

<b>Unimed</b> Tupã	<b>POLITICAS</b>	Código:POL_TI_344 Data de Emissão: 05/05/2025
	<b>Política de Privacidade e Proteção de Dados Pessoais</b>	Data da Revisão: 05/05/2026 Revisão Nº: 1

A Unimed de Tupã, por meio desta política, se compromete em garantir que, no exercício de suas atividades corporativas, os dados pessoais de clientes, beneficiários, dependentes, parceiros, demais colaboradores, fornecedores e prestadores de serviços serão tratados com o mais alto nível de cuidado, confidencialidade e conformidade com a Lei Geral de Proteção de Dados Pessoais (LGPD) e demais legislações aplicáveis.

A presente política tem como objetivo apresentar, aos colaboradores da organização, as determinações sobre a forma pela qual os dados pessoais serão manuseados, armazenados e transmitidos, a fim de atender às necessidades organizacionais e cumprir requisitos legais.

Esta política deverá atuar e ser cumprida em conjunto com o Regimento Interno, o Termo de Confidencialidade e Proteção de Dados Pessoais, a Política Interna de Privacidade e Proteção de Dados Pessoais, o Termo de Responsabilidade de Uso de Equipamento de Informática, o Termo de Responsabilidade de Uso de Celular Corporativo e a Política de Segurança da Informação aplicados pela organização.

O DPOnet, inscrito no CNPJ sob o nº 36.487.128/0001-79, foi nomeado como nosso Encarregado de Dados. Assim, ele está apto a exercer todas as funções e atribuições do cargo, previstas na LGPD.

**Caso você deseje exercer qualquer um de seus direitos expressos na Lei, basta clicar no Selo “Canal de Comunicação LGPD” em nosso site, e preencher o “Formulário de Atendimento ao Titular de Dados”.**

Para facilitar a sua compreensão, saiba que nossa Política Interna de Privacidade e Proteção de Dados Pessoais está organizada da seguinte forma:

1	Disposições Gerais
2	Objetivos
3	Diretrizes
4	Registros de Operações
5	Auditoria de Processos
6	Relatório de Impacto (RIPD)
7	Incidentes
8	Comitê de Proteção de Dados

9	Encarregado
10	Treinamentos
11	Direitos dos Titulares
12	Segurança
13	Responsabilidades
14	Disposições Finais

## 1. DISPOSIÇÕES GERAIS:

1.1. Para fins desta política, passa-se a adotar as definições expressas pela LGPD, quais sejam:

- Dado Pessoal: informação relacionada a pessoa natural identificada ou identificável;
- Dado Pessoal Sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou 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;
- Dado Anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;
- Titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;
- Controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;
- Operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;
- Encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD);
- Agentes de Tratamento: o controlador e o operador;
- Tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento,

<b>Unimed</b> Tupã	<b>POLITICAS</b>	Código:POL_TI_344 Data de Emissão: 05/05/2025
	<b>Política de Privacidade e Proteção de Dados Pessoais</b>	Data da Revisão: 05/05/2026 Revisão Nº: 1

armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;

- 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;
- Consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;
- Transferência Internacional de Dados: transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro;
- Relatório de Impacto à Proteção de Dados Pessoais (RIPD): documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco.
- Autoridade Nacional de Proteção de Dados (ANPD): órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional.

1.2. A LGPD determinou que as atividades de tratamento deverão observar a boa-fé e os seguintes princípios:

- Finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
- Adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
- Necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;
- Livre Acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;
- Qualidade dos Dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;

	<b>POLITICAS</b>	Código:POL_TI_344
	<b>Política de Privacidade e Proteção de Dados Pessoais</b>	Data de Emissão: 05/05/2025
		Data da Revisão: 05/05/2026
		Revisão Nº: 1

- Transparéncia: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;
- Segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;
- Prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;
- Não Discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;
- Responsabilização e Prestação de Contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

1.3. A LGPD determinou que o tratamento de dados pessoais somente poderá ser realizado nas hipóteses previstas em seu art. 7º, quais sejam:

- Consentimento do titular;
- Cumprimento de obrigação legal ou regulatória;
- Execução de políticas públicas;
- Estudos por órgãos de pesquisa;
- Execução de contratos;
- Exercício regular de direitos em processo judicial, administrativo ou arbitral;
- Proteção da vida;
- Tutela da saúde;
- Legítimo interesse do controlador;
- Proteção do crédito.

1.4. A LGPD determinou que o tratamento de dados pessoais sensíveis somente poderá ser realizado nas hipóteses previstas no art. 11, quais sejam:

- Consentimento do titular;
- Cumprimento de obrigação legal ou regulatória;
- Execução de políticas públicas;
- Estudos por órgãos de pesquisa;
- Execução de contratos;

	<b>POLITICAS</b>	Código:POL_TI_344
		Data de Emissão: 05/05/2025
	<b>Política de Privacidade e Proteção de Dados Pessoais</b>	Data da Revisão: 05/05/2026
		Revisão Nº: 1

- Exercício regular de direitos inclusive em contrato e em processo judicial, administrativo ou arbitral;
- Proteção da vida;
- Tutela da saúde;
- Prevenção à fraude e à segurança do titular.

## **2. OBJETIVOS:**

2.1. Durante o exercício de suas atividades corporativas, os colaboradores da organização realizam o tratamento de dados pessoais de seus clientes, beneficiários, dependentes, parceiros, demais colaboradores, fornecedores e prestadores de serviços. Essa política visa demonstrar o compromisso da organização em:

- Estabelecer diretrizes que garantem o cumprimento de normas e boas práticas relacionadas à proteção de dados pessoais;
- Realizar o tratamento dos dados pessoais dos titulares acima qualificados com a devida proteção, transparência, segurança e confidencialidade;
- Prevenir possíveis causas de violações à proteção dos dados pessoais tratados e incidentes envolvendo dados pessoais;
- Minimizar os riscos de perdas financeiras, da confiança de clientes, parceiros, prestadores de serviços ou qualquer outro impacto negativo ao negócio da organização, como resultado da violação à proteção dos dados pessoais.

2.2. Esta política se aplica à organização e a todas as empresas por ela controladas, bem como a todos os colaboradores que, em algum momento, possam ter contato com dados pessoais dos titulares qualificados no item 1.1;

2.3. Outras políticas adicionais poderão ser criadas para casos específicos, principalmente se exigido por Lei ou Regulamento.

## **3. DIRETRIZES:**

3.1. A organização se compromete a realizar o tratamento dos dados pessoais para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;

3.2. A organização se compromete em realizar o tratamento dos dados pessoais de forma compatível com as finalidades informadas ao titular, de acordo com o contexto do tratamento;

3.3. A organização se compromete em realizar o tratamento dos dados pessoais limitando-se ao mínimo necessário para a realização de suas finalidades, com

	<b>POLITICAS</b>	Código:POL_TI_344
		Data de Emissão: 05/05/2025
<b>Política de Privacidade e Proteção de Dados Pessoais</b>	Data da Revisão: 05/05/2026	
	Revisão Nº: 1	

abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;

3.4. A organização garante, aos titulares de dados, consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;

3.5. A organização garante, aos titulares de dados, exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;

3.6. A organização garante, aos titulares de dados, informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial, através de Termos de Ciência e de Consentimento;

3.7. A organização garante a utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações accidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;

3.8. A organização garante a adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais, conforme descrito no item 3.11.

3.9. A organização não realizará tratamentos de dados pessoais para fins discriminatórios ilícitos ou abusivos;

3.10. A organização garante a demonstração da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas, conforme descrito no item 3.11;

3.11. Os integrantes da organização, no exercício de suas funções corporativas, declaram a adoção de medidas de segurança capazes de proteger os dados pessoais de acessos não autorizados, bem como de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito, tais como:

- Estabelecer Políticas de Privacidade que contemplem a conscientização de colaboradores e parceiros de negócios referente a importância da proteção de dados pessoais, restando vedado o relacionamento com pessoas, físicas ou jurídicas, que venham a descumprir tais normas institucionais;
- Conscientizar seus colaboradores acerca da impossibilidade de compartilhamento de dados de acesso, como logins e senhas, com terceiros, uma vez que são de uso pessoal, intransferível e de conhecimento exclusivo do próprio usuário.

3.12. A organização se compromete a armazenar dados pessoais apenas pelo tempo mínimo necessário para atendimento da finalidade pretendida e cumprimento de

<b>Unimed</b> Tupã	<b>POLITICAS</b>	Código:POL_TI_344 Data de Emissão: 05/05/2025
	<b>Política de Privacidade e Proteção de Dados Pessoais</b>	Data da Revisão: 05/05/2026 Revisão Nº: 1

eventuais obrigações legais que regulam determinada atividade de tratamento e, posteriormente, destruí-los, bloqueá-los ou anonimiza-los com segurança, por meio de picotadoras ou incineradores, sendo proibido o uso direto de lixeiras, ou eliminação de dados pessoais em hardwares e banco de dados digitais.

3.13. A organização se compromete a finalizar o tratamento de dados pessoais nas seguintes hipóteses: quando verificar que a finalidade foi alcançada ou que os dados deixaram de ser necessários ou pertinentes ao alcance da finalidade; fim do período do tratamento; comunicação do titular, inclusive no exercício de seu direito de revogação do consentimento; e determinação da ANPD, quando houver violação à LGPD.

3.14. É vedada a reprodução física ou digital, para fins não profissionais, de qualquer imagem ou documento que contenha dados pessoais que possam identificar ou tornar identificável colaboradores, clientes, parceiros ou fornecedores, sob pena de responder pelos prejuízos causados e demais cominações legais e administrativas;

3.15. É proibido o compartilhamento de logins e senhas, tanto corporativas quanto não profissionais, para uso de *e-mails*, plataformas ou sistemas, sob pena de responder pelos prejuízos causados, e demais cominações legais e administrativas, inclusive demissão por justa causa;

3.16. A organização, atualmente, realiza a transferência internacional de dados pessoais, de acordo com as determinações específicas para esse tipo de tratamento, conforme art. 33 e 34, da LGPD, e as especificações da Resolução CD/ANPD nº 19/2024, que regulamenta os artigos da LGPD que tratam da transferência internacional de dados.

3.16. A organização, atualmente, não realiza a transferência internacional de dados pessoais. Caso seja necessário esse tipo de transferência, se compromete a seguir as determinações específicas para esse tipo de tratamento, conforme art. 33 e 34, da LGPD, e as especificações da Resolução CD/ANPD nº 19/2024, que regulamenta os artigos da LGPD que tratam da transferência internacional de dados.

3.17. Os integrantes da organização, no exercício de suas funções institucionais, devem comunicar aos seus superiores e ao DPO (*Data Protection Officer*), imediatamente e, de forma detalhada, toda e qualquer ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares, bem como sobre qualquer evento adverso confirmado, relacionado à violação na segurança de dados pessoais, tais como acesso não autorizado, acidental ou ilícito que resulte na destruição, perda, alteração, vazamento ou ainda, qualquer forma de tratamento de dados inadequada ou ilícita, para que estes adotem as devidas providências;

3.18. Os integrantes da organização deverão utilizar os equipamentos de trabalho (computadores, notebooks, tablets e celulares corporativos) apenas para fins corporativos, sendo proibido o uso deles para outras funções ou, ainda, para acesso de

<b>Unimed</b> Tupã	<b>POLITICAS</b>	Código:POL_TI_344 Data de Emissão: 05/05/2025
	<b>Política de Privacidade e Proteção de Dados Pessoais</b>	Data da Revisão: 05/05/2026 Revisão Nº: 1

endereços eletrônicos ilegais ou com conteúdo que não condizem com as políticas da empresa;

3.19. Os integrantes da organização deverão utilizar o e-mail corporativo e demais recursos tecnológicos da empresa para fins exclusivamente profissionais. Permanece estabelecida, ainda, a possibilidade da empresa ter acesso ao conteúdo do e-mail corporativo do integrante e computadores, com aviso antecedente;

3.20. Os integrantes da organização deverão atuar com muito cuidado e atenção no encaminhamento de mensagens eletrônicas, conferindo, sempre antes do respectivo envio, o endereço, o conteúdo e o destinatário;

3.21. O distanciamento do integrante de seu equipamento eletrônico deverá ser precedido do devido bloqueio (*logoff*);

3.22. Os integrantes da organização deverão adotar condutas para manter sua mesa, impressoras e scanners livres de documentos expostos que contenham dados pessoais de colaboradores, clientes, parceiros ou fornecedores;

3.23. É terminantemente proibida a utilização de softwares não licenciados ou não autorizados nas dependências da organização, sob pena de rescisão contratual, sem prejuízo de resarcimento de eventuais danos sofridos pela organização;

3.24. É obrigatório que os integrantes da organização mantenham seus equipamentos com sistema de antivírus válido e atualizado, sendo de sua responsabilidade a comunicação de vencimento ao responsável técnico;

3.25. Aos integrantes da organização, é permitido o acesso remoto aos dados necessários ao exercício de sua função somente mediante prévio conhecimento e autorização dos responsáveis técnico e administrativo, e, após auditoria da segurança de ambiental proporcionada pelo integrante, sendo seu acesso interrompido a qualquer tempo, sem aviso prévio, conforme conveniência da organização;

3.26. Aos integrantes da organização, é proibido fotografar, filmar, reproduzir ou compartilhar quaisquer imagens de suas dependências e/ou outros integrantes, salvo se integrar a atividade da empresa e expressamente autorizado pela Diretoria;

3.27. Aos integrantes da organização, é proibido o uso de dispositivos removíveis nas portas USB, CD/DVD ou gravador de CD/DVD, salvo se permitido nos termos da Política de Segurança da Informação adotada;

3.28. O compartilhamento interno ou externo de documentos que contenham dados pessoais simples, sensíveis, financeiros, comportamentais, de menores ou de quaisquer outras naturezas, que possam identificar ou tornar identificável eventual titular, far-se-á mediante o que estabelecido na Política de Segurança da Informação adotada;

<b>Unimed</b> Tupã	<b>POLITICAS</b>	Código:POL_TI_344 Data de Emissão: 05/05/2025
	<b>Política de Privacidade e Proteção de Dados Pessoais</b>	Data da Revisão: 05/05/2026 Revisão Nº: 1

3.29. Os integrantes da organização deverão adotar condutas de confidencialidade e sigilo de todas as informações de dados pessoais simples, sensíveis, financeiros, comportamentais, de menores ou de quaisquer outras naturezas, que possam identificar ou tornar identificável eventual titular, que tenha acesso no exercício de sua função;

3.30. Quando o tratamento de dados pessoais envolver a finalidade de pesquisa, a organização garante, sempre que possível, a anonimização dos dados pessoais envolvidos, através de métodos seguros e eficazes.

3.31. O tratamento de dados pessoais de crianças e adolescentes deverá ser realizado observadas as determinações previstas na Seção III, da LGPD, denominada como “Do Tratamento de Dados Pessoais de Crianças e de Adolescentes”, quais sejam:

- a) O tratamento de dados pessoais de crianças e adolescentes poderá ser realizado com base nas hipóteses legais previstas no art. 7º ou no art. 11 da LGPD, desde que observado e prevalecente o seu melhor interesse, a ser avaliado no caso concreto, nos termos do art. 14 da Lei;
- b) O consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal deve ser aplicado quando for efetivamente a melhor hipótese legal no caso concreto, não sendo expressamente necessário. Caso seja, a organização deverá realizar todos os esforços razoáveis para verificar que o consentimento foi dado pelo responsável pela criança, consideradas as tecnologias disponíveis
- c) No tratamento de dados mencionado no item “a”, a organização deverá manter pública a informação sobre os tipos de dados coletados, a forma de sua utilização e os procedimentos para o exercício dos direitos dos titulares;
- d) Poderão ser coletados dados pessoais de crianças sem o consentimento a que se refere o item “a” quando a coleta for necessária para contatar os pais ou o responsável legal, utilizados uma única vez e sem armazenamento, ou para sua proteção, e em nenhum caso poderão ser repassados a terceiro sem o consentimento de que trata o item “a”;
- e) A organização não deverá condicionar a participação dos titulares de que trata o item “a” em jogos, aplicações de internet ou outras atividades ao fornecimento de informações pessoais além das estritamente necessárias à atividade;
- f) As informações sobre o tratamento de dados referidas neste item deverão ser fornecidas de maneira simples, clara e acessível, consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, com uso de recursos audiovisuais quando adequado, de forma a proporcionar a informação

	<b>POLÍTICAS</b>	Código:POL_TI_344
		Data de Emissão: 05/05/2025
	<b>Política de Privacidade e Proteção de Dados Pessoais</b>	Data da Revisão: 05/05/2026
		Revisão Nº: 1

necessária aos pais ou ao responsável legal e adequada ao entendimento da criança;

- g) Em caso de transferência internacional de dados, serão aplicadas salvaguardas adicionais, incluindo medidas que assegurem que o tratamento seja realizado em seu melhor interesse, nos termos da Legislação Nacional e dos instrumentos pertinentes de direito internacional.

3.32. Com relação às atividades de tratamento de dados pessoais pautadas pelo consentimento, caberá à organização avaliar a licitude dessa autorização, pois ela deverá ser fornecida por escrito ou por outro meio que demonstre a manifestação de vontade do titular, além de obedecer finalidades específicas, podendo ser revogado a qualquer momento, mediante manifestação de vontade do titular, conforme previsto no art. 8º, da LGPD.

3.33. Dados pessoais fornecidos por terceiros externos à organização somente poderão ser recebidos mediante celebração de contrato que incluam cláusulas de privacidade e proteção de dados pessoais robustas o suficiente, conforme orientações fornecidas pelo departamento jurídico interno e pelo Encarregado de Dados, que deverão verificar idoneidade e aplicabilidade das cláusulas adotadas, bem como se foram abordados todos os pontos necessários para garantir a completa adequação do documento à LGPD.

3.34. Os integrantes da organização se comprometem a não disponibilizar essa Política Interna de Privacidade e Proteção de Dados Pessoais com terceiros externos à organização, por tratar-se de documentação interna que reúne todas as diretrizes de conduta corporativa adotadas pelos colaboradores.

#### **4. REGISTROS DE OPERAÇÕES DE TRATAMENTO DE DADOS PESSOAIS:**

4.1. Para acompanhar a maneira como os mapeamentos deverão ser realizados, os colaboradores da organização deverão assistir ao treinamento disponibilizado na plataforma do DPOnet.

4.2. A organização deverá manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse, devendo conter as seguintes informações:

- Departamento responsável pelo registro;
- Nome do processo;
- Origem dos dados;
- Finalidade do tratamento;

	<b>POLITICAS</b>	Código:POL_TI_344
		Data de Emissão: 05/05/2025
	<b>Política de Privacidade e Proteção de Dados Pessoais</b>	Data da Revisão: 05/05/2026
		Revisão Nº: 1

- Tempo de armazenamento do registro na organização;
- Categoria de titulares envolvidos;
- Faixa etária dos titulares envolvidos;
- Quantidade aproximada de titulares envolvidos;
- Tipos de dados pessoais tratados;
- Local de armazenamento do registro;
- Tempo de armazenamento do registro no departamento responsável e respectiva justificativa;
- Como os dados pessoais são dispostos;
- Forma de recuperação do registro;
- Forma de proteção do registro;
- Com quem esse registro é compartilhado;
- Como esse registro é compartilhado;
- Por quê esse registro é compartilhado;
- Se é realizada a transferência internacional de dados pessoais;
- Se é utilizada alguma plataforma, software ou aplicativo para a realização do compartilhamento;
- Quem são os agentes de tratamento envolvidos na relação;
- Análise de ameaças;
- Necessidade e proporcionalidade dos dados pessoais tratados, armazenados e compartilhados.

4.3. Deverão ser registradas todas as atividades que envolvam o tratamento de dados pessoais, sensíveis, comportamentais, financeiros e de menores realizadas pelos membros da organização, em todos os seus departamentos e níveis.

4.4. Caberá aos líderes de departamento realizar os registros das atividades que envolvam o tratamento de dados pessoais ou delimitar outros colaboradores de seu departamento para realizarem essa atividade.

Para auxílio e documentação dos registros das operações de tratamento de dados pessoais, todos os setores da organização realizarão o mapeamento das atividades realizadas na plataforma do DPOnet.

Para acessá-lo, conecte-se à tela inicial do DPOnet com seu login e senha e clique no link “Treinamentos”, localizado no canto esquerdo da tela. Ao ser direcionado a uma nova página, clique em “Curso inicial de implementação da LGPD para Líderes de departamento” e assista ao módulo “Processos”, localizado no item “Treinamentos tutoriais do DPOnet”.

	<b>POLITICAS</b>	Código:POL_TI_344
		Data de Emissão: 05/05/2025
	<b>Política de Privacidade e Proteção de Dados Pessoais</b>	Data da Revisão: 05/05/2026
		Revisão Nº: 1

4.5. Todos os setores da organização deverão se responsabilizar pela atualização dos registros mapeados, bem como se certificar que eles estejam de acordo com a realidade da empresa.

4.6. A atribuição da hipótese legal dos registros caberá ao nosso Encarregado de Dados, o DPOnet.

4.7. Sobre atividades de tratamento enquadradas na hipótese legal do legítimo interesse:

- a) Permite que uma organização processe dados pessoais sem o consentimento explícito do titular dos dados, desde que esse processamento seja necessário para fins legítimos e mediante uma análise de equilíbrio entre os interesses do controlador (ou de terceiros) e os direitos e liberdades fundamentais do titular dos dados.
- b) A hipótese legal do legítimo interesse não é aplicável ao tratamento de dados pessoais sensíveis, apenas aos dados pessoais comuns.
- c) Para aplicar essa hipótese legal do legítimo interesse, é necessário a realização de um teste de balanceamento, denominado pela GDPR como “Legitimate Interest Assessment (LIA)”, composto por três fases:
  - Finalidade: nesta fase, deve-se analisar o contexto do tratamento, com foco sobre os benefícios gerados e as finalidades que se pretende alcançar;
  - Necessidade: a segunda fase do teste é fundamentada no art. 7º, inciso IX, que utiliza a expressão “quando necessário” e, mais especificamente, no art. 10, §1º, ambos da LGPD, que prevê que “quando o tratamento for baseado no legítimo interesse do controlador, somente os dados pessoais estritamente necessários para a finalidade pretendida poderão ser tratados”;
  - Balanceamento e Salvaguardas: a terceira fase do teste é a etapa de realização da ponderação entre, de um lado, os interesses do controlador ou de terceiro e, de outro, os direitos e liberdades fundamentais do titular;
- d) A realização do teste permite a constituição do Relatório de Legítimo Interesse, que poderá ser gerado pela plataforma DPOnet. Tal processo será explicado posteriormente, no tópico 6.9.

## 5. AUDITORIA DE PROCESSOS:

	<b>POLITICAS</b>	Código:POL_TI_344 Data de Emissão: 05/05/2025
	<b>Política de Privacidade e Proteção de Dados Pessoais</b>	Data da Revisão: 05/05/2026 Revisão Nº: 1

5.1. Com o objetivo de auxiliar a organização a garantir a atualização dos mapeamentos realizados, o DPOnet fornece um serviço denominado como “auditoria de processos”.

Após o período de adequação (três meses), será iniciada uma contagem de seis meses para que os processos recomendados ou adicionados sejam auditados. Para isso, será feita uma seleção de 2% dos processos, com data de atualização mais antiga, cadastrados na empresa. Os processos que forem selecionados ficarão com o status “pendente”, até que:

- O responsável indique que não há necessidade de mudanças, ou seja, que o processo está atualizado; ou
- O responsável faça as mudanças necessárias para readequar o processo à realidade da empresa.

5.2. O período de auditoria se encerra em 30 (trinta) dias. Será possível acessar o histórico de auditorias da organização, monitorar e verificar os processos que foram modificados após as auditorias.

5.3. Para realizar a auditoria, após verificar que o processo encontra-se com o status “pendente”, será possível selecionar duas opções: está atualizado ou necessário editar. Caso o processo corresponda à realidade da empresa, clique em “está atualizado”. Caso contrário, clique em “necessário editar” e faça as mudanças necessárias.

Após realizar as mudanças necessárias, é preciso enviar o processo para a revisão, para que o DPOnet analise e valide as novas informações cadastradas.

## **6. RELATÓRIOS GERADOS PELA PLATAFORMA DPONET:**

6.1. Alguns relatórios, tanto aqueles relacionados à obrigações legais, quanto aqueles que possam auxiliar a organização no andamento da gestão da privacidade e no processo de adequação à LGPD, poderão ser gerados pela plataforma DPOnet, a partir das informações nela inseridas;

**6.2. O Relatório Gerencial é um resumo de informações-chave que fornece uma visão geral do desempenho da organização,** auxiliando a alta administração na tomada de decisões estratégicas e operacionais.

Nele, é possível visualizar o status dos processos mapeados, das medidas de segurança, da distribuição de ameaças por grau de severidade, das ameaças com medidas vinculadas, das medidas por categoria, dos departamentos por menor e maior

	<b>POLITICAS</b>	Código:POL_TI_344
		Data de Emissão: 05/05/2025
<b>Política de Privacidade e Proteção de Dados Pessoais</b>	Data da Revisão: 05/05/2026	
	Revisão Nº: 1	

quantidade de ameaças e dos departamentos por menor e maior severidade de ameaças.

Para gerá-lo, acesse a tela inicial do DPOnet com seu login e senha e, no canto esquerdo da tela, clique em “Relatórios” > “Relatório Gerencial”. No canto superior direito da tela, clique em “Gerar Relatório”.

6.3. O **Relatório de Impacto à Proteção de Dados Pessoais (RIPD)** é um documento que reúne as atividades de tratamento que podem causar risco aos direitos e liberdades individuais dos titulares de dados pessoais. Portanto, precisará ser gerado quando houver atividades de tratamento que possam causar risco aos direitos e liberdades individuais dos titulares de dados pessoais.

Sendo a elaboração desse documento uma exigência prevista pela LGPD, o DPOnet fornece uma maneira de gerá-lo, sempre que for necessário. Para gerar o RIPD, conecte-se à tela inicial do DPOnet com seu login e senha e clique no link “Relatório de Impacto”, localizado no canto esquerdo da tela. Depois, é só informar o endereço de e-mail para o qual será enviado o relatório e, em poucos minutos, poderá ser visualizado.

Os Relatórios de Impacto gerados são documentos internos e não devem ser publicados ou disponibilizados a terceiros. Contudo, poderão ser objeto de requisição da ANPD, a qualquer tempo.

6.4. O **Registro das Atividades de Tratamento (RoPA)**, traduzido da sigla em inglês “Record of Processing Activities”, é um documento que detalha todas as atividades de tratamento de dados pessoais realizadas pela organização, incluindo informações sobre a finalidade do processamento, as categorias de dados pessoais envolvidos, os enquadramentos legais, os destinatários dos dados, os prazos de retenção dos dados e as medidas de segurança implementadas, dentre outras informações. Esse relatório desempenha um papel fundamental no processo de conformidade da organização, auxiliando-a a demonstrar transparência e responsabilidade no tratamento de dados pessoais.

Para gerá-lo, acesse a tela inicial do DPOnet com seu login e senha e, no canto esquerdo da tela, clique em “Relatórios” > “RoPA”. Na nova tela, informe uma justificativa para a exportação do relatório e, no canto superior direito da tela, clique em “Gerar Relatório”. O documento será enviado ao e-mail de login.

6.5. O **Relatório de Prestação de Contas** tem como objetivo demonstrar que o agente adotou medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais, estabelecendo um paralelo entre as funcionalidades da plataforma e os requisitos da LGPD.

	<b>POLITICAS</b>	Código:POL_TI_344 Data de Emissão: 05/05/2025
	<b>Política de Privacidade e Proteção de Dados Pessoais</b>	Data da Revisão: 05/05/2026 Revisão Nº: 1

Para gerá-lo, acesse a tela inicial do DPOnet com seu login e senha e, no canto esquerdo da tela, clique em “Relatórios” > “Relatório de Conformidade”. No canto superior direito da tela, clique em “Gerar Relatório”.

**6.6. O Relatório de Medidas de Segurança** tem como objetivo avaliar se a organização cumpre regulamentações e políticas estabelecidas, identificando áreas de risco e oportunidades de melhoria. É essencial para garantir transparência e conformidade legal. É elaborado com base nos questionários respondidos pela organização e nas medidas de segurança que passarão a ser adotadas, após a realização do plano de ação.

Nesse item, é possível gerar dois relatórios: um relatório completo, que contempla controles e plano de ação; e um relatório simplificado, que contempla apenas controles.

Para gerá-los, acesse a tela inicial do DPOnet com seu login e senha e, no canto esquerdo da tela, clique em “Relatórios” > “Relatório de Medidas de Segurança”. Na nova tela, escolha a versão do relatório (completo ou simplificado). No canto superior direito da tela, clique em “Gerar Relatório”.

**6.7. O Relatório de Ameaças** proporciona uma visão abrangente das ameaças presentes na organização, detalhando suas medidas de segurança e os locais em que podem ocorrer.

Para gerá-lo, acesse a tela inicial do DPOnet com seu login e senha e, no canto esquerdo da tela, clique em “Relatórios” > “Relatório de Ameaças”. No canto superior direito da tela, clique em “Gerar Relatório”.

**6.8. O Relatório de Treinamento** trata-se de um documento que permite acompanhar a evolução da conscientização dos colaboradores da organização. É uma ferramenta valiosa para identificar bons e maus resultados.

Para gerá-lo, acesse a tela inicial do DPOnet com seu login e senha e, no canto esquerdo da tela, clique em “Relatórios” > “Relatório de Treinamento”. No canto superior direito da tela, clique em “Gerar Relatório”.

**6.9. O Relatório de Legítimo Interesse** descreve detalhadamente as razões pelas quais uma organização considera que o processamento de dados pessoais é justificado com base no princípio do legítimo interesse.

Nesse item, é possível gerar dois relatórios: um relatório completo, que contempla todos os processos que contém LIA; e um relatório unitário, que contempla somente um processo. Para gerá-lo, acesse a tela inicial do DPOnet com seu login e senha e, no canto esquerdo da tela, clique em “Relatórios” > “Relatório de Legítimo Interesse”. No canto superior direito da tela, clique em “Gerar Relatório”.

	<b>POLITICAS</b>	Código:POL_TI_344 Data de Emissão: 05/05/2025
	<b>Política de Privacidade e Proteção de Dados Pessoais</b>	Data da Revisão: 05/05/2026 Revisão Nº: 1

6.10. O **Relatório de Consentimentos** formaliza a autorização ou o acordo de uma pessoa para participar em uma atividade, projeto ou processo, especialmente em contextos onde a privacidade, a segurança ou a ética são preocupações importantes.

Nesse item, é possível gerar três relatórios: por pessoa, por formulário e completo (todos os formulários com todos os recibos). Para gerá-lo, acesse a tela inicial do DPOnet com seu login e senha e, no canto esquerdo da tela, clique em “Relatórios” > “Relatório de Consentimentos”. No canto superior direito da tela, clique em “Gerar Relatório”.

6.10. O **Relatório de Auditoria** é essencial para identificar quais processos foram atualizados e quais estão desatualizados durante a auditoria.

Nesse item, é possível gerar dois relatórios: o completo e o simplificado. Para gerá-lo, acesse a tela inicial do DPOnet com seu login e senha e, no canto esquerdo da tela, clique em “Relatórios” > “Relatório de Auditoria”. No canto superior direito da tela, clique em “Gerar Relatório”.

## 7. INCIDENTES:

7.1. Um incidente de segurança com dados pessoais é qualquer evento adverso confirmado, relacionado à violação na segurança de dados pessoais, tais como acesso não autorizado, acidental ou ilícito que resulte na destruição, perda, alteração, vazamento ou ainda, qualquer forma de tratamento de dados inadequada ou ilícita, os quais possam ocasionar risco para os direitos e liberdades do titular dos dados pessoais.

7.2. Os integrantes da organização, no exercício de suas funções institucionais, devem comunicar aos seus superiores e ao DPO (*Data Protection Officer*), imediatamente e, de forma detalhada, toda e qualquer ocorrência relacionada a um possível incidente envolvendo dados pessoais;

7.3. O DPOnet, enquanto plataforma de gerenciamento de dados pessoais apresenta, uma funcionalidade que auxilia na gestão de incidentes de segurança envolvendo dados pessoais, permitindo ao cliente registrar e detalhar o fato ocorrido, bem como descrever as medidas de contenção adotadas durante e logo após o incidente.

Para acessá-la, conecte-se à tela inicial do DPOnet com seu login e senha e clique no link “Incidentes”, localizado no canto esquerdo da tela. Caso queira registrar um incidente, clique no link “Novo Incidente”, no canto superior direito da tela e, na nova tela, clique em “sim”. Depois, é só preencher os campos em aberto com as características do incidente:

- Como ele foi detectado;
- Tipo de violação (confidencialidade, integridade ou disponibilidade);

	<b>POLITICAS</b>	Código:POL_TI_344 Data de Emissão: 05/05/2025
	<b>Política de Privacidade e Proteção de Dados Pessoais</b>	Data da Revisão: 05/05/2026 Revisão Nº: 1

- Quais dados foram violados;
- Como e por que (a causa, se conhecida) ocorreu o incidente;
- Data e hora do incidente;
- Medidas de contenção adotadas durante e logo após o incidente;
- Quantidade estimada de titulares afetados;
- Processos afetados.

7.4. O DPOnet irá apoiar a organização para realizar as notificações e esclarecimentos necessários. Após o registro do incidente, será possível realizar o tratamento do incidente, ou seja, quais foram os riscos específicos para a empresa e os planos de ação adotados para saná-los, bem como as lições aprendidas após o incidente.

7.5. A organização possui um documento denominado como “Plano de Gestão de Incidentes”, que descreve todas as etapas do gerenciamento realizado pelo DPOnet.

## **8. COMITÊ DE PROTEÇÃO DE DADOS:**

8.1. A criação de um Comitê é considerada como uma boa prática de proteção de dados pessoais. Portanto, a organização instituiu seu próprio Comitê, como uma maneira de demonstrar que se preocupa com os dados pessoais que circulam dentro dos departamentos, diariamente.

8.2. Esse grupo de colaboradores é responsável por garantir a comunicação do programa de privacidade, discutir e tomar decisões sobre novas atividades de tratamento, avaliar os mecanismos de tratamento e segurança adotados pela organização, visando o cumprimento da LGPD.

### 8.3. São atribuições do Comitê de Proteção de Dados:

- Criação de políticas em geral, para a empresa e para departamentos específicos;
- Auxílio para identificar atividades de tratamento e orientar o menor risco possível;
- Auxílio e realização de atividades de educação e cultura;
- Análise de problemas envolvendo produtos e serviços;
- Apoio em caso de incidentes de dados pessoais;
- Auxílio na manutenção de todo o programa de gestão da proteção de dados pessoais.

8.4. Para que o Comitê de Proteção de Dados da organização esteja devidamente formalizado, o DPOnet disponibiliza os seguintes documentos, com as seguintes finalidades:

	<b>POLITICAS</b>	Código:POL_TI_344 Data de Emissão: 05/05/2025
	<b>Política de Privacidade e Proteção de Dados Pessoais</b>	Data da Revisão: 05/05/2026 Revisão Nº: 1

- Ata de Nomeação dos Membros: com este documento e indicadas as pessoas que irão participar do Comitê, ele estará formalmente constituído.
- Ata de Eleição da Presidência e Vice-Presidência: com este documento e realizando a eleição de quem será Presidente e Vice-Presidente, será possível identificar os responsáveis por desempenhar funções para que o Comitê realize suas atividades;
- Regulamento Interno: este documento contém as regras internas do Comitê, as funções e os períodos que irão acontecer as reuniões.

8.5. Os documentos mencionados no tópico anterior deverão ser preenchidos na etapa de implementação e deverão ser armazenados em uma pasta própria, segura e dedicada aos documentos de proteção de dados pessoais da organização.

8.6. A organização garante que já adotou a utilização de toda a documentação acima mencionada, relacionada à formalização do Comitê de Proteção de Dados.

## **9. DO ENCARREGADO PELO TRATAMENTO DE DADOS PESSOAIS:**

9.1. O DPOnet foi nomeado como nosso Encarregado de Dados. Assim, ele está apto a exercer todas as funções e atribuições do cargo, previstas na LGPD.

9.2. As atividades do Encarregado consistem em:

- Aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;
- Receber comunicações da ANPD e adotar providências;
- Orientar os funcionários e os contratados da organização a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e
- Executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.

Ao receber comunicações da ANPD, o encarregado deverá adotar as medidas necessárias para o atendimento da solicitação e para o fornecimento das informações pertinentes, adotando, entre outras, as seguintes providências:

- Encaminhar internamente a demanda para as unidades competentes;
- Fornecer a orientação e a assistência necessárias ao agente de tratamento; e

	<b>POLITICAS</b>	Código:POL_TI_344
		Data de Emissão: 05/05/2025
	<b>Política de Privacidade e Proteção de Dados Pessoais</b>	Data da Revisão: 05/05/2026
		Revisão Nº: 1

- Indicar expressamente o representante do agente de tratamento perante a ANPD para fins de atuação em processos administrativos, quando esta função não for exercida pelo próprio encarregado.

Cabe, ainda, ao encarregado, nos termos do art. 10, inciso II, deste Regulamento, prestar assistência e orientação ao agente de tratamento na elaboração, definição e implementação, conforme o caso, de:

- registro e comunicação de incidente de segurança;
- registro das operações de tratamento de dados pessoais;
- relatório de impacto à proteção de dados pessoais;
- mecanismos internos de supervisão e de mitigação de riscos relativos ao tratamento de dados pessoais;
- medidas de segurança, técnicas e 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;
- processos e políticas internas que assegurem o cumprimento da Lei nº 13.709, de 14 de agosto de 2018, e dos regulamentos e orientações da ANPD;
- instrumentos contratuais que disciplinem questões relacionadas ao tratamento de dados pessoais;
- transferências internacionais de dados;
- regras de boas práticas e de governança e de programa de governança em privacidade, nos termos do art. 50 da Lei nº 13.709, de 14 de agosto de 2018;
- produtos e serviços que adotem padrões de design compatíveis com os princípios previstos na LGPD, incluindo a privacidade por padrão e a limitação da coleta de dados pessoais ao mínimo necessário para a realização de suas finalidades; e
- outras atividades e tomada de decisões estratégicas referentes ao tratamento de dados pessoais.

9.3. A ANPD poderá estabelecer normas complementares sobre a definição e as atribuições do encarregado, inclusive hipóteses de dispensa da necessidade de sua indicação, conforme a natureza e o porte da entidade ou o volume de operações de tratamento de dados.

9.4. As reclamações e comunicações dos titulares serão aceitas e recebidas através do **Selo “Canal de Comunicação LGPD”**, incluído no site da organização, que poderá ser acessado através do link a seguir: <https://www.unimedtupa.com.br/>

	<b>POLITICAS</b>	Código:POL_TI_344 Data de Emissão: 05/05/2025
	<b>Política de Privacidade e Proteção de Dados Pessoais</b>	Data da Revisão: 05/05/2026 Revisão Nº: 1

9.5. Por meio do Selo, qualquer interessado é direcionado ao Portal Privacidade&Você e pode verificar a autenticidade da adequação da empresa à LGPD, inclusive, podendo verificar: a última revisão de seus mecanismos de controle com a exibição da data e hora em que foi feita a revisão; as políticas de privacidade da empresa; o meio de contato dos titulares de dados; e o meio de contato da ANPD.

9.6. Caso você deseje exercer qualquer um de seus direitos expressos na LGPD, basta clicar no **Selo “Canal de Comunicação LGPD”** em nosso site, e preencher o **“Formulário de Atendimento ao Titular de Dados”**.

9.7. Para dúvidas jurídicas, contratuais, de Segurança da Informação, confidencialidade dos dados tratados ou demais assuntos relacionados à proteção de dados pessoais, entrar em contato com o DPOnet através do e-mail [“atendimento@dponet.com.br”](mailto:atendimento@dponet.com.br). Também é possível entrar em contato com a empresa pela tela inicial do DPOnet. Para isso, conecte-se à tela inicial do DPOnet com seu login e senha e clique no link “Entre em contato”, localizado no canto inferior esquerdo da tela.

## **10. TREINAMENTOS:**

10.1. Todos os colaboradores da organização que estiverem envolvidos nas atividades de tratamento de dados pessoais deverão receber treinamentos periódicos, decididos e organizados pelo Comitê de Proteção de Dados, especificamente sobre:

- Conceitos gerais de privacidade e proteção de dados pessoais, incluindo a apresentação dessa Política Interna, o Regimento Interno, o Termo de Confidencialidade e Proteção de Dados Pessoais, a Política Interna de Privacidade e Proteção de Dados Pessoais, o Termo de Responsabilidade de Uso de Equipamento de Informática, o Termo de Responsabilidade de Uso de Celular Corporativo e a Política de Segurança da Informação adotados pela organização;
- Conceitos específicos de privacidade e proteção de dados pessoais, aplicados às atividades de cada área.

10.2. O treinamento mencionado no item anterior deverá ocorrer pelo menos 1 vez ao ano.

10.3. O treinamento mencionado no item 9.1 deverá fazer parte do procedimento de integração de novos colaboradores da organização.

10.4. Além dos treinamentos mencionados nos itens anteriores, o DPOnet disponibiliza cursos à distância para o representante, para a Diretoria e para os líderes de departamento. Ao final da finalização dos cursos, será possível emitir um certificado de conclusão.

	<b>POLITICAS</b>	Código:POL_TI_344 Data de Emissão: 05/05/2025
	<b>Política de Privacidade e Proteção de Dados Pessoais</b>	Data da Revisão: 05/05/2026 Revisão Nº: 1

Para acessá-los, conecte-se à tela inicial do DPOnet com seu login e senha e clique no link “Treinamentos”, localizado no canto esquerdo da tela. Ao ser direcionado a uma nova página, selecione o curso que deseja assistir.

## **11.DIREITOS DOS TITULARES:**

11.1. Em cumprimento à LGPD, a organização garante ao titular a possibilidade de solicitação dos seguintes direitos:

- Confirmação da existência de tratamento;
- Acesso aos dados;
- Correção de dados incompletos, inexatos ou desatualizados;
- Anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com a Lei;
- Portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial;
- Eliminação dos dados pessoais tratados com o consentimento do titular;
- Informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;
- Informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;
- Revogação do consentimento.

11.2. Com relação ao recebimento das requisições, o titular deverá enviá-las através do **Selo “Canal de Comunicação LGPD”**. Todas as requisições serão recebidas e avaliadas pelo DPOnet, que irá confirmar a identidade do titular e a licitude da requisição enviada, para que a organização possa realizar o que foi solicitado.

11.3. O DPOnet informará à organização quanto à possibilidade, ou não, de atendimento da requisição do titular, através de justificativas legais, bem como entrará em contato com o titular para informá-lo sobre essa justificativa e, caso seja legalmente permitida, sobre a realização do que foi solicitado por parte da organização.

## **12.SEGURANÇA DA INFORMAÇÃO:**

12.1. Para garantir a segurança dos dados pessoais tratados no exercício das atividades corporativas da organização e evitar acessos indevidos ou não autorizados, perda, destruição ou qualquer outro evento que comprometa a integridade, disponibilidade ou confidencialidade das informações, a organização se compromete a

	<b>POLITICAS</b>	Código:POL_TI_344 Data de Emissão: 05/05/2025
	<b>Política de Privacidade e Proteção de Dados Pessoais</b>	Data da Revisão: 05/05/2026 Revisão Nº: 1

adotar e manter os melhores mecanismos de Segurança da Informação, proteção de dados pessoais e confidencialidade.

12.2. Para tanto, os mecanismos adotados serão expostos na Política de Segurança da Informação aplicada pela organização, que deverá ser analisada em conjunto com a presente Política Interna de Privacidade e Proteção de Dados Pessoais e demais documentações internas.

### **13. RESPONSABILIDADE:**

13.1. Em caso de prejuízos causados pelos colaboradores à organização, em razão da quebra de confidencialidade das informações às quais teve acesso, ou qualquer incidente de vazamento de dados que for constatado ser decorrente de sua conduta no tratamento dos dados, como também em desconformidade com as orientações da organização, incorre em falta disciplinar grave, sujeito às sanções previstas em Lei ou constantes nos processos disciplinares internos da organização, inclusive serem responsabilizados pessoalmente, judicial ou extrajudicialmente.

### **14. DISPOSIÇÕES FINAIS:**

14.1. Esta Política Interna de Privacidade e Proteção de Dados Pessoais foi elaborada com base nas determinações expressas pela LGPD.

14.2. A organização se reserva no direito de atualizar esta Política Interna de Privacidade e Proteção de Dados Pessoais quantas vezes forem necessárias, a fim de que as determinações expressas no documento estejam sempre atualizadas e em conformidade com a legislação vigente.

14.3. Os casos omissos serão avaliados pelo Comitê de Proteção de Dados, como também pelo Encarregado de Dados, para posterior deliberação.

Elaboração	Revisão	Aprovação
<b>André Gustavo Bisi</b> Gerente de TI	<b>Roberta S. Boaventura</b> Coordenadora da Qualidade	<b>Ana Paula A. A. Pereira</b> Gerente