POLÍTICA CORPORATIVA DE PRIVACIDADE E GOVERNANÇA DE DADOS PESSOAIS

Ver.: 00
Data: 28/04/2025

Av. Levy Ramos Martins, 803 - Nova Brasília
CEP 88780-000 - Imbituba/SC - Telefone: (48) 3254 7200
contato@onix.seg.br

1. OBJETIVOS

A presente **Política Corporativa de Privacidade e Proteção de Dados Pessoais** ("Política") estabelece as **diretrizes institucionais e procedimentais** a serem seguidas pela Onix Tecnologia no **Tratamento de Dados Pessoais**, em conformidade com a **Lei nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais (LGPD)**, bem como com os princípios estabelecidos em normas internacionais de referência, como a **ISO/IEC 27701** e a **ISO/IEC 29100**.

Esta Política tem como objetivos:

- Promover a proteção dos direitos fundamentais de liberdade, privacidade e livre desenvolvimento da personalidade dos titulares de dados pessoais;
- Estabelecer princípios e obrigações para o adequado tratamento de dados pessoais em todas as atividades conduzidas pela Onix;
- Consolidar uma cultura organizacional baseada em ética, transparência, segurança da informação e responsabilidade no uso de dados.

2. APLICAÇÃO

As diretrizes contidas nessa Política aplicam-se, **sem exceção**, a:

- Todos os **Colaboradores da Onix**, independentemente de seu nível hierárquico ou vínculo contratual;
- Todas as **operações que envolvam o Tratamento de Dados Pessoais**, seja em meio físico ou digital, realizadas diretamente pela Onix ou por terceiros atuando em seu nome.

O conhecimento, a compreensão e a aplicação integral das disposições desta Política são **obrigatórios** e constituem **requisito essencial para a conformidade corporativa** com os princípios da privacidade e proteção de dados pessoais.

Termos e expressões iniciados com letra maiúscula nesta Política possuem o significado definido no **Glossário**, localizado ao final deste documento.

3. PAPÉIS E RESPONSABILIDADES

3.1. Programa de Privacidade

O Programa de Privacidade da Onix é composto pelo conjunto de pessoas, processos, diretrizes, cultura e estruturas organizacionais que, de forma integrada, visam garantir a adoção efetiva das boas práticas de proteção de dados pessoais, em conformidade com a Lei nº 13.709/2018 (LGPD), regulamentações complementares emitidas pela Autoridade Nacional de Proteção de Dados (ANPD), e normas técnicas reconhecidas internacionalmente, como a ISO/IEC 27701.

O Programa tem como missão assegurar o tratamento ético, justo, proporcional e seguro dos dados pessoais, promovendo uma cultura de respeito à privacidade e aos direitos dos Titulares.

3.2. Responsabilidade Institucional

Na qualidade de Agente de Tratamento, a Onix deve garantir que todo e qualquer Tratamento de Dados Pessoais ocorra de forma lícita, transparente, limitada à sua finalidade e com segurança, sendo corresponsável pela implementação dos controles organizacionais, técnicos e procedimentais exigidos pela legislação e pelas melhores práticas de mercado.

Av. Levy Ramos Martins, 803 - Nova Brasília
CEP 88780-000 - Imbituba/SC - Telefone: (48) 3254 7200
contato@onix.seg.br
ISO 9001
ACATE Member

3.3. Encarregado pelo Tratamento de Dados Pessoais (Data Protection Officer – DPO)

O Encarregado pelo Tratamento de Dados Pessoais, também denominado Data Protection Officer (DPO), é o profissional designado pela Onix para:

- Promover e supervisionar a aplicação das normas internas e legais de proteção de dados;
- Atuar como canal de comunicação entre os Titulares dos Dados, a Autoridade Nacional de Proteção de Dados (ANPD) e as áreas internas da organização.

A designação do Encarregado deve considerar a estrutura e complexidade das operações da Onix, sendo possível a nomeação de colaborador interno ou a contratação de profissional ou empresa externa. O profissional designado deve:

- Possuir capacitação e experiência em normas de proteção de dados, segurança da informação e privacidade;
- Ter independência funcional para o exercício do cargo, sem conflito de interesses;
- Possuir visão sistêmica de riscos e sensibilidade quanto às operações de tratamento e seus impactos sobre os direitos dos titulares.

A identidade e o contato do Encarregado deverão estar publicamente disponíveis no website institucional da Onix, conforme previsto no Art. 41, §1º da LGPD.

3.4. Atribuições do Encarregado

Compete ao Encarregado, sem prejuízo de outras atribuições previstas em normativos legais ou internos:

1. Capacitação e Cultura Organizacional
- Organizar e/ou ministrar treinamentos sobre proteção de dados pessoais para colaboradores e terceiros;
- Promover a cultura organizacional de privacidade na Onix.

2. Governança e Documentação
- Elaborar e revisar políticas e procedimentos internos relacionados à proteção de dados;
- Garantir a disponibilidade e ampla divulgação dos documentos de privacidade na organização.

3. Controle e Monitoramento
- Acompanhar e avaliar riscos de tratamento de dados pessoais nas atividades da empresa;
- Apoiar a definição de controles técnicos e organizacionais para garantir a confidencialidade, integridade e disponibilidade dos dados.

4. Mapeamento e Avaliação de Riscos
- Manter atualizado o mapeamento de fluxos de dados pessoais;
- Avaliar e emitir pareceres sobre Relatórios de Impacto à Proteção de Dados Pessoais (RIPD).

5. Resposta a Incidentes
- Apoiar na resposta e apuração de incidentes de segurança envolvendo dados pessoais;
- Apoiar a definição de medidas corretivas e aplicação de sanções internas.

Av. Levy Ramos Martins, 803 - Nova Brasília
CEP 88780-000 - Imbituba/SC - Telefone: (48) 3254 7200
contato@onix.seg.br
ISO 9001
ACATE Member

6. Regulatório e Jurídico

- Realizar o acompanhamento das normas e diretrizes emitidas pela ANPD;
- Auxiliar a Assessoria Jurídica na análise de transferências internacionais de dados, contratos com fornecedores e ajustes de finalidade de tratamento.

7. Atendimento aos Titulares e à ANPD

- Receber e responder comunicações da ANPD;
- Atender aos pedidos dos titulares de dados, conforme seus direitos legais;
- Atuar como facilitador de consultas e orientações às áreas internas e aos demais Agentes de Tratamento.

3.5. Comitê de Privacidade

O Comitê de Privacidade da Onix é um órgão colegiado de caráter estratégico, responsável por apoiar a governança do Programa de Privacidade, promover a tomada de decisão institucional e garantir o alinhamento entre as iniciativas de proteção de dados e os objetivos corporativos da organização.

O Comitê atua como instância de análise e deliberação sobre temas críticos relacionados ao Tratamento de Dados Pessoais e exerce papel fundamental na consolidação da cultura de privacidade na Onix.

Compete ao Comitê:

- Analisar, discutir e deliberar sobre os relatórios, recomendações e incidentes reportados pelo Encarregado pelo Tratamento de Dados Pessoais;
- Garantir o suporte da alta gestão às ações, investimentos e iniciativas voltadas à proteção de dados pessoais;
- Orientar as diretrizes estratégicas do Programa de Privacidade, promovendo o engajamento entre as áreas envolvidas;
- Acompanhar a efetividade das políticas e controles implementados, propondo ajustes e melhorias contínuas, quando necessário;
- Avaliar situações críticas ou excepcionais que envolvam transferências internacionais, mudanças significativas nas finalidades de tratamento, ou projetos com alto impacto em dados pessoais;
- Auxiliar na definição de responsabilidades, aplicação de sanções internas e resolução de impasses interdepartamentais relacionados à privacidade;
- Garantir a conformidade com os princípios da LGPD e demais legislações e normas técnicas aplicáveis.

A composição, frequência de reuniões, forma de deliberação e responsabilidades adicionais do Comitê serão definidas por ato interno complementar, elaborado pela Diretoria Executiva ou pela área responsável pela Governança Corporativa.

3.6. Área de Tecnologia da Informação (TI)

Compete à Área de Tecnologia da Informação (TI) da Onix atuar como responsável técnico pela implantação, manutenção e monitoramento dos controles de segurança da informação relacionados ao Tratamento de Dados Pessoais, em conformidade com a Política Geral de Segurança da Informação, esta Política de Privacidade e Proteção de Dados Pessoais, e demais normas internas aplicáveis.

A Área de TI deverá, no âmbito de suas atribuições:

Av. Levy Ramos Martins, 803 - Nova Brasília
CEP 88780-000 - Imbituba/SC - Telefone: (48) 3254 7200
contato@onix.seg.br
ISO 9001
ACATE Member

- Assegurar que todos os sistemas, serviços, aplicações e equipamentos utilizados no Tratamento de Dados Pessoais estejam configurados e operados dentro de padrões aceitáveis de segurança da informação, conforme critérios técnicos estabelecidos pela NBR ISO/IEC 27001, 27002 e demais boas práticas reconhecidas;
- Analisar os aspectos técnicos de segurança e privacidade em todo produto ou serviço de terceiros que venha a ser contratado para o Tratamento de Dados Pessoais, incluindo, mas não se limitando a, soluções de computação em nuvem, dispositivos de armazenamento, equipamentos de rede e software de gestão;
- Implementar e manter medidas técnicas e organizacionais apropriadas para assegurar a confidencialidade, integridade, disponibilidade e resiliência dos dados pessoais e dos ambientes tecnológicos associados;
- Coletar, manter e disponibilizar registros das atividades de tratamento de dados pessoais realizadas em sistemas sob sua responsabilidade, de forma a assegurar a rastreabilidade e o cumprimento de requisitos legais, em especial o disposto nos Artigos 37 e 41 da LGPD;
- Investigar incidentes de segurança da informação que envolvam dados pessoais, em conjunto com o Encarregado pelo Tratamento de Dados Pessoais e demais áreas competentes, propondo e implementando medidas de mitigação e remediação;
- Garantir a aplicação de controles preventivos e detectivos contra acesso não autorizado, vazamentos, destruição, alteração ou qualquer forma de tratamento inadequado ou ilícito de dados pessoais;
- Apoiar a execução dos planos de resposta a incidentes e participar da avaliação de risco dos ativos tecnológicos que envolvam o Tratamento de Dados Pessoais;
- Cumprir todas as demais responsabilidades previstas na Política Geral de Segurança da Informação e demais normativos internos correlatos.

A atuação da Área de TI deve estar orientada pelo princípio da privacidade desde a concepção ("Privacy by Design") e da privacidade por padrão ("Privacy by Default"), em todas as fases dos projetos e operações tecnológicas.

3.7. Assessoria Jurídica

A Assessoria Jurídica da Onix atua como suporte especializado para garantir a conformidade legal das atividades de Tratamento de Dados Pessoais, sendo corresponsável pela mitigação de riscos jurídicos e regulatórios relacionados à proteção de dados.

Compete à Assessoria Jurídica, no âmbito desta Política:

- Prestar consultoria jurídica especializada nos processos de contratação e aquisição de produtos, serviços, tecnologias ou parcerias que envolvam o Tratamento de Dados Pessoais, assegurando a aderência às exigências legais aplicáveis, incluindo cláusulas de proteção de dados em instrumentos contratuais;
- Apoiar o Encarregado pelo Tratamento de Dados Pessoais (DPO) na análise e validação de operações de transferência internacional de dados pessoais, em conformidade com os requisitos previstos nos Artigos 33 a 36 da LGPD, avaliando a existência de garantias adequadas no país destinatário;
- Assessorar a elaboração de respostas, manifestações e comunicações formais à Autoridade Nacional de Proteção de Dados (ANPD), em conjunto com o Encarregado, sempre que demandado;
- Fornecer orientação jurídica especializada em casos de ocorrência de incidentes de segurança envolvendo dados pessoais, incluindo suporte na análise de obrigação de notificação aos titulares e à ANPD, conforme o disposto no Artigo 48 da LGPD;

Av. Levy Ramos Martins, 803 - Nova Brasília
CEP 88780-000 - Imbituba/SC - Telefone: (48) 3254 7200
contato@onix.seg.br
ISO 9001
ACATE Member

- Apoiar o Encarregado na interpretação e aplicação prática das políticas internas de proteção de dados pessoais, propondo ajustes e melhorias quando necessário, a fim de refletir a evolução normativa, regulatória ou jurisprudencial;
- Contribuir na avaliação dos riscos legais e regulatórios relacionados às atividades de Tratamento de Dados Pessoais realizadas pela Onix.

A atuação da Assessoria Jurídica deve ser pautada pelos princípios da ética, transparência, diligência e responsabilidade, em estreita colaboração com o Encarregado e as demais áreas envolvidas na governança de dados pessoais.

3.8. Área Administrativa

A Área Administrativa da Onix é corresponsável pelo fortalecimento da cultura de proteção de dados pessoais no ambiente organizacional, assegurando que as práticas de gestão de pessoas e de processos internos estejam alinhadas às disposições desta Política e às exigências da legislação vigente, especialmente a Lei Geral de Proteção de Dados Pessoais (LGPD – Lei nº 13.709/2018).

Compete à Área Administrativa:

- Promover a cultura de proteção de dados pessoais, em conjunto com o Encarregado pelo Tratamento de Dados Pessoais, através da realização periódica de campanhas internas de conscientização, programas de capacitação e divulgação ativa de informações sobre os direitos dos titulares e as boas práticas de segurança da informação;
- Assegurar a ampla divulgação interna dos documentos que compõem esta Política e demais políticas, normas e procedimentos internos relacionados à privacidade e proteção de dados pessoais;
- Garantir a transparência para com os colaboradores da Onix sobre:
  - ✓ Quais dados pessoais são coletados;
  - ✓ Para quais finalidades;
  - ✓ Como são tratados, armazenados e eliminados;
  - ✓ Quais são os direitos dos colaboradores enquanto titulares de dados;
- Definir, implementar e monitorar controles de proteção de dados pessoais nos processos administrativos de:
  - ✓ Contratação de novos colaboradores e prestadores de serviços;
  - ✓ Desligamento ou encerramento da prestação de serviços;
  - ✓ Modificação de atividades internas, como promoções, movimentações ou mudanças de função;
  - ✓ Afastamentos temporários, como férias, licenças médicas, licenças maternidade/paternidade ou suspensões.

A atuação da Área Administrativa deverá estar orientada pelos princípios da prevenção, transparência, responsabilização e prestação de contas, em conformidade com as diretrizes da Onix para segurança da informação e proteção de dados pessoais.

3.9. Gestores

Os Gestores da Onix desempenham papel fundamental na aplicação e sustentação do Programa de Privacidade, atuando como responsáveis diretos pelo cumprimento, disseminação e monitoramento das diretrizes previstas nesta Política no contexto das atividades sob sua supervisão.

Av. Levy Ramos Martins, 803 - Nova Brasília
CEP 88780-000 - Imbituba/SC - Telefone: (48) 3254 7200
contato@onix.seg.br
ISO 9001
ACATE Member

Compete aos Gestores:

- Cumprir e assegurar o cumprimento desta Política e de seus documentos complementares por parte de todos os colaboradores sob sua gestão, promovendo a conscientização, o alinhamento e a aplicação das boas práticas de proteção de dados pessoais;
- Consultar o Encarregado pelo Tratamento de Dados Pessoais (DPO) sempre que houver alteração, criação ou ampliação das finalidades de tratamento de dados pessoais nas atividades sob sua responsabilidade;
- Realizar e manter atualizado o mapeamento dos fluxos de dados pessoais vinculados à sua área, incluindo identificação de categorias de dados, bases legais, agentes de tratamento, tempo de retenção e mecanismos de segurança aplicáveis;
- Assegurar que o tratamento de dados pessoais realizado por sua equipe ocorra exclusivamente no âmbito das atividades profissionais autorizadas pela Onix, conforme os termos desta Política e demais normativos internos;
- Identificar e avaliar riscos operacionais, regulatórios e éticos relacionados ao tratamento de dados pessoais nas atividades sob sua coordenação, propondo ações corretivas, melhorias ou planos de mitigação;
- Submeter à análise prévia do Encarregado todos os novos processos, projetos, aplicações, produtos ou serviços que envolvam o tratamento de dados pessoais, com vistas à avaliação de impacto e à definição de controles adequados;
- Reportar imediatamente ao Encarregado qualquer ocorrência de violação de dados pessoais, incidente de segurança, comportamento atípico ou dúvida relevante quanto ao tratamento de dados pessoais, promovendo a resposta rápida e coordenada aos riscos identificados.

Os Gestores devem exercer suas atribuições com base nos princípios da responsabilização, prevenção, prestação de contas e colaboração, integrando-se ao modelo de governança em privacidade da Onix.

3.10. Colaboradores

Os Colaboradores da Onix, independentemente de seu cargo, área de atuação ou vínculo contratual, são corresponsáveis pelo correto Tratamento de Dados Pessoais no âmbito de suas atividades profissionais, devendo observar estritamente as disposições desta Política e da legislação vigente.

Compete aos Colaboradores:

- Cumprir integralmente as diretrizes, normas e procedimentos estabelecidos nesta Política e em seus documentos complementares, bem como respeitar as determinações da legislação aplicável à proteção de dados pessoais, especialmente a Lei Geral de Proteção de Dados Pessoais (LGPD - Lei nº 13.709/2018);
- Realizar o Tratamento de Dados Pessoais sob responsabilidade da Onix apenas para fins expressamente autorizados, de forma ética, lícita, proporcional e respeitosa aos direitos dos Titulares, seguindo rigorosamente as orientações contidas nesta Política e nos instrumentos normativos internos;
- Zelar pela integridade, disponibilidade, confidencialidade, autenticidade e legalidade dos dados pessoais acessados ou tratados, abstendo-se de utilizar, copiar, enviar, transmitir, compartilhar ou manipular informações pessoais de forma inadequada, ilícita ou fora do escopo de suas atribuições profissionais, em qualquer meio, físico ou eletrônico, incluindo plataformas de comunicação digital e internet;

Av. Levy Ramos Martins, 803 - Nova Brasília
CEP 88780-000 - Imbituba/SC - Telefone: (48) 3254 7200
contato@onix.seg.br

- Reportar imediatamente ao Encarregado pelo Tratamento de Dados Pessoais (DPO) quaisquer eventos, suspeitas, violações efetivas, incidentes de segurança ou qualquer situação de risco envolvendo Dados Pessoais de que venha a ter conhecimento, utilizando os canais formais estabelecidos pela Onix.

O descumprimento destas obrigações poderá sujeitar o Colaborador às medidas disciplinares e sanções previstas nas normas internas da Onix, sem prejuízo das responsabilidades legais aplicáveis.

4. DIRETRIZES DE PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS

As diretrizes estabelecidas nesta Política devem ser observadas desde a fase de concepção ("Privacy by Design") de novas operações de Tratamento de Dados Pessoais, bem como na criação, desenvolvimento e execução de produtos, serviços, processos e sistemas que envolvam dados pessoais no âmbito da Onix Tecnologia.

A Onix deverá ser capaz de demonstrar a efetividade da adoção das diretrizes de proteção de dados sempre que apropriado, inclusive perante solicitações da Autoridade Nacional de Proteção de Dados (ANPD) ou de outras autoridades competentes, em consonância com os princípios da responsabilização e prestação de contas (accountability) previstos na Lei nº 13.709/2018 (LGPD).

Nesse contexto, a Onix, seus Gestores, Colaboradores e Prestadores de Serviços deverão observar, no mínimo, as seguintes diretrizes gerais:

- Incorporação da proteção de dados pessoais como requisito obrigatório em todas as fases de projetos, serviços e processos, considerando segurança desde a concepção e proteção por padrão ("Privacy by Design" e "Privacy by Default");
- Adoção de medidas técnicas e administrativas aptas a proteger os dados pessoais contra acessos não autorizados, situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;
- Minimização do tratamento de dados pessoais, limitando a coleta, utilização e retenção apenas ao estritamente necessário para a finalidade pretendida;
- Garantia da transparência e da informação adequada aos titulares de dados, especialmente sobre as finalidades do tratamento, compartilhamento, tempo de retenção e direitos aplicáveis;
- Implementação de controles internos, procedimentos e políticas documentadas que assegurem o cumprimento desta Política e demais obrigações legais aplicáveis;
- Promoção contínua da conscientização e treinamento dos colaboradores sobre proteção de dados pessoais e privacidade;
- Avaliação prévia de riscos e impactos à proteção de dados pessoais antes da implementação de novos tratamentos ou tecnologias (Privacy Impact Assessments);
- Adoção de mecanismos de resposta a incidentes de segurança, com comunicação tempestiva às autoridades e titulares de dados, conforme exigido pela legislação;
- Revisão periódica dos processos, controles e documentos de privacidade, para assegurar sua atualização diante de alterações legislativas, regulatórias ou tecnológicas.

O descumprimento destas diretrizes será considerado violação grave às normas internas da Onix e poderá acarretar a aplicação de sanções administrativas, cíveis e disciplinares.

4.1. Tratamento de Dados Pessoais

Para fins desta Política, Tratamento de Dados Pessoais significa toda operação realizada com dados pessoais, por meios automatizados ou não, envolvendo, dentre outras atividades:

- Coleta, recepção;
- Produção, reprodução, utilização, acesso;
- Processamento, classificação, avaliação, controle;
- Modificação, extração;
- Comunicação, transmissão, difusão, distribuição, transferência;
- Arquivamento, armazenamento;
- Eliminação.

O conceito de Tratamento aqui adotado está em conformidade com a definição prevista no Artigo 5º, inciso X da Lei nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais (LGPD), e deve ser interpretado de forma ampla, abrangendo qualquer manipulação de dados de pessoas físicas.

4.1.1. Observância à Política e à Legislação

Toda operação de Tratamento de Dados Pessoais realizada no âmbito da Onix deve ser conduzida:

- Em estrita conformidade com as diretrizes estabelecidas nesta Política e em seus documentos complementares;
- Com observância rigorosa aos princípios e fundamentos estabelecidos na LGPD e em demais legislações aplicáveis;
- De maneira ética, transparente, segura e proporcional ao propósito legítimo para o qual os dados foram coletados.

4.1.2. Hipóteses Legais para o Tratamento

Conforme disposto no Artigo 7º da LGPD, a Onix poderá realizar o Tratamento de Dados Pessoais apenas nas seguintes hipóteses legais:

- Mediante o consentimento do titular, de forma livre, informada e inequívoca;
- Para cumprimento de obrigação legal ou regulatória pela Onix;
- Pela administração pública, para o tratamento necessário ao atendimento de políticas públicas previstas em normas ou contratos;
- Para a execução de contratos ou de procedimentos preliminares relacionados a contrato do qual o titular seja parte, a pedido do titular;
- Para o exercício regular de direitos em processos judiciais, administrativos ou arbitrais;
- Para a proteção da vida ou da incolumidade física do titular ou de terceiros;
- Para a tutela da saúde, em procedimentos realizados por profissionais da saúde, serviços de saúde ou autoridade sanitária;
- Quando necessário para atender aos interesses legítimos da Onix ou de terceiros, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular;
- Para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

A definição da base legal aplicável deve ser cuidadosamente avaliada antes do início de qualquer Tratamento de Dados Pessoais, em conformidade com a metodologia de Governança em Privacidade da Onix.

4.1.3. Tratamento de Dados Pessoais Sensíveis

A legislação de proteção de dados pessoais brasileira, especialmente a Lei nº 13.709/2018 (LGPD), classifica determinados tipos de dados pessoais como Dados Pessoais

Av. Levy Ramos Martins, 803 - Nova Brasília
CEP 88780-000 - Imbituba/SC - Telefone: (48) 3254 7200
contato@onix.seg.br

Sensíveis, em razão de sua natureza e da maior capacidade de causar danos, discriminações ou violações de direitos fundamentais ao seu Titular.

Dada sua criticidade, os Dados Pessoais Sensíveis devem receber tratamento prioritário e reforçado em termos de segurança da informação, controles internos, acesso restrito e mitigação de riscos.

4.1.3.1. Conceito de Dados Pessoais Sensíveis

São considerados Dados Pessoais Sensíveis, para fins desta Política, aqueles que revelem:

- Origem racial ou étnica;
- Opiniões políticas;
- Convicções religiosas ou filosóficas;
- Filiação a sindicato ou a organização de caráter religioso, filosófico ou político;
- Dados genéticos;
- Dados biométricos, tratados com o objetivo de identificar uma pessoa natural;
- Dados relacionados à saúde;
- Dados relativos à vida sexual ou à orientação sexual do Titular.

Esta classificação está em conformidade com o disposto no Artigo 5º, inciso II, combinado com o Artigo 11 da LGPD.

4.1.3.2. Tratamento Específico de Dados Sensíveis

O Tratamento de Dados Pessoais Sensíveis pela Onix somente poderá ocorrer nas hipóteses legais expressamente autorizadas, devendo observar:

- Consentimento específico e destacado do titular, salvo exceções legais;
- Cumprimento de obrigações legais ou regulatórias;
- Proteção da vida ou da incolumidade física do titular ou de terceiros;
- Tutela da saúde em procedimento realizado por profissionais ou serviços de saúde;
- Exercício regular de direitos, inclusive em contrato e processos judiciais, administrativos ou arbitrais.

Além disso, os Dados Sensíveis devem ser protegidos por:

- **Medidas técnicas rigorosas** (criptografia, controle de acesso reforçado, segregação de ambientes, etc.);
- **Restrições de acesso baseadas no princípio da necessidade (need-to-know basis)**;
- **Monitoramento contínuo** de incidentes de segurança e avaliação de riscos periódica;
- **Exclusão segura** ao término do tratamento, conforme as regras estabelecidas nesta Política e nas normas aplicáveis.

O descumprimento das diretrizes específicas aplicáveis ao Tratamento de Dados Pessoais Sensíveis poderá acarretar a aplicação de sanções disciplinares internas e responsabilidades administrativas, civis e criminais previstas em lei.

Av. Levy Ramos Martins, 803 - Nova Brasília
CEP 88780-000 - Imbituba/SC - Telefone: (48) 3254 7200
contato@onix.seg.br

4.1.3.3. Tratamento de Dados Pessoais de Crianças, Adolescentes e Idosos

O tratamento de dados pessoais de **crianças**, **adolescentes** e **idosos** deverá ocorrer **em caráter excepcionalíssimo**, sendo admitido apenas nas hipóteses estritamente necessárias, em conformidade com o princípio do melhor interesse do titular e as diretrizes estabelecidas pela **Lei Geral de Proteção de Dados (Lei nº 13.709/2018)**, bem como com os requisitos de segurança previstos nas normas **ISO/IEC 27001** e **ISO/IEC 27002**.

Nesses casos, o tratamento deverá observar os seguintes parâmetros:

- **Finalidade voltada ao melhor interesse do titular:** O tratamento somente poderá ocorrer visando beneficiar, direta ou indiretamente, a criança, o adolescente ou o idoso, não sendo admitidas finalidades que possam resultar em prejuízo ou discriminação.
- **Comunicação clara e acessível:** Todas as informações relativas ao tratamento de dados pessoais destinadas a estes públicos deverão ser prestadas de forma **clara, adequada e compreensível**, considerando as condições físico-motoras, perceptivas, sensoriais, intelectuais e mentais dos titulares, podendo ser utilizados recursos audiovisuais ou de tecnologia assistiva, sempre que necessário para assegurar o entendimento.
- **Consentimento específico e destacado:** Em se tratando de **dados pessoais de crianças**, é obrigatória a obtenção de **consentimento específico e em destaque** fornecido por, no mínimo, um dos pais ou pelo responsável legal, conforme disposto no artigo 14 da LGPD. Deverão ser mantidas públicas as informações acerca:
  - ✓ Dos tipos de dados coletados;
  - ✓ Da finalidade específica do tratamento;
  - ✓ Da forma e duração do tratamento;
  - ✓ Dos direitos assegurados aos titulares, conforme previsto na legislação aplicável.

O tratamento de dados pessoais desses grupos deverá observar, ainda, os princípios da **necessidade**, **segurança**, **transparência** e **não discriminação**, com a implementação de controles de segurança da informação compatíveis com a classificação sensível dos dados, nos termos das políticas internas da organização e das melhores práticas estabelecidas pelas normas internacionais de segurança.

4.1.4. Direitos dos Titulares

Em toda atividade de tratamento de dados pessoais, a Onix deverá adotar medidas apropriadas para garantir o pleno exercício dos direitos dos titulares, conforme previstos na Lei Geral de Proteção de Dados Pessoais (LGPD – Lei nº 13.709/2018).

Para tanto, observar-se-á:

- A verificação da identidade do titular requerente, por meio de procedimentos seguros e eficazes, de forma a mitigar riscos de acesso indevido às informações pessoais.
- O atendimento das requisições deverá ocorrer sempre sob a orientação e supervisão do Encarregado pelo Tratamento de Dados Pessoais, conforme previsto no art. 41 da LGPD.

Av. Levy Ramos Martins, 803 - Nova Brasília
CEP 88780-000 - Imbituba/SC - Telefone: (48) 3254 7200
contato@onix.seg.br

A Onix disponibiliza canal específico para o recebimento de solicitações de exercício de direitos dos titulares, o qual poderá ser acessado por meio do endereço eletrônico: dpo@onix.seg.br.

Eventuais decisões de recusa no atendimento às requisições deverão ser expressamente fundamentadas e previamente validadas pelo Encarregado, em consonância com a legislação vigente, as diretrizes internas de proteção de dados pessoais e os princípios de transparência e não discriminação.

O tratamento das solicitações de titulares deverá respeitar, ainda, os princípios de segurança da informação estabelecidos nas normas ISO/IEC 27001 e ISO/IEC 27002, garantindo-se a integridade, a confidencialidade e a disponibilidade dos dados pessoais envolvidos.

Direito	Descrição
Direito à Informação e ao Acesso	Ao titular, mediante sua expressa requisição, é garantido o direito de confirmação da existência de Tratamento de seus Dados Pessoais. A Onix 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, 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.
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.
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 estiver em desconformidade com as determinações da LGPD. Em hipótese de ocorrência de requisições de eliminação de Dados Pessoais, a Onix, considerando que nenhum direito possui caráter absoluto, deverá verificar se o Tratamento dos dados objeto de requisição se justifica em algumas das hipóteses de exceção previstas pela LGPD, caso em que a solicitação e, por consequência, o direito do Titular dos dados não deverá prevalecer.
Direito a 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 Onix deixar de observar e cumprir algumas das disposições trazidas na legislação que trata sobre o tema.
Direito a 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, os Dados Pessoais do Titular requerente devem ser desvinculados de dados de outros Titulares, e fornecidos em formato interoperável, tal como XLS, CSV ou JSON.
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.

4.1.5.Gestão de Descarte

Todo tratamento de dados pessoais deverá observar um processo formal de gestão de descarte de informações, assegurando que a Onix apenas mantenha dados pessoais armazenados pelo tempo estritamente necessário para o cumprimento da finalidade informada, no âmbito e limites técnicos das respectivas atividades.

O descarte deverá atender aos seguintes parâmetros:

- Retenção mínima necessária:

  Os dados pessoais deverão ser eliminados ou anonimizados em todas as fontes em que estiverem armazenados, sejam meios eletrônicos ou físicos, de acordo com as disposições estabelecidas nesta Política.
- Processo de descarte seguro:

  Os procedimentos de eliminação deverão adotar técnicas e mecanismos que impeçam o acesso

Av. Levy Ramos Martins, 803 - Nova Brasília
CEP 88780-000 - Imbituba/SC - Telefone: (48) 3254 7200
contato@onix.seg.br

não autorizado, a recuperação indevida ou o uso impróprio dos dados descartados, em conformidade com os controles exigidos pelas normas ISO/IEC 27001 e ISO/IEC 27002.

- Responsabilidade pelo descarte de mídias:

  O descarte de mídias físicas ou eletrônicas que contenham dados pessoais sensíveis deverá ser realizado sob a coordenação e validação da Área de Tecnologia da Informação (TI), garantindo-se a aplicação de métodos de destruição segura, compatíveis com o nível de criticidade da informação e os requisitos legais vigentes.
- Registro e evidência:

  Sempre que aplicável, o processo de descarte deverá ser documentado, de modo a permitir auditorias e assegurar a rastreabilidade das ações realizadas, em consonância com os princípios de prestação de contas e responsabilidade ("accountability") previstos na LGPD.

4.1.6.Compartilhamento de Dados Pessoais

O compartilhamento de dados pessoais com terceiros deverá ser regido por instrumentos jurídicos adequados, que estabeleçam de forma clara as garantias, responsabilidades e medidas necessárias à conformidade com a Lei Geral de Proteção de Dados Pessoais (LGPD – Lei nº 13.709/2018), além da observância às Políticas Corporativas de Privacidade, Proteção de Dados Pessoais e normas relacionadas.

Tais instrumentos devem contemplar, no mínimo:

- As finalidades específicas do compartilhamento de dados pessoais;
- As obrigações de proteção de dados impostas aos terceiros envolvidos;
- As medidas técnicas e administrativas a serem adotadas para garantir a segurança, integridade, confidencialidade e disponibilidade dos dados compartilhados, em conformidade com os requisitos estabelecidos nas normas ISO/IEC 27001 e ISO/IEC 27002;
- As previsões sobre direitos e deveres dos titulares, acesso, eliminação, correção e eventual responsabilização em caso de incidentes de segurança.

O compartilhamento de dados pessoais com terceiros deverá ocorrer, como regra, única e exclusivamente:

I. para a consecução da finalidade legítima que motivou a coleta inicial dos dados pessoais;
II. em estrita conformidade com a atividade que fundamenta a relação jurídica ou contratual existente entre a Onix e o terceiro.

Em qualquer hipótese, o compartilhamento deverá observar os princípios da necessidade, transparência, não discriminação e accountability, sendo vedado o uso dos dados pessoais compartilhados para finalidades distintas daquelas previamente autorizadas ou estabelecidas em contrato.

4.1.7.Representantes Externos

A contratação de representantes externos poderá representar **riscos potenciais** à Onix, especialmente no que tange à responsabilidade solidária ou subsidiária decorrente de incidentes de tratamento indevido de dados pessoais.

Considerando tal cenário, a Onix deverá adotar as seguintes medidas:

- **Instrumentalização Contratual:**

  Todos os instrumentos de contratação de representantes externos deverão conter cláusula

específica prevendo a **obrigatoriedade de observância** integral das diretrizes estabelecidas na presente **Política Corporativa de Privacidade e Governança de Dados Pessoais**, bem como nas demais políticas internas correlatas.

- **Responsabilização e Sanções:** Deverá ser previsto, ainda, que o não cumprimento das normas de privacidade e proteção de dados poderá ensejar a **rescisão contratual** e a **aplicação de penalidades**, sem prejuízo da apuração de perdas e danos.
- **Adoção de Medidas Técnicas e Administrativas:** Sempre que aplicável, os representantes externos deverão comprovar a implementação de **medidas técnicas e administrativas** aptas a proteger os dados pessoais tratados, em conformidade com as exigências da **Lei Geral de Proteção de Dados Pessoais (LGPD)** e das normas internacionais de segurança da informação, **ISO/IEC 27001** e **ISO/IEC 27002**.

O relacionamento com representantes externos deverá ser continuamente monitorado, de modo a garantir o cumprimento efetivo das obrigações assumidas e a preservação dos direitos dos titulares de dados pessoais.

5. TREINAMENTO

A Onix promoverá ações contínuas de treinamento e capacitação de seus colaboradores, fornecedores e parceiros internos, com o objetivo de assegurar a correta compreensão e aplicação das diretrizes estabelecidas nesta Política Corporativa de Privacidade e Governança de Dados Pessoais, bem como nas demais políticas e boas práticas de proteção de dados, segurança da informação e privacidade.

A realização dos treinamentos observará os seguintes princípios:

- Periodicidade e Atualização: A Onix poderá repetir ou realizar novos treinamentos sempre que julgar necessário, em especial nas seguintes hipóteses:

  - ✓ Atualizações legislativas ou regulatórias relevantes;
  - ✓ Alterações substanciais nas políticas internas;
  - ✓ Ocorrência de incidentes de segurança da informação;
  - ✓ Identificação de gaps de conhecimento ou riscos no processo de governança de dados.

- Adequação ao Público-Alvo:

  O conteúdo dos treinamentos será adaptado às funções e responsabilidades dos públicos envolvidos, garantindo que todos compreendam suas atribuições específicas no âmbito da proteção de dados pessoais e da segurança da informação.

- Registro e Controle:

  A participação em treinamentos será devidamente registrada, visando assegurar a rastreabilidade e a comprovação do cumprimento das obrigações de capacitação previstas na LGPD e nas normas ISO/IEC 27001 e ISO/IEC 27002.

Av. Levy Ramos Martins, 803 - Nova Brasília
CEP 88780-000 - Imbituba/SC - Telefone: (48) 3254 7200
contato@onix.seg.br

5.1. Tipos de Treinamentos

Público-Alvo	Tema Central	Formato	Observações
Todos os colaboradores	Reforço da Política de Privacidade e Segurança da Informação	EAD / Webinar gravado	Integração com novos colaboradores
Lideranças, Gestores de Área, TI, Jurídico, Compliance	Atualizações regulatórias e gestão de riscos em dados pessoais	Treinamento presencial ou online síncrono	Inclusão de simulações práticas
Todos os colaboradores	Boas práticas diárias de proteção de dados e gestão de riscos (ex.: phishing, vazamento de dados, incidentes)	Campanha interna + Quiz gamificado	Avaliação de retenção de conhecimento
Todos os colaboradores	Segurança Digital e Cultura de Proteção de Dados	Workshop + Envio de materiais visuais	Atividades lúdicas e de engajamento

6. NORMAS E DOCUMENTOS RELACIONADOS

O tratamento de dados pessoais no âmbito da Onix está sujeito, além das diretrizes estabelecidas na presente Política Corporativa de Privacidade e Governança de Dados Pessoais, à observância de outras normas e regulamentos aplicáveis, dentre os quais se destacam:

- Lei nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais (LGPD);
- Lei nº 12.965/2014 – Marco Civil da Internet;
- Regulamentos, diretrizes e normativas emitidas pela Autoridade Nacional de Proteção de Dados Pessoais (ANPD);
- Leis e regulamentações nacionais ou estrangeiras vigentes nos países onde a Onix atue, desde que aplicáveis às suas operações de tratamento de dados pessoais.

Adicionalmente, aplicam-se as boas práticas e controles estabelecidos nas normas internacionais de gestão de segurança da informação, notadamente:

- ISO/IEC 27001 – Sistema de Gestão de Segurança da Informação (SGSI);
- ISO/IEC 27002 – Código de práticas para controles de segurança da informação.

Em caso de identificação de conflito ou divergência entre as normas aplicáveis e as diretrizes internas, a situação deverá ser imediatamente submetida à análise da Assessoria Jurídica e do Encarregado pelo Tratamento de Dados Pessoais (DPO) da Onix, para definição da interpretação ou medida corretiva adequada.

Av. Levy Ramos Martins, 803 - Nova Brasília
CEP 88780-000 - Imbituba/SC - Telefone: (48) 3254 7200
contato@onix.seg.br

7. DISPOSIÇÕES GERAIS

Esta Política Corporativa de Privacidade e Governança de Dados Pessoais deverá ser revisada, no mínimo, anualmente, ou sempre que houver a necessidade de atualização em decorrência de:

- Alterações legislativas ou regulatórias aplicáveis;
- Mudanças nos critérios definidos pelas demais normas e políticas internas da Onix;
- Identificação de melhorias decorrentes de auditorias internas, externas ou eventos relacionados à segurança da informação e proteção de dados pessoais.

As disposições desta Política, bem como das demais normas, procedimentos e políticas relacionadas ao tratamento de dados pessoais, encontram-se disponíveis para consulta no ERP da Qualidade e no Site da Onix. Em caso de indisponibilidade do acesso, os documentos poderão ser solicitados diretamente ao Encarregado pelo Tratamento de Dados Pessoais (DPO), por meio do endereço eletrônico: dpo@onix.seg.br.

Esta Política entra em vigor na data de sua publicação oficial, revogando-se quaisquer disposições internas em contrário que tenham tratado anteriormente da matéria.

Av. Levy Ramos Martins, 803 - Nova Brasília
CEP 88780-000 - Imbituba/SC - Telefone: (48) 3254 7200
contato@onix.seg.br

ANEXO I - PAPÉIS E CONTATOS IMPORTANTES DO PROGRAMA PRIVACIDADE E GOVERNANÇA DE DADOS PESSOAIS DA ONIX

Encarregado de Proteção de Dados:
Jurídico e TI

Responsável pela área de Tecnologia da Informação:
Rafael Faust Rodrigues

Assessoria Jurídica:
Dr. Daniel Vinício Arantes Neto

Responsável pela área Administrativa:
Katyuse Dandolini

Participantes do Comitê de Privacidade:
Fernanda Ortiz
Katyuse Dandolini
Ingrid Borba
Juliana Nascimento
Rafael Faust Rodrigues
William Vara
Dr. Daniel Vinício Arantes Neto (terceirizado)

Av. Levy Ramos Martins, 803 - Nova Brasília
CEP 88780-000 - Imbituba/SC - Telefone: (48) 3254 7200
contato@onix.seg.br