotam em razão da contínua evolução tecnológica, da legislação vigente e constante surgimento de novas ameaças e requisitos. Desta forma, não se constitui rol enumerativo, sendo obrigação do usuário da informação, adotar, sempre que possível, outras medidas de segurança além das aqui previstas, com o objetivo de garantir proteção de dados pessoais tratados pela Unimed Araxá.

9. Revisões

9.1. Esta política é revisada com periodicidade anual ou conforme o entendimento do Comitê Gestor de Proteção de Dados Pessoais.

10. Gestão da Política

10.1. A Política Geral de Proteção de Dados Pessoais é aprovada pelo Comitê Gestor de Proteção de Dados Pessoais, em conjunto com Conselho de Administração.

Histórico de Revisões

Versão 1.0 – A presente política foi aprovada no dia 05/07/2021.

11. GLOSSÁRIO

11.1. ANONIMIZAÇÃO: Utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo.

11.2. AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS**:** Órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento da Lei Geral de Proteção de Dados Pessoais (Lei n. 13.709/2018) em todo território nacional brasileiro.

11.3. BLOQUEIO**:** Suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados.

11.4. COMITÊ GESTOR DE PROTEÇÃO DE DADOS – CGPD**:** Grupo de trabalho multidisciplinar permanente, efetivado pela diretoria da Unimed Araxá que tem por finalidade tratar questões ligadas à Proteção de Dados Pessoais.

11.5. CONSENTIMENTO**:** Manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada.

11.6. CONTROLADOR**:** Pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais.

11.7. DADO ANONIMIZADO**:** Dado relativo ao titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento.

11.8. DADO PESSOAL SENSÍVEL**:** Dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato o a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

11.9. DADO PESSOAL**:** Informação relacionada a pessoa natural identificada ou identificável.

11.10. ELIMINAÇÃO**:** Exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado.

11.11. OPERADOR**:** Pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.

11.12. SEGURANÇA DA INFORMAÇÃO**:** A preservação das propriedades de confidencialidade, integridade e disponibilidade das informações da Unimed Araxá.

11.13. TITULAR**:** Pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.

11.14. TRATAMENTO DE DADOS PESSOAIS: Toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

11.15. USUÁRIO DA INFORMAÇÃO**:** Empregados com vínculo empregatício de qualquer área das empresas que compõem a Unimed ou terceiros alocados na prestação de serviços a Unimed indiferente do regime jurídico a que estejam submetidos, assim como outros indivíduos ou organizações devidamente autorizadas a utilizar manipular qualquer ativo de informação da Unimed para o desempenho de suas atividades profissionais.

11.16. VIOLAÇÃO DE DADOS PESSOAIS**:** Situação em que dados pessoais são processados violando um ou mais requisitos relevantes de proteção da privacidade.