Título do Documento:

Política de Privacidade de Dados Pessoais

Informações Importantes

Copyright

FENOX TECNOLOGIA LTDA
Avenida Salmão, 325 - Salas 91 a 96 e 101
São José dos Campos - SP
CEP: 12246-260 - Brasil
(12) 98134-2294

www.fenoxtec.com.br
fenox@fenoxtec.com.br

INFORMAÇÕES DO DOCUMENTO

DADOS DO DOCUMENTO			
Título do Documento: Política de Privacidade de Dados Pessoais **Título do Resumido:** P.P.D.P.			
CONSIDERANDO a necessidade de estabelecer, manter e controlar os processos relacionados à continuidade das operações de tratamento de dados pessoais, este documento estabelece diretrizes e responsabilidades para prevenção, gestão de resposta e recuperação em situações de contingência, garantindo a integridade, disponibilidade e proteção de dados pessoais, bem como a rastreabilidade das atividades e a retomada controlada, em conformidade com a Lei de Proteção de Dados Pessoais (LGPD), ISO/IEC 27701 e ISO 22301.			
Tipo: Documento publico	**Numeração: 26021856-P-SP**		**Páginas**:29
Área Emitente: Qualidade / Operações	**Distribuição**: ☒ Interno		☒ Externo
Distribuído por: Qualidade	**Autor:** Leonardo Machado	**Cliente:** FENOX	**Data:** 09/02/2026
Palavras Chaves: P.P.D.P.	**Categoria:** Documento publico		

REFERÊNCIA
Documentos de Referência: Manual de Sistema de Gestão Integrado

DADOS DO PROJETO	
Cliente: FENOX TECNOLOGIA	**Projeto**: Unificação do padrão de codificação e armazenamento da documentação da FENOX, com foco na proteção de dados pessoais, rastreabilidade, controle de acesso e conformidade com a Política de Privacidade e Segurança da Informação.

ELABORAÇÃO / REVISÃO

Rev.	Data	Ordem	Departamento	Quem	Justificativa	Status
00	24/02/2026	Elaboração	Qualidade	LM	ISO 27701:2019	P/ Aprovação
01	18/03/2026	Revisão	Diretoria	JLA	Revisão de texto	Aprovado
02	09/06/26	Revisão	Qualidade	LRM	Inclusão de texto para controle da SoA A.12.1 Localização geográfica do DP	Aprovado

Índice

1 PRIVACIDADE E PROTEÇÃO DE DADOS 7
2 OBJETIVOS 7
2.1 GARANTIR CONFORMIDADE LEGAL E NORMATIVA: 7
2.2 INTEGRAR PRIVACIDADE AO SISTEMA DE GESTÃO INTEGRADO (SGI): 7
2.3 FORTALECER A CONFIANÇA E A TRANSPARÊNCIA NAS RELAÇÕES: 7
2.4 PREVENIR INCIDENTES E MITIGAR RISCOS DE PRIVACIDADE: 7
2.5 DEFINIR PAPÉIS, RESPONSABILIDADES E GOVERNANÇA: 7
2.6 PROMOVER A CULTURA DA PRIVACIDADE E A CAPACITAÇÃO CONTÍNUA: 7
2.7 ASSEGURAR O TRATAMENTO ÉTICO E PROPORCIONAL DOS DADOS PESSOAIS: 8
2.8 SUSTENTAR A MELHORIA CONTÍNUA DO SISTEMA DE GESTÃO DA PRIVACIDADE DA INFORMAÇÃO (SGPI): 8
2.9 INCORPORAR A PRIVACIDADE NA TECNOLOGIA E NOS PRODUTOS FENOX: 8
2.10 REFORÇAR A RESPONSABILIDADE SOCIAL E CORPORATIVA: 8
2.11 PROTEÇÃO DE DADOS PESSOAIS E CORPORATIVOS 8
3 SIGLAS / DEFINIÇÕES 8
4 PROCEDIMENTOS DE CONSENTIMENTO 11
5 ESCOPO E APLICABILIDADE 12
6 ABRANGÊNCIA ORGANIZACIONAL 12
7 ABRANGÊNCIA TECNOLÓGICA 12
8 ABRANGÊNCIA FÍSICA 12
9 ABRANGÊNCIA CONTRATUAL E DE TERCEIROS 13
9.1 SUBCONTRATADOS 13
9.2 RELAÇÃO CONTROLADOR/OPERADOR E INSTRUÇÕES DOCUMENTADAS (ISO/IEC 27701) 13
9.2.1 DEVOLUÇÃO OU DESTRUIÇÃO PÓS-CONTRATO 13
9.2.2 NOTIFICAÇÕES LEGAIS DE DIVULGAÇÃO 14
9.2.3 DIVULGAÇÃO LEGAL DE DADOS PESSOAIS 14
9.2.4 CLASSIFICAÇÃO DE DADOS 14
9.2.5 CONTROLADOR CONJUNTO 14
9.3 CONTROLE CONJUNTO 14
9.4 PROIBIÇÃO DE MARKETING (OPERADOR) 14
9.5 RESTRIÇÃO DE USO COMERCIAL 14
10 ESCOPOS CERTIFICADOS DO SGI FENOX 15
10.1.1 NORMA ABNT NBR ISO 9001:2015 15

10.1.2 NORMA ABNT NBR ISO/IEC 20000-1:2020 15
10.1.3 NORMA ABNT NBR ISO/IEC 27001:2022 15
10.1.4 NORMA ABNT NBR ISO 22301:2020 15
10.1.5 NORMA ABNT NBR ISO/IEC 27701:2019 (SGPI) 16
10.1.6 DIRETRIZES DE SEGURANÇA PARA SERVIÇOS EM NUVEM – ABNT NBR ISO/IEC 27017:2016 16
10.1.7 DIRETRIZES DE PROTEÇÃO DE DADOS PESSOAIS EM NUVEM – ABNT NBR ISO/IEC 27018:2025 16
11 EXCLUSÃO DE ESCOPO 16
12 PRINCÍPIOS DA PRIVACIDADE E PROTEÇÃO DE DADOS 18
12.1 PROTEÇÃO DE INFORMAÇÕES 18
13 BASE LEGAL E FINALIDADES DE TRATAMENTO 18
14 RETENÇÃO E PRESERVAÇÃO DE DADOS 19
14.1 FORNECIMENTO DE CÓPIA ESTRUTURADA DOS DADOS PESSOAIS 19
14.2 MÍDIA DE ARMAZENAMENTO 19
14.2.1 GESTÃO DE MÍDIAS E DESCARTE FÍSICO 20
14.3 DESCARTE DE EQUIPAMENTO 20
14.4 TRANSFERÊNCIAS INTERNACIONAIS 20
15 TRATAMENTO DE DADOS PESSOAIS E SENSÍVEIS 21
16 DIREITO DOS TITULARES 21
16.1 DECISÕES AUTOMATIZADAS 21
16.2 NOTIFICAÇÃO A TERCEIROS 21
17 GERENCIAMENTO DE INCIDENTES DE SEGURANÇA 21
17.1 REGISTRO DE DIVULGAÇÃO A TERCEIROS 22
17.2 REGISTRO DE CONSENTIMENTO DO TITULAR 22
17.2.1 NATUREZA DA COLETA: 22
17.2.2 OBTENÇÃO DO CONSENTIMENTO 22
17.2.3 RASTREABILIDADE 22
17.2.4 INTEGRAÇÃO COM O ROPA 23
18 GOVERNANÇA E RESPONSABILIDADE 23
18.1.1 PAPÉIS 23
18.1.2 CANAIS 23
18.1.3 RESPONSABILIZAÇÃO 23
18.1.4 CAPACITAÇÃO E SENSIBILIZAÇÃO 23
18.2 REVISÃO INDEPENDENTE 23
19 REGISTRO DAS OPERAÇÕES DE TRATAMENTO (ROPA) 23
19.1 EXEMPLO DE APLICAÇÃO PRÁTICA (ROPA) 24

20 INTEGRAÇÃO OPERACIONAL ENTRE ROPA, DPIA E PLANO DE INCIDENTES 24
20.1.1 DOCUMENTOS E PAPÉIS NA INTEGRAÇÃO 24
20.2 GESTÃO AUDITÁVEL DE INCIDENTES 25
20.3 fundamentos da integração no sgpi fenox 25
21 EVIDÊNCIAS E AUDITORIA DE PRIVACIDADE 25
21.1.1 EVIDÊNCIAS DE CONFORMIDADE 25
21.1.2 AUDITORIA E MELHORIA CONTÍNUA 26
21.1.3 EVIDÊNCIAS MÍNIMAS 26
21.1.4 ANÁLISE CRÍTICA 26
21.1.5 INDICADORES 26
21.2 POLÍTICAS AMBIENTAIS DE SEGURANÇA 26
21.2.1 MESA LIMPA E TELA LIMPA 26
21.3 POLÍTICA DE BACKUP E RECUPERAÇÃO 26
22 DECISÕES AUTOMATIZADAS E IA 26
23 DESENVOLVIMENTO SEGURO 27
23.1 REFERÊNCIA À POLÍTICA DE DESENVOLVIMENTO SEGURO 27
24 DIREÇÃO 27
24.1 INSTRUÇÃO ILEGAL 27
24.2 INSTRUÇÃO ILEGAL/ ASSISTÊNCIA AO CONTROLADOR 27
25 ANEXO A 28
25.1 ATO DE DESIGNAÇÃO DO ENCARREGADO DE DADOS (DPO) E CONSTITUIÇÃO DO COMITÊ DE SEGURANÇA E PRIVACIDADE 28
25.2 ENCARREGADO DE DADOS (DPO) 28
25.3 COMITÊ DE SEGURANÇA E PRIVACIDADE 28
25.4 COMPOSIÇÃO DO COMITÊ 28
25.5 COMPETÊNCIAS DO COMITÊ 29
25.6 VIGÊNCIA E REVISÃO 29
26 PERIODICIDADE DE REVISÃO 29

1 PRIVACIDADE E PROTEÇÃO DE DADOS

A Fenox Tecnologia estabelece esta Política de Privacidade e Proteção de Dados como parte do Sistema de Gestão Integrada (SGI), com o objetivo de assegurar conformidade com a legislação aplicável (LGPD) e com as normas ABNT NBR ISO/IEC 27701:2019, extensão da ISO/IEC 27001:2022. A Política orienta o tratamento ético, transparente e seguro de dados pessoais, inclusive dados sensíveis, fortalecendo a governança de privacidade diante das demandas da transformação digital e promovendo confiança junto a clientes, colaboradores, parceiros e órgãos reguladores.

2 OBJETIVOS

A Política de Privacidade e Proteção de Dados da Fenox Tecnologia tem como objetivo orientar e padronizar o tratamento de dados pessoais e sensíveis, assegurando que todas as etapas – da coleta ao descarte – ocorram de forma segura, transparente e em conformidade com a legislação aplicável. A Política reforça a privacidade como elemento essencial da qualidade e da segurança da informação, servindo como referência prática para colaboradores, prestadores e parceiros, com base na LGPD e na ABNT NBR ISO/IEC 27701:2019.

2.1 GARANTIR CONFORMIDADE LEGAL E NORMATIVA:

Assegurar que a coleta, o armazenamento, o uso, o compartilhamento e a exclusão de dados pessoais realizados pela Fenox ocorram dentro das bases legais da LGPD e em conformidade com os controles definidos pela ISO/IEC 27701 e ISO/IEC 27001. Assim, os dados serão tratados para finalidades legítimas, com base legal registrada e acesso restrito a pessoas autorizadas.

2.2 INTEGRAR PRIVACIDADE AO SISTEMA DE GESTÃO INTEGRADO (SGI):

Incorporar a gestão de privacidade como componente permanente do SGI Fenox, integrando-a às políticas de Segurança da Informação, Qualidade e Serviços de TI. Dessa forma, a privacidade deixa de ser uma iniciativa isolada e passa a fazer parte do planejamento, da execução e da melhoria contínua de todos os processos corporativos.

2.3 FORTALECER A CONFIANÇA E A TRANSPARÊNCIA NAS RELAÇÕES:

Demonstrar a clientes, colaboradores, fornecedores e órgãos públicos que a Fenox adota condutas éticas e práticas adequadas para proteger os dados que lhe são confiados. A empresa busca fortalecer a credibilidade e a transparência, mantendo canais de comunicação claros sobre o tratamento de dados pessoais e atendendo, de forma organizada e tempestiva, às solicitações dos titulares.

2.4 PREVENIR INCIDENTES E MITIGAR RISCOS DE PRIVACIDADE:

Implementar medidas de prevenção, detecção, resposta e correção de incidentes que possam comprometer a confidencialidade, integridade ou disponibilidade de dados pessoais. A Fenox adota práticas de contingência e medidas de contenção que apoiam a continuidade das operações e a proteção dos titulares, incluindo, quando aplicável, comunicação e registros do incidente.

2.5 DEFINIR PAPÉIS, RESPONSABILIDADES E GOVERNANÇA:

Estabelecer uma estrutura de governança clara para o tratamento de dados, com papéis e responsabilidades definidos entre a Direção, o Encarregado (DPO), a área de Infraestrutura, o Jurídico e a Qualidade. Dessa forma, as atividades de tratamento passam a ser conduzidas de maneira organizada, controlada e acompanhada, com definição de responsáveis e monitoramento contínuo.

2.6 PROMOVER A CULTURA DA PRIVACIDADE E A CAPACITAÇÃO CONTÍNUA:

Promover treinamentos, campanhas de conscientização e materiais orientativos para que colaboradores compreendam como lidar corretamente com dados pessoais no dia a dia. O objetivo é tornar a privacidade um valor prático e constante, aplicado desde o atendimento ao cliente até o desenvolvimento e a operação de sistemas.

2.7 ASSEGURAR O TRATAMENTO ÉTICO E PROPORCIONAL DOS DADOS PESSOAIS:

Assegurar que os dados pessoais sejam tratados de forma ética, justa e proporcional, limitados ao necessário para finalidades legítimas, evitando coletas excessivas e usos indevidos. Isso se aplica a dados de clientes, colaboradores, prestadores e às informações relacionadas a registros de vistoria veicular tratadas nos sistemas da Fenox.
A Fenox adota práticas para manter a qualidade, precisão e atualização dos dados sob sua guarda, realizando correções quando necessário e preservando registros de alterações relevantes, quando aplicável.

2.8 SUSTENTAR A MELHORIA CONTÍNUA DO SISTEMA DE GESTÃO DA PRIVACIDADE DA INFORMAÇÃO (SGPI):

Realizar auditorias periódicas, revisões de eficácia e análises críticas para assegurar a evolução dos controles de privacidade e a conformidade com a LGPD e as normas ISO aplicáveis. O SGPI integra o ciclo de melhoria contínua da Fenox e se conecta ao Sistema de Gestão da Qualidade e ao Sistema de Gestão de Serviços (ISO/IEC 20000-1).

2.9 INCORPORAR A PRIVACIDADE NA TECNOLOGIA E NOS PRODUTOS FENOX:

Incorporar os princípios de *Privacy by Design* (Privacidade desde a concepção) e *Privacy by Default* (configuração padrão voltada à proteção de dados) nas soluções tecnológicas da Fenox, como sistemas de vistoria, *backoffice*, portais e integrações com órgãos reguladores. Assim, novas funcionalidades passam a ser desenvolvidas já considerando requisitos de privacidade e segurança, reduzindo a necessidade de ajustes corretivos posteriores.

2.10 REFORÇAR A RESPONSABILIDADE SOCIAL E CORPORATIVA:

Reforçar a imagem da Fenox como uma empresa ética, confiável e comprometida com a proteção de dados pessoais e corporativos, tornando a conformidade um diferencial competitivo e um elemento de qualidade nos contratos e serviços.

2.11 PROTEÇÃO DE DADOS PESSOAIS E CORPORATIVOS

Consolidar a proteção de dados pessoais e corporativos como padrão de qualidade nos serviços e contratos. Em síntese, esta Política orienta as áreas da Fenox, convertendo a LGPD e as normas ISO em práticas de proteção de dados. Assim, a privacidade é incorporada à cultura organizacional, aos processos e à inovação tecnológica da empresa, tornando a conformidade um diferencial competitivo e um requisito de qualidade em todos os contratos e serviços.

3 SIGLAS / DEFINIÇÕES

	Definição / Descrição
Dado Pessoal	Informação relacionada a uma pessoa natural identificada ou identificável. Inclui nome, CPF, e-mail, telefone, endereço, IP ou geolocalização.

Dado Pessoal Sensível	Informação sobre origem racial, convicção religiosa, opinião política, saúde, vida sexual, dados genéticos ou biométricos. Requer controles adicionais.
Titular de Dados	Pessoa natural a quem se referem os dados pessoais (clientes, colaboradores, parceiros etc.).
Tratamento de Dados	Qualquer operação com dados pessoais: coleta, armazenamento, uso, transmissão, compartilhamento ou descarte.
Controlador	Entidade que define as finalidades e os meios de tratamento de dados pessoais.
Operador	Entidade que realiza o tratamento de dados pessoais sob orientação e diretrizes do controlador.
Encarregado (DPO)	Ponto de contato entre a organização, os titulares e a ANPD. Orienta sobre práticas de conformidade.
ANPD	Autoridade Nacional de Proteção de Dados. Órgão responsável por fiscalizar o cumprimento da LGPD.
Consentimento	Manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento para uma finalidade específica.
Base Legal	Fundamento jurídico que autoriza o tratamento (contrato, obrigação legal, legítimo interesse, consentimento etc.).
Violação de Dados	Evento de segurança que resulta em acesso, alteração ou destruição não autorizada de dados pessoais.
Privacy by Design	Princípio de incorporar a privacidade desde o planejamento inicial de sistemas e processos.
Privacy by Default	Configuração padrão que garante a coleta apenas do mínimo necessário de dados.
RoPA	*Record of Processing Activities*. Registro formal das operações de tratamento de dados pessoais.
DPIA	*Data Protection Impact Assessment*. Relatório de impacto à proteção de dados para avaliar riscos e consequências.
Anonimização	Processo técnico que impossibilita a identificação do titular (o dado deixa de ser considerado pessoal).
Pseudonimização	Substituição de dados identificáveis por códigos, permitindo reidentificação apenas sob condições controladas.

Titular Requerente	Pessoa natural que exerce seus direitos (acesso, correção, exclusão) junto à organização.
LGPD	Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018).
SGPI	Sistema de Gestão da Privacidade da Informação (baseado na ISO/IEC 27701).
SGI	Sistema de Gestão Integrado (reúne ISO 9001, 20000-1, 27001 e 27701).
Sistema Fenox	Plataforma tecnológica para vistorias veiculares e processos tecnológicos com controles auditáveis.
Data Center / Nuvem	Infraestrutura para processamento e armazenamento de dados em provedores certificados.
Vulnerabilidade	Fragilidade técnica ou humana que pode ser explorada para comprometer a segurança.
Risco de Privacidade	Possibilidade de evento negativo aos direitos dos titulares; avaliado no contexto do SGPI.
Mitigação de Risco	Adoção de medidas para reduzir a probabilidade ou o impacto de riscos à privacidade.
Auditoria de Privacidade	Avaliação sistemática e independente da conformidade com a LGPD e normas ISO.
Colaboradores	Empregados, estagiários e prestadores com acesso autorizado a dados e sistemas.
API	*Application Programming Interface*. Integra sistemas garantindo segurança e rastreabilidade.
AD	*Active Directory*. Gerencia autenticação e permissões de acesso em ambiente corporativo.
CFTV	Circuito Fechado de Televisão. Monitoramento de imagens para segurança física.
DLP	*Data Loss Prevention*. Tecnologias para evitar vazamento ou uso indevido de informações.
DNS	*Domain Name System*. Sistema de resolução de nomes para tradução de endereços IP.
EPI	Equipamento de Proteção Individual. Inclui práticas de segurança física e controle de acesso.

HD	*Hard Disk*. Dispositivo físico de armazenamento; requer descarte seguro e criptografia.
HTTP / HTTPS	Protocolos de comunicação web. O HTTPS assegura transmissão criptografada.
IPS	*Intrusion Prevention System*. Sistema que detecta e bloqueia tráfego malicioso em tempo real.
ISO / IEC	Entidades internacionais de padronização técnica (ex: ISO/IEC 27001).
LAN / WAN	Redes locais (LAN) ou de longa distância (WAN) com políticas de monitoramento.
NDA	*Non-Disclosure Agreement*. Acordo de confidencialidade e sigilo entre as partes.
NIST	*National Institute of Standards and Technology*. Referência em padrões de segurança de TI.
PCI-DSS	Padrão de segurança para transações e dados de cartões de pagamento.
RAID	Tecnologia de redundância em discos rígidos para tolerância a falhas.
REST	Arquitetura de APIs para troca estruturada e segura de dados via HTTP.
SAN	*Storage Area Network*. Rede dedicada para armazenamento de alta disponibilidade.
SGSI	Sistema de Gestão da Segurança da Informação (baseado na ISO/IEC 27001).
SLA	*Service Level Agreement*. Acordo que define níveis de serviço e prazos técnicos.
SMTP	Protocolo para envio de e-mails; exige criptografia para segurança.
SQL	Linguagem para gestão de bancos de dados sob diretrizes de controle de acesso.
TLS / SSL	Protocolos de segurança que criptografam a comunicação entre sistemas.
VPN	*Virtual Private Network*. Túnel criptografado para acesso remoto seguro.
WAF	*Web Application Firewall*. Proteção contra-ataques direcionados a aplicações web.
XML / JSON	Formatos estruturados para intercâmbio de dados entre sistemas.
2FA / MFA	Autenticação de dois ou múltiplos fatores para elevar a segurança de acesso.

4 PROCEDIMENTOS DE CONSENTIMENTO

Quando a base legal do tratamento for o consentimento**,** a Fenox obtém a manifestação livre, informada e inequívoca do titular por meio de termo físico de consentimento, assinado no momento de

ingresso/contratação (quando aplicável), contendo as finalidades do tratamento e orientação sobre a possibilidade de revogação.

O termo assinado é arquivado na pasta individual do colaborador (repositório do RH), como evidência do consentimento. No Podio/SGPI ficam disponíveis esta Política e o modelo do termo de consentimento utilizado, para padronização e referência interna. O DPO acompanha periodicamente a adequação do modelo e do processo de arquivamento.

5 ESCOPO E APLICABILIDADE

Esta Política de Privacidade e Proteção de Dados aplica-se a todas as atividades de tratamento de dados pessoais realizadas sob responsabilidade da Fenox Tecnologia Ltda., abrangendo operações em que a organização atue como controladora e/ou operadora**.**

O escopo contempla ambientes físicos e digitais, sistemas corporativos, infraestruturas tecnológicas e processos organizacionais que envolvam coleta, uso, armazenamento, compartilhamento, transmissão, análise, manutenção e descarte de dados pessoais, inclusive dados sensíveis, quando aplicável.

6 ABRANGÊNCIA ORGANIZACIONAL

Esta Política abrange todas as áreas administrativas, operacionais e técnicas da Fenox – incluindo Infraestrutura, Desenvolvimento, Qualidade, Suporte Técnico, Mesa de Análise, Comercial, Jurídico e Recursos Humanos – sempre que realizarem, direta ou indiretamente, atividades de tratamento de dados pessoais.

A Política também se aplica a todas as pessoas que, por vínculo contratual ou de relação de colaboração, tenham acesso a dados pessoais sob custódia da Fenox, independentemente do tipo de vínculo, função ou nível hierárquico.

Inclui, ainda, os dados pessoais tratados no contexto da prestação de serviços de tecnologia, vistoria, *backoffice*, integração com órgãos públicos e gestão de sistemas contratados. Quando atuar em nome de terceiros, a Fenox observará as diretrizes de privacidade, confidencialidade e segurança previstas nesta Política.

Por fim, esta Política contempla os titulares cujos dados são tratados nos sistemas da Fenox, como vistoriadores, representantes de empresas credenciadas, clientes finais e demais usuários das plataformas digitais da empresa.

7 ABRANGÊNCIA TECNOLÓGICA

Esta Política aplica-se a todos os sistemas, plataformas, aplicações, bancos de dados, interfaces e APIs desenvolvidos, hospedados ou operados pela Fenox, incluindo:

- **Sistema Fenox** (vistoria, laudos e relatórios);
- **Portal BackOffice** (gestão web e administrativa);
- **Ambientes de integração** com DETRAN e órgãos públicos;
- **Soluções hospedadas** em Data Centers e ambientes de nuvem contratados;
- **Sistemas internos** de gestão corporativa e comunicação (ex.: e-mails, *SharePoint*, Podio, ERP).

A Política também se estende aos ambientes de desenvolvimento, homologação e produção, considerando que todos podem conter dados pessoais (inclusive para testes), sujeitos às mesmas diretrizes de privacidade e segurança da informação.

8 ABRANGÊNCIA FÍSICA

Aplica-se também aos ambientes físicos corporativos, incluindo:
• Estações de trabalho, copa, salas de reunião e áreas técnicas;
• Equipamentos que armazenem ou processem informações pessoais;
• Documentos impressos ou formulários físicos que contenham dados pessoais;
• Ambientes monitorados por CFTV, com gravação e retenção de imagens de pessoas.

Todos os espaços físicos sob gestão da Fenox devem manter condições adequadas de segurança, controle de acesso e confidencialidade, compatíveis com o nível de sensibilidade das informações tratadas.

9 ABRANGÊNCIA CONTRATUAL E DE TERCEIROS

Os compromissos de privacidade e proteção de dados previstos nesta Política aplicam-se também a fornecedores, parceiros, subcontratados e demais terceiros sempre que houver tratamento ou compartilhamento de dados pessoais relacionado às atividades da Fenox. Nessas situações, a relação deve ser formalizada por instrumento adequado (contrato e/ou cláusulas específicas de proteção de dados) e, quando houver acesso a dados pessoais, também por compromisso de confidencialidade (NDA ou cláusula equivalente), assegurando padrões de privacidade e segurança compatíveis com os exigidos pela Fenox.

9.1 SUBCONTRATADOS

A utilização de subcontratados que realizem tratamento de dados pessoais, quando aplicável, será previamente informada ao cliente.
A inclusão ou substituição de subcontratados ocorrerá conforme previsão contratual e mediante comunicação ao cliente, assegurando, quando previsto, o direito de oposição nos termos do contrato.

9.2 RELAÇÃO CONTROLADOR/OPERADOR E INSTRUÇÕES DOCUMENTADAS (ISO/IEC 27701)

Para assegurar a governança e a rastreabilidade sobre o ciclo de vida dos dados, a Fenox formaliza os papéis exercidos (Controladora e/ou Operadora) e as instruções aplicáveis ao tratamento:

- **Fenox como Operadora:** Quando a Fenox atua em nome de clientes, o tratamento de dados pessoais ocorre conforme **instruções documentadas**, consolidadas em contratos, aditivos técnicos, escopos de serviços e registros de solicitações (quando aplicável). Nessas situações, a Fenox presta suporte ao Controlador, conforme previsto contratualmente, em temas como atendimento a solicitações de titulares, incidentes e auditorias.

- **Fenox como Controladora:** Quando a Fenox define as finalidades e os meios de tratamento (ex: gestão de RH ou vistorias próprias), ela mantém os registros aplicáveis de governança (ex.: RoPA e quando necessário, relatório de impacto/DPIA) e assegura que subcontratados/suboperadores observem as diretrizes desta Política.

- **Referência Cruzada:** Para cada operação registrada, é indicado o papel exercido pela Fenox (Controladora ou Operadora), a base legal aplicável e o documento de referência (contrato/instrução), assegurando transparência e rastreabilidade.

- **Identificação do papel no Registro de Tratamento (RoPA):** para cada operação de tratamento registrada no RoPA, é identificado explicitamente o papel exercido pela Fenox (Controladora ou Operadora), a base legal aplicável e as responsabilidades associadas, assegurando transparência, rastreabilidade e conformidade com a LGPD e com os requisitos da ISO/IEC 27701.

9.2.1 DEVOLUÇÃO OU DESTRUIÇÃO PÓS-CONTRATO

Ao término da vigência contratual, a Fenox poderá manter sob sua guarda dados pessoais e registros de vistorias pelo prazo necessário ao cumprimento de obrigações legais e regulatórias, incluindo exigências de fiscalização de órgãos de trânsito (ex.: DETRAN/SENATRAN), quando aplicável. A eliminação definitiva

ocorrerá após o transcurso dos prazos aplicáveis e mediante descarte seguro, preservando-se, durante todo o período de retenção, a confidencialidade e a integridade das informações.

9.2.2 NOTIFICAÇÕES LEGAIS DE DIVULGAÇÃO

Caso receba solicitações legais, judiciais ou administrativas de divulgação de dados pessoais, a Fenox, quando atuar como Operadora, notificará o Controlador (cliente) tão logo possível, salvo se houver vedação legal. A Fenox não atenderá solicitações sem fundamento jurídico válido e, diante de ordem válida, limitará a divulgação ao mínimo necessário, registrando o evento e comunicando o Controlador conforme aplicável.

9.2.3 DIVULGAÇÃO LEGAL DE DADOS PESSOAIS

Quando a Fenox, na condição de Operadora, receber ordem judicial ou administrativa válida para divulgação de dados pessoais, deverá:
I. **Registrar** a solicitação (órgão requisitante, data, base legal e categoria de dados solicitados);
II. **Comunicar** o Controlador (cliente) sobre a requisição, sempre que permitido por lei; e
III. **Adotar medidas cabíveis** de preservação de sigilo e limitação do compartilhamento, quando aplicável, sem prejuízo do cumprimento de determinação judicial.
Os registros relacionados à divulgação compulsória serão mantidos conforme a governança interna de privacidade (ex.: sob acompanhamento do DPO).

9.2.4 CLASSIFICAÇÃO DE DADOS

As informações sob responsabilidade da Fenox devem ser classificadas conforme seu nível de sensibilidade (ex.: Pública, Interna, Confidencial e Restrita), com critérios definidos internamente. Dados pessoais devem receber classificação compatível com seu risco e sensibilidade, e os controles de proteção e retenção devem ser proporcionais a essa classificação.

9.2.5 CONTROLADOR CONJUNTO

Quando houver situações de controladoria conjunta em projetos compartilhados, a Fenox formalizará Acordos de Controladores Conjuntos, definindo responsabilidades, finalidades e a forma de atendimento aos direitos dos titulares, assegurando transparência e governança conforme LGPD e requisitos aplicáveis da ISO/IEC 27701.

9.3 CONTROLE CONJUNTO

Quando a Fenox atuar em conjunto com outra entidade no tratamento de dados pessoais (controladores conjuntos), será formalizado acordo específico entre as partes, definindo responsabilidades e obrigações de cada co-controlador, inclusive quanto à transparência aos titulares.

Esse acordo indicará como serão prestadas as informações aos titulares e como será realizado o atendimento aos seus direitos, conforme aplicável. A existência de controladoria conjunta e as responsabilidades pactuadas serão registradas nos controles internos pertinentes (ex.: RoPA), garantindo rastreabilidade.

9.4 PROIBIÇÃO DE MARKETING (OPERADOR)

A Fenox não utilizará dados pessoais tratados em nome do cliente para fins próprios de marketing ou publicidade, salvo quando houver consentimento específico e independente do titular, quando aplicável, e conforme a legislação.

9.5 RESTRIÇÃO DE USO COMERCIAL

Os dados pessoais coletados para o cumprimento de obrigações regulatórias (como vistorias vinculadas ao DETRAN) possuem finalidade específica e vinculada. É proibido utilizar, compartilhar ou cruzar essas bases de dados para fins de marketing, publicidade ou prospecção comercial, salvo mediante consentimento específico, destacado e inequívoco do titular, quando aplicável.

10 ESCOPOS CERTIFICADOS DO SGI FENOX

10.1.1 NORMA ABNT NBR ISO 9001:2015

Português:
"Prestação de serviços de suporte tecnológico e de gestão para a captura, armazenamento, integração de dados e de imagens para a emissão de Laudo de Vistoria Veicular fixa e/ou móvel, de acordo com as normatizações dos Órgãos de Trânsito pertinentes."

Inglês:
"Provision of technological support and management services for the capture, storage, integration of data and images for the issuance of a Vehicle Inspection Report, fixed and/or mobile, in accordance with the regulations of the relevant Traffic Bodies.

10.1.2 NORMA ABNT NBR ISO/IEC 20000-1:2020

Português:
"O Sistema de Gestão de Serviços que suporta a entrega dos serviços de vistoria fixa e móvel, realizadas por Empresas Credenciadas de Vistoria (ECV), mediante a homologação de Sistemas Informatizados pelos Departamentos Estaduais de Trânsito (DETRAN), a partir das instalações da empresa em São José dos Campos, de acordo com o catálogo de serviços."

Inglês:
"The Service Management System that supports the delivery of fixed and mobile inspection services, carried out by Accredited Inspection Companies (ECV), through the approval of Computerized Systems by the State Traffic Departments (DETRAN), from the company's facilities in São José dos Campos, according to the service catalog."

10.1.3 NORMA ABNT NBR ISO/IEC 27001:2022

Português:
"Sistema de Gestão de Segurança da Informação, aplicado aos processos de captura, armazenamento, tráfego de dados e imagens para a emissão de Laudo de Vistoria Veicular fixa e/ou móvel, pelo DETRAN, utilizando a solução tecnológica FenoxTec. Referente à Declaração de Aplicabilidade – Revisão 03.1."

Inglês:
"Information Security Management System, applied to the capture, storage, data and image traffic processes for the issuance of a Vehicle Inspection Report, fixed and/or mobile, by DETRAN, using the technological solution FENOX Tec. Regarding the Declaration of Applicability - Revision 03.1."

10.1.4 NORMA ABNT NBR ISO 22301:2020

Português:
"Sistema de Gestão da Continuidade do Negócio (SGCN), suporta os processos relacionados à captura, armazenamento, tráfego de dados, imagens e vídeos para a emissão de Laudo de Vistoria de Identificação Veicular fixa e/ou móvel, de acordo com as normatizações dos órgãos executivos de trânsito pertinentes."

Inglês:
"Business Continuity Management System (BCMS), supports the processes related to capture, storage,

data traffic, images and videos for the issuance of Vehicle Inspection Reports, fixed and/or mobile, in accordance with the regulations of the relevant transit executive bodies."

10.1.5 NORMA ABNT NBR ISO/IEC 27701:2019 (SGPI)

Português:
"Sistema de Gestão de Privacidade da Informação aplicado ao tratamento de dados pessoais e dados pessoais sensíveis, incluindo biometria facial, imagens, vídeos, documentos e registros capturados, armazenados e processados pela solução tecnológica FenoxTec para a emissão de Laudos de Vistoria Veicular fixa e/ou móvel, abrangendo coleta, uso, compartilhamento, retenção, anonimização, descarte e proteção das informações tratadas pela Fenox, na condição de Controladora e Operadora, conforme a LGPD e os requisitos da ISO/IEC 27701:2019."

Inglês:
"Privacy Information Management System applied to the processing of personal and sensitive personal data, including facial biometrics, images, videos, documents, and records captured, stored, and processed by the FenoxTec technological solution for issuing fixed and/or mobile Vehicle Inspection Reports, covering collection, use, sharing, retention, anonymization, disposal, and protection of information processed by Fenox as both Controller and Processor, in accordance with LGPD and the requirements of ISO/IEC 27701:2019."

10.1.6 DIRETRIZES DE SEGURANÇA PARA SERVIÇOS EM NUVEM – ABNT NBR ISO/IEC 27017:2016

Português:
Sistema de gestão de Segurança da Informação para prestação e utilização de serviços em nuvem, aplicáveis a atividade de computação em nuvem utilizados no tratamento de dados, imagens, vídeos, biometria facial e demais evidências digitais associadas aos serviços de Vistoria Veicular fixa e/ou móvel executados por meio da solução tecnológica FenoxTec.

Inglês:
Information Security Management System for the provision and use of cloud services, applicable to cloud computing activities used in the processing of data, images, videos, facial biometrics and other digital evidence associated with fixed and/or mobile Vehicle Inspection services executed through the FenoxTec technological solution.

10.1.7 DIRETRIZES DE PROTEÇÃO DE DADOS PESSOAIS EM NUVEM – ABNT NBR ISO/IEC 27018:2025

Português:
A Fenox Tecnologia adota controles de proteção de informações pessoais identificáveis alinhados às diretrizes da ABNT NBR ISO/IEC 27018:2022, aplicáveis ao tratamento de dados pessoais e dados pessoais sensíveis processados em serviços de computação em nuvem utilizados pela solução tecnológica FenoxTec.

Inglês:
Fenox Tecnologia adopts controls for the protection of personally identifiable information aligned with the guidelines of ABNT NBR ISO/IEC 27018:2022, applicable to the processing of personal and sensitive personal data handled in cloud computing services used by the FenoxTec technological solution.

11 EXCLUSÃO DE ESCOPO

As exclusões de escopo são definidas com base em análise crítica documentada, considerando aplicabilidade, impacto nos serviços e conformidade normativa, sendo revisadas periodicamente pela Direção.

Esta política não se aplica a:

Dados anonimizados de forma irreversível, que não permitam a identificação de pessoas;
• Informações públicas acessíveis conforme legislação aplicável;
• Dados corporativos ou institucionais que não se relacionem a pessoas físicas.

Está excluído do escopo da organização o requisito 7.1.5.2 – Rastreabilidade de Medição, da norma ISO 9001:2015, por não ser aplicável às atividades da Fenox Tecnologia, uma vez que a organização não executa medições e calibrações em equipamentos utilizados por clientes e não possui internamente equipamentos destinados a essa finalidade.

ABNT NBR ISO/IEC 27701:2025

- A.7.3.10 – Tomada de decisão automatizada (não aplicável, pois a Fenox não realiza decisões com efeitos jurídicos ou impacto significativo aos titulares baseadas exclusivamente em tratamento automatizado).

ABNT NBR ISO/IEC 27018:2025

- A.8.1 – Divulgação de tratamento de DP subcontratado.
- A.11.12 – Tratamento de DP subcontratado.

Adicionalmente, a Fenox Tecnologia não realiza subcontratação de atividades que envolvam tratamento de dados pessoais em seu nome, tampouco terceiriza suas atividades-fim de desenvolvimento de software, suporte especializado ou gestão operacional dos processos abrangidos pelo escopo certificado.

Entretanto, a organização mantém formalmente implementado e disponível o controle **A.8.30 – Desenvolvimento Terceirizado**, previsto na Declaração de Aplicabilidade (SoA) da ABNT NBR ISO/IEC 27001:2022, garantindo que eventuais necessidades futuras de contratação de terceiros para atividades de desenvolvimento sejam conduzidas de forma controlada, segura e em conformidade com os requisitos do Sistema de Gestão Integrado.

Dessa forma, os controles relacionados à utilização de subcontratados para tratamento de dados pessoais, previstos na **ABNT NBR ISO/IEC 27018**, são considerados não aplicáveis ao contexto operacional atual da organização:

- **A.8.1 – Divulgação de tratamento de dados pessoais subcontratado;**
- **A.11.12 – Tratamento de dados pessoais subcontratado.**

Da mesma forma, o controle **A.7.3.10 – Tomada de decisão automatizada**, da **ABNT NBR ISO/IEC 27701**, é considerado não aplicável, uma vez que a Fenox não realiza decisões que produzam efeitos jurídicos ou impactos significativos aos titulares baseadas exclusivamente em tratamento automatizado de dados pessoais. Os processos existentes possuem intervenção humana para análise, validação e decisão final.

A utilização de provedores de infraestrutura, serviços em nuvem, telecomunicações, hospedagem, backup, licenciamento de software e demais serviços de apoio tecnológico não caracteriza subcontratação das atividades abrangidas pelos controles mencionados. Tais fornecedores atuam como provedores de serviços ou operadores de suporte tecnológico, permanecendo sujeitos aos requisitos contratuais, controles de segurança da informação, privacidade, gestão de riscos, monitoramento contínuo e demais controles

estabelecidos pelo Sistema de Gestão Integrado (SGI) e pelo Sistema de Gestão da Privacidade da Informação (SGPI).

12 PRINCÍPIOS DA PRIVACIDADE E PROTEÇÃO DE DADOS

A Fenox Tecnologia fundamenta sua Política de Privacidade nos princípios estabelecidos pela Lei nº 13.709/2018 (LGPD) e nas normas internacionais de gestão da privacidade da informação, assegurando que o tratamento de dados pessoais ocorra de forma ética, transparente, proporcional e segura.

Esses princípios orientam todas as atividades de coleta, uso, armazenamento, compartilhamento e descarte de dados pessoais no contexto das operações tecnológicas e corporativas da Fenox.

O tratamento de dados é realizado para finalidades legítimas, específicas e previamente definidas, sendo limitado ao objetivo originalmente previsto e compatível com a base legal aplicável. A coleta e o uso restringem-se ao mínimo necessário, em alinhamento aos princípios da necessidade e minimização.

A Fenox assegura aos titulares acesso facilitado às informações relacionadas ao tratamento de seus dados, por meio de canais formais administrados pelo Encarregado de Dados (DPO), promovendo transparência, clareza e atendimento aos prazos legais aplicáveis.

A **Fenox** adota uma postura proativa e responsável no tratamento de dados pessoais, com base nos seguintes pilares:

- **Segurança e Qualidade:** Adoção de medidas técnicas e administrativas para proteger os dados e preservar sua integridade, reduzindo riscos de acessos não autorizados e incidentes.
- **Gestão de Riscos e Responsabilização (*accountability*):** Manutenção de práticas de avaliação e melhoria contínua para reduzir riscos e apoiar a conformidade.
- **Ética e Retenção:** Compromisso com o tratamento não discriminatório e descarte seguro após o atendimento da finalidade, utilizando, quando aplicável, técnicas como anonimização e pseudonimização.
- **Cultura Organizacional:** Fortalecimento da cultura de privacidade entre colaboradores e terceiros com acesso à informação sob custódia da Fenox.

De forma complementar, os dados pessoais são protegidos por controles compatíveis com a sensibilidade das informações e os riscos envolvidos, incluindo, quando aplicável, criptografia, controle de acesso por perfil (RBAC), autenticação multifator (MFA), segregação de ambientes e monitoramento de logs.

12.1 PROTEÇÃO DE INFORMAÇÕES

Toda informação tratada pela Fenox será classificada conforme seu nível de sensibilidade (ex.: Pública, Interna, Confidencial e Secreta/Restrita), de acordo com as diretrizes internas do SGI. Materiais e mídias que contenham dados pessoais ou informações estratégicas deverão ser identificados de forma compatível com sua classificação, conforme a política interna de classificação da informação.

As categorias e critérios aplicáveis constam na documentação do SGI, assegurando manuseio, acesso e proteção compatíveis com cada nível de sensibilidade.

13 BASE LEGAL E FINALIDADES DE TRATAMENTO

O tratamento de dados pessoais na Fenox é realizado com fundamento em base legal adequada e registrada, vinculada a uma finalidade específica. As operações de tratamento são mapeadas e mantidas em registros internos (ex.: RoPA), de forma a garantir rastreabilidade e consistência entre finalidade, base legal e evidências.

Principais bases legais utilizadas pela Fenox:

- **Obrigação Legal ou Regulatória:** Atendimento a normas do DETRAN, LGPD, legislação trabalhista e fiscal.
- **Execução de Contrato:** Indispensável para serviços tecnológicos, suporte e vistoria veicular.
- **Legítimo Interesse:** Operações com benefício legítimo à Fenox, mediante análise de impacto (DPIA).
- **Consentimento:** Manifestação livre e revogável do titular, registrada eletronicamente.
- **Proteção da Vida e da Saúde:** Quando aplicável, em situações que demandem proteção de pessoas
- **Exercício Regular de Direitos:** Uso de dados para defesa e condução de processos judiciais, administrativos ou arbitrais.

Finalidades Institucionais: Prestação de serviços de vistoria, gestão tecnológica, segurança de sistemas, controle de qualidade, atendimento e suporte, e cumprimento de exigências de órgãos reguladores. Cada finalidade é vinculada à respectiva base legal e registrada nos controles internos pertinentes (ex.:RoPA).

14 RETENÇÃO E PRESERVAÇÃO DE DADOS

A retenção de dados na Fenox, especialmente aqueles vinculados a laudos e contratos de vistoria, é pautada pela natureza regulatória da atividade e pela necessidade de manter rastreabilidade e segurança jurídica.

• **Critério de retenção:** *devido à responsabilidade solidária e às exigências de fiscalização do DETRAN, os dados de vistorias e laudos são preservados para garantir a segurança jurídica e a rastreabilidade histórica das operações.*
• **Fundamentação:** a manutenção desses registros baseia-se no cumprimento de obrigação regulatória e no exercício regular de direitos, prevenindo sanções administrativas ou contestações judiciais futuras.
• **Segurança no armazenamento:** *durante todo o período de guarda, os dados permanecem em ambiente controlado (Podio/Servidores), com acesso restrito e monitorado, garantindo que a preservação seja acompanhada por medidas adequadas de proteção.*
• **Registro de exceção/descarte:** quando ocorrer a eliminação de dados não regulatórios (ex.: currículos ou cadastros comerciais antigos), o descarte será formalizado por meio de **Registro de Descarte no SGPI (Podio)**, contendo data, responsável, método aplicado e validação pelo DPO, quando aplicável, servindo como evidência de conformidade.
• **Encerramento da finalidade:** ao término da finalidade ou da obrigação aplicável, os dados pessoais serão excluídos ou anonimizados, salvo hipóteses legais de retenção.
• **Arquivos temporários:** arquivos temporários de processamento (ex.: cache, staging e logs transitórios) serão eliminados conforme prazos técnicos definidos internamente.

A retenção de dados na Fenox, especialmente os dados vinculados a laudos e contratos de vistoria, é pautada pela natureza regulatória da atividade e pela necessidade de manter rastreabilidade e segurança jurídica.

14.1 FORNECIMENTO DE CÓPIA ESTRUTURADA DOS DADOS PESSOAIS

Mediante liberação da Diretoria e solicitação legítima do titular, a Fenox fornecerá cópia dos dados pessoais tratados em formato eletrônico estruturado e interoperável (ex.: CSV, JSON ou outro formato compatível), observados os cuidados de segurança e a proteção de informações de terceiros e de segredos comerciais. O atendimento será documentado no SGPI (Registro de Solicitações), com prazo máximo de resposta de 15 (quinze) dias úteis, prorrogável por igual período mediante justificativa técnica registrada no sistema.

14.2 MÍDIA DE ARMAZENAMENTO

Dispositivos de armazenamento removíveis que contenham dados pessoais (ex.: HD externo, mídia de *backup, pendrive*) devem ser identificados e protegidos conforme a política interna de classificação e segurança da informação. Ao término do uso, essas mídias serão destinadas a descarte seguro**,** por

destruição física ou sanitização apropriada, de forma a impedir a recuperação dos dados. O descarte de mídias seguirá procedimentos formais (Registro de Descarte), igualmente auditados pelo DPO.

14.2.1 GESTÃO DE MÍDIAS E DESCARTE FÍSICO

Todo suporte físico ou mídia removível que contenha dados pessoais terá ciclo de vida gerenciado (aquisição → uso → transporte → armazenamento → eliminação). A eliminação seguirá procedimento de sanitização aplicável e contará com evidência registrada, assinada pelo responsável técnico, incluindo nº do ativo, método utilizado (ex.: trituração ou descarte certificado) e data.

14.3 DESCARTE DE EQUIPAMENTO

Equipamentos de TI e dispositivos móveis (computadores, notebooks, tablets, smartphones, servidores) que tenham armazenado ou processado dados pessoais somente poderão ser descartados, doados, vendidos ou reutilizados após apagamento seguro dos dados, por método apropriado (ex.: sanitização/limpeza segura de mídia ou destruição física, quando aplicável).

14.4 TRANSFERÊNCIAS INTERNACIONAIS

A Fenox identifica, documenta e mantém registro das bases legais e salvaguardas aplicáveis às transferências internacionais de dados pessoais, quando ocorrerem.

As transferências internacionais são registradas nos controles internos pertinentes (ex.: RoPA), incluindo, quando aplicável, categoria de dados, destinatário e base legal. Sempre que atuar como Operadora, a Fenox informará o cliente sobre alterações relevantes relacionadas a transferências internacionais, conforme previsão contratual.

Quando necessário, a Fenox adota salvaguardas adequadas (ex.: cláusulas contratuais e medidas equivalentes) e realiza avaliação compatível com o risco, registrando as evidências aplicáveis.

15 LOCALIZAÇÃO DOS DADOS, JURISDIÇÃO E CONTINGÊNCIA / SOBERANIA, LOCALIZAÇÃO E RESIDÊNCIA DOS DADOS

A Fenox adota como diretriz prioritária o armazenamento de dados pessoais e demais informações sob sua custódia em infraestrutura localizada no território brasileiro, observando os requisitos da LGPD, da ABNT NBR ISO/IEC 27701, da ABNT NBR ISO/IEC 27018 e demais normas aplicáveis.

Os dados pessoais processados pela organização permanecem armazenados em ambiente principal localizado no Brasil (Zona 1), sendo mantida redundância operacional em ambiente secundário localizado também no Brasil (Zona 2), com o objetivo de assegurar disponibilidade, continuidade dos serviços, recuperação de informações e resiliência operacional.

Como medida de contingência para eventos de indisponibilidade severa, desastre ou comprometimento simultâneo dos ambientes nacionais, a Fenox mantém capacidade de recuperação em ambiente alternativo localizado na região Leste dos Estados Unidos (US East), utilizado exclusivamente para continuidade dos serviços, recuperação de dados e restabelecimento das operações críticas.

A ativação do ambiente de contingência internacional ocorre somente mediante necessidade operacional devidamente justificada, observando controles de segurança da informação, rastreabilidade, gestão de acessos, proteção de dados pessoais e requisitos legais aplicáveis.

Os mecanismos de replicação, redundância, backup e recuperação devem assegurar a integridade, confidencialidade, disponibilidade e rastreabilidade das informações durante todo o ciclo de vida dos dados.

A utilização de infraestrutura localizada fora do território nacional, quando necessária para fins de contingência e continuidade dos negócios, deve observar as salvaguardas técnicas, contratuais e

organizacionais estabelecidas pela legislação vigente e pelos controles definidos no Sistema de Gestão Integrado da Fenox.

16 TRATAMENTO DE DADOS PESSOAIS E SENSÍVEIS

A Fenox realiza o tratamento de dados de forma ética e segura, respeitando os princípios da **finalidade**, **necessidade (minimização)** e **confidencialidade**.

- **Dados pessoais (exemplos):** dados de identificação e contato, dados profissionais, registros de atendimento e suporte, e registros técnicos de uso dos sistemas (logs).
- **Dados pessoais sensíveis (quando aplicável):** a Fenox não realiza tratamento rotineiro de dados sensíveis como regra geral, exceto quando houver necessidade operacional ou regulatória.
- **Biometria facial (obrigatória por exigência regulatória):** quando aplicável, a Fenox realiza o tratamento de **biometria facial**, considerada **dado pessoal sensível**, para atender exigências de órgãos reguladores (ex.: DETRAN) relacionadas à identificação/autenticação e à segurança do processo. Esse tratamento é limitado à finalidade exigida e protegido com controles reforçados e acesso restrito.
- **Segurança:** os dados são armazenados em infraestrutura controlada, com registros de acesso e medidas de monitoramento compatíveis. Revisões e verificações podem ser realizadas pelas áreas responsáveis (ex.: DPO e Qualidade), conforme a governança interna.

17 DIREITO DOS TITULARES

A Fenox busca assegurar transparência e atendimento aos direitos previstos na LGPD, permitindo que o titular, quando aplicável:

- Confirme a existência de tratamento e acesse seus dados;
- Solicite correção de informações incompletas, inexatas ou desatualizadas;
- Solicite anonimização, bloqueio ou eliminação, quando cabível;
- Requeira portabilidade dos dados, quando aplicável;
- Revogue o consentimento e/ou se oponha ao tratamento;
- Solicite revisão de decisões automatizadas.

Gestão de Requisições: As solicitações são processadas via Sistema Podio, com rastreabilidade total e supervisão do DPO no SGPI. Colaboradores, prestadores e terceiros que tenham acesso a dados pessoais devem possuir termo de confidencialidade (NDA) formalizado e registrado.

As solicitações dos titulares serão analisadas e respondidas dentro dos prazos estabelecidos pela Lei Geral de Proteção de Dados (LGPD), sendo mantidos registros formais das requisições, das análises realizadas e das respostas fornecidas, garantindo rastreabilidade e evidência para fins de auditoria.

17.1 DECISÕES AUTOMATIZADAS

A Fenox registrará decisões automatizadas, quando aplicável, e assegurará ao titular o direito de solicitar revisão com intervenção humana, manifestar-se e contestar, conforme LGPD.

17.2 NOTIFICAÇÃO A TERCEIROS

Sempre que houver correção, exclusão ou oposição relacionada a dados compartilhados com terceiros, a Fenox notificará tais terceiros para que adotem medidas equivalentes.

18 GERENCIAMENTO DE INCIDENTES DE SEGURANÇA

A Fenox mantém um Plano de Gerenciamento de Incidentes de Segurança da Informação, coordenado pelo Comitê de Segurança e Privacidade e supervisionado pelo DPO. O plano contempla a identificação**,** classificação e resposta a incidentes, considerando impactos à confidencialidade, integridade e disponibilidade das informações.

Em caso de suspeita ou confirmação de incidente envolvendo dados pessoais, a ocorrência será comunicada internamente às áreas responsáveis e à Alta Direção para avaliação e contenção. Quando aplicável, a Fenox realizará a notificação à ANPD e/ou a outros órgãos competentes, bem como aos titulares afetados**,** nos termos da legislação e regulamentação aplicáveis e conforme a avaliação do impacto e risco do incidente.

Todos os incidentes serão registrados, incluindo a cronologia do evento, ações de contenção e correção, e lições aprendidas, como evidência para fins de governança e melhoria contínua.

18.1 REGISTRO DE DIVULGAÇÃO A TERCEIROS

Toda divulgação ou compartilhamento de dados pessoais a terceiros (nacional ou internacional), quando aplicável, deverá ser registrada no RoPA com, no mínimo, as seguintes informações:

I. **ID da operação**;
II. **Finalidade**;
III. **Categorias de dados divulgadas**;
IV. **Destinatário** (nome e CNPJ/identificação, quando aplicável);
V. **Base legal**;
VI. **Data/hora do envio**;
VII. **Evidência documental** do envio (ex.: contrato, ordem judicial, comprovante técnico);
VIII. **Responsável pelo envio**.

Esse registro servirá como evidência de rastreabilidade e conformidade para fins de auditoria e governança.

18.2 REGISTRO DE CONSENTIMENTO DO TITULAR

18.2.1 NATUREZA DA COLETA:

A Fenox, como fornecedora de tecnologia para Empresas Credenciadas de Vistoria (ECVs), trata dados pessoais cuja coleta é, em grande parte, decorrente de obrigações legais e regulatórias, conforme normas e portarias aplicáveis dos órgãos competentes (ex.: DETRAN).

18.2.2 OBTENÇÃO DO CONSENTIMENTO

Quando o tratamento não se enquadrar em obrigação legal/regulatória, execução de contrato ou outra base legal aplicável e exigir consentimento, a Fenox assegura que a manifestação do titular será obtida de forma clara, específica e destacada, com possibilidade de revogação, quando cabível.

18.2.3 RASTREABILIDADE

Para fins de conformidade e demonstração (*accountability*), os consentimentos coletados por meio das plataformas da Fenox, quando aplicável, devem ser registrados com, no mínimo:

- **Identificação:** identificação do titular (ID único, quando aplicável) e do responsável/sistema que realizou a coleta;
- **Contexto e finalidade:** finalidade específica autorizada e seu vínculo com o serviço/funcionalidade;
- **Evidência temporal:** data e hora (*timestamp*) da manifestação;

- **Evidência do meio:** canal de coleta (ex.: assinatura em tablet, termo eletrônico no check-in, portal/sistema web);
- **Integridade:** versão do termo/política aceita no momento da coleta.

18.2.4 INTEGRAÇÃO COM O ROPA

Os registros de consentimento, quando existentes, são vinculados aos controles internos pertinentes (ex.: RoPA), apoiando o atendimento a solicitações de titulares, auditorias e exigências regulatórias, assegurando rastreabilidade do fundamento do tratamento.

19 GOVERNANÇA E RESPONSABILIDADE

Estrutura de responsabilidades distribuídas:

19.1.1 PAPÉIS

- **Direção**: Aprovação estratégica e provisão de recursos.
- **Comitê de Segurança e Privacidade**: Análise de riscos e supervisão de incidentes.
- **DPO (Encarregado)**: Supervisão do SGPI, interface com a ANPD e manutenção do RoPA/DPIA.
- **Jurídico & TI/SI**: Conformidade contratual e aplicação de controles técnicos.
- **Qualidade**: Controle de versões, auditorias e evidências (ISO 9001/27001).
- **Colaboradores:** Cumprimento da política e reporte de desvios.

19.1.2 CANAIS

Pontos de contato oficiais para requisições de titulares, suporte à privacidade e comunicação imediata de incidentes.

19.1.3 RESPONSABILIZAÇÃO

Dever de prestação de contas (*accountability*) e aplicação de medidas corretivas em caso de descumprimento das diretrizes de segurança.
Os dados pessoais são protegidos por controles técnicos e administrativos específicos, incluindo criptografia, controle de acesso baseado em função (RBAC), autenticação multifator, segregação de ambientes e monitoramento contínuo de logs.

19.1.4 CAPACITAÇÃO E SENSIBILIZAÇÃO

A Fenox implementará programa de treinamento obrigatório para todos os colaboradores com ciclo mínimo anual, com conteúdo sobre LGPD, controles de privacidade, resposta a incidentes e segurança da informação; os registros de participação e avaliação serão mantidos no SGPI como evidência.

19.2 REVISÃO INDEPENDENTE

Além das auditorias internas, a Fenox poderá realizar auditorias externas independentes e periódicas do SGPI, conduzidas por auditorias certificadoras ou terceiros qualificados, para verificar a conformidade com requisitos legais, contratuais e normativos (incluindo a ISO/IEC 27701). Os resultados serão apresentados e analisados pela Alta Direção, com definição e acompanhamento de ações corretivas e melhorias, quando aplicável.

20 REGISTRO DAS OPERAÇÕES DE TRATAMENTO (ROPA)

O RoPA é o repositório formal da Fenox que consolida finalidades, categorias de dados, bases legais e prazos de retenção.

1. Revisado periodicamente pela Qualidade e DPO;
2. Possui controle e rastreabilidade total;
3. Atua como evidência para auditorias de certificação
4. O **RoPA** da Fenox constitui o Inventário Oficial de Dados Pessoais da organização, atendendo ao controle A.8.1.1 da ISO/IEC 27701

20.1 EXEMPLO DE APLICAÇÃO PRÁTICA (ROPA)

Para fins de transparência e padronização, a Fenox mantém o inventário de dados no SGPI (Podio). Abaixo, apresenta-se um exemplo de como uma operação de tratamento é documentada:

ID RoPA	SGPI-0016
Título / Controle	Gestão Comercial e Relacionamento com Clientes
Finalidade	Viabilizar a execução de contratos, prestação de serviços, faturamento e atendimento ao cliente.
Papel Fenox	**Controladora** (Define finalidades e meios de tratamento).
Titulares	Clientes, vistoriadores credenciados e responsáveis legais.
Categorias de Dados	Identificação (CPF/Nome), Contato, Financeiros, Imagem/Áudio (Vistorias) e operacionais (Logs).
Base Legal Principal	**Execução de Contrato** (Art. 7º, V da LGPD) e **Obrigação Legal**.
Retenção	5 anos (padrão contratual/fiscal) ou conforme regulação específica.
Método de Descarte	Exclusão lógica controlada e descarte seguro com registro no sistema.
Medidas de Segurança	Criptografia, Controle de Acesso (RBAC), MFA e Logs de Auditoria.

21 INTEGRAÇÃO OPERACIONAL ENTRE ROPA, DPIA E PLANO DE INCIDENTES

A Fenox estabelece uma integração funcional e sistêmica entre os três pilares da privacidade corporativa, assegurando rastreabilidade, coerência e governança do tratamento de dados pessoais.

21.1.1 DOCUMENTOS E PAPÉIS NA INTEGRAÇÃO

Documento	Finalidade	Integração e Encadeamento
RoPA (Registro das Operações de Tratamento)	Mapeia todos os processos de tratamento, bases legais, categorias de dados e controles aplicados.	Serve como base obrigatória para identificação de riscos e abertura de novos DPIAs.
DPIA (Relatório de Impacto à Proteção de Dados)	Avalia riscos e define medidas mitigatórias para operações identificadas no RoPA.	Alimenta o Plano de Incidentes com riscos classificados como médios ou altos.
Plano de Incidentes LGPD	Define etapas de resposta, prazos, responsáveis e critérios de comunicação à ANPD e aos titulares.	É verificado pelo DPO, que monitora riscos do DPIA e gera ações corretivas e preventivas.

21.2 GESTÃO AUDITÁVEL DE INCIDENTES

Para atender aos requisitos de fiscalização e auditoria, todo incidente de privacidade é registrado no app SGPI (Podio), contendo os seguintes elementos:

- **Classificação (C.I.D.)**: Identificação se o incidente afetou a Confidencialidade (vazamento), Integridade (alteração indevida) ou Disponibilidade (perda de acessos) dos dados.
- **Classificação interna** (Baixo, Médio ou Alto) baseada no risco aos titulares.
- **Fluxo de Decisão:** Registro formal da decisão de notificar ou não a ANPD e os titulares, com a devida justificativa técnica do DPO.
- **Ações Corretivas (PDCA):** Registro das lições aprendidas e das melhorias aplicadas nos processos para evitar a reincidência, garantindo a melhoria contínua do sistema.

21.3 FUNDAMENTOS DA INTEGRAÇÃO NO SGPI FENOX

Essa integração é sustentada pela implementação sistêmica no SGPI Fenox, garantindo:

- Encadeamento lógico entre identificação de riscos, ações corretivas e evidências de mitigação;
- Rastreabilidade total entre processo (RoPA), avaliação (DPIA) e controle aplicado (Plano de Incidentes);
- Geração automática de evidências utilizadas em auditorias internas e externas.

Essa arquitetura assegura que o tratamento de dados pessoais seja **rastreável, mensurável e verificável**, em conformidade com os controles **A.7.4.1 a A.7.4.5 da ISO/IEC 27701**.

22 EVIDÊNCIAS E AUDITORIA DE PRIVACIDADE

22.1.1 EVIDÊNCIAS DE CONFORMIDADE

As evidências são mantidas em **repositórios eletrônicos do SGPI Fenox (Podio)**, com acesso controlado, incluindo:

- Relatórios e aprovações de DPIA;
- Registros de RoPA atualizados;
- Planos de mitigação executados;
- Registros de incidentes e comunicações formais.

Esses registros constituem **prova objetiva de conformidade** perante órgãos reguladores, clientes e auditores de certificação.

22.1.2 AUDITORIA E MELHORIA CONTÍNUA

- A auditoria do SGPI segue o mesmo ciclo do SGI, contemplando:
- Revisões internas anuais de conformidade com a LGPD e ISO/IEC 27701;
- Auditorias externas conforme o plano de certificações Fenox;
- Relatórios de constatações e planos de ação corretiva acompanhados pela Qualidade e pelo DPO;
- Integração dos resultados às **Análises Críticas pela Direção**, sustentando o processo de melhoria contínua.

22.1.3 EVIDÊNCIAS MÍNIMAS

- As provas objetivas de conformidade são mantidas em repositórios eletrônicos do SGPI Fenox (Podio), com acesso controlado, incluindo:
- Relatórios e aprovações de DPIA;
- Registros de RoPA atualizados;
- Planos de mitigação executados;
- Registros de incidentes e comunicações formais.

22.1.4 ANÁLISE CRÍTICA

- Integração dos resultados às reuniões de Análise Crítica pela Direção, garantindo o suporte estratégico e os recursos necessários para a melhoria contínua.

22.1.5 INDICADORES

- Monitoramento de métricas de desempenho do SGPI (ex: tempo de resposta a incidentes, nível de atualização do RoPA) para mensurar a eficácia dos controles.

22.2 POLÍTICAS AMBIENTAIS DE SEGURANÇA

22.2.1 MESA LIMPA E TELA LIMPA

Deve ser observada a política de mesa limpa e tela limpa**.** Documentos que contenham dados pessoais devem permanecer no local de trabalho apenas durante o uso, devendo ser guardados de forma segura ao final do expediente. As estações de trabalho devem permanecer bloqueadas quando estiverem sem supervisão, com bloqueio automático por inatividade ou logout. Dispositivos móveis e notebooks utilizados para atividades corporativas devem possuir mecanismo de bloqueio (senha e/ou biometria) e utilizar recursos de segurança aprovados pela área de TI.

22.3 POLÍTICA DE BACKUP E RECUPERAÇÃO

A Fenox manterá rotina regular de backup dos bancos de dados e sistemas que contenham dados pessoais, com armazenamento em ambiente seguro e, quando aplicável, com criptografia. Testes periódicos de restauração serão realizados para verificar a eficácia dos backups e a capacidade de recuperação. A retenção de backups seguirá os prazos legais, regulatórios e contratuais aplicáveis. Na ausência de exigência específica, poderá ser adotado prazo mínimo de retenção conforme diretrizes internas, observado o princípio da necessidade e eventuais orientações regulatórias.

23 DECISÕES AUTOMATIZADAS E IA

A Fenox identifica e registra, quando aplicável, operações que envolvam tratamento automatizado de dados pessoais, incluindo rotinas de validação biométrica**,** análises automatizadas de evidências digitais e apoio ao processamento de informações associadas a laudos e vistorias.

Quando houver decisão baseada exclusivamente em tratamento automatizado e isso for aplicável ao caso, o titular poderá solicitar revisão por pessoa natural, bem como receber informações claras, em nível adequado, sobre os critérios utilizados, observadas limitações técnicas, proteção de terceiros e segredos comerciais.

A Fenox adota transparência e controles proporcionais ao risco, com mecanismos de supervisão humana**,** rastreabilidade e medidas de segurança, aplicando tais recursos exclusivamente em conformidade com as exigências dos órgãos de trânsito competentes e com a legislação de proteção de dados pessoais.

24 DESENVOLVIMENTO SEGURO

Os sistemas internos e soluções de TI da Fenox são desenvolvidos com diretrizes de segurança ao longo do ciclo de vida de desenvolvimento (SSDLC), considerando requisitos de segurança desde a especificação até a implantação. Entre as práticas adotadas, quando aplicável, incluem-se: definição de requisitos de segurança, revisões e validações de código, testes de segurança antes da entrada em produção e segregação adequada entre ambientes de desenvolvimento/teste e produção. Os requisitos de segurança de aplicações (ex.: autenticação adequada, controle de acesso e criptografia, quando aplicável) são documentados e podem ser verificados em auditorias internas e externas.

Observação (terceiros): quando houver participação de terceiros em atividades relacionadas ao desenvolvimento ou manutenção, estes deverão seguir as diretrizes de segurança e privacidade estabelecidas pela Fenox, conforme contrato e governança interna.

24.1 REFERÊNCIA À POLÍTICA DE DESENVOLVIMENTO SEGURO

As práticas, requisitos e evidências de desenvolvimento seguro estão detalhadas no documento “SG-PL-07_01 — Política de Desenvolvimento Seguro”**,** que integra e complementa esta Política, sendo de observância obrigatória pelas equipes envolvidas no desenvolvimento e manutenção de sistemas. O descumprimento das diretrizes poderá resultar em bloqueio de release e adoção de medidas corretivas, conforme governança interna. O SG-PL-07_01 contempla, entre outros pontos, requisitos de segurança por fase do SDLC, gestão de ambientes, regras para uso e tratamento de dados em testes, revisões de código, testes de segurança (SAST/DAST) e diretrizes contratuais aplicáveis quando houver participação de terceiros.

25 DIREÇÃO

A Direção da Fenox Tecnologia reafirma, por meio desta política, seu compromisso com a ética, a transparência e a proteção dos dados pessoais sob sua responsabilidade.

Todos os níveis hierárquicos têm o dever de cumprir as diretrizes aqui estabelecidas e de zelar pela integridade, confidencialidade e disponibilidade das informações tratadas.

“A privacidade é parte essencial da confiança que a Fenox constrói com clientes, colaboradores e parceiros.
Este compromisso é contínuo, mensurável e integrado à nossa forma de trabalhar.”

Direção Geral – Fenox Tecnologia Ltda.

25.1 INSTRUÇÃO ILEGAL

Caso a Fenox identifique que instrução de tratamento fornecida pelo cliente infringe requisitos legais aplicáveis, notificará formalmente o cliente antes de executar o tratamento

25.2 INSTRUÇÃO ILEGAL/ ASSISTÊNCIA AO CONTROLADOR

Ao receber instrução que aparente infringir norma legal aplicável, a Fenox:
I. Suspenderá a execução da instrução até definição formal;
II. Notificará o Controlador por escrito em até 24 (vinte e quatro) horas;
III. Registrará no SGPI as evidências e a justificativa técnica;
IV. Quando necessário, submeterá o tema ao Jurídico e ao Comitê de Segurança e Privacidade para deliberação.

26 ANEXO A

26.1 ATO DE DESIGNAÇÃO DO ENCARREGADO DE DADOS (DPO) E CONSTITUIÇÃO DO COMITÊ DE SEGURANÇA E PRIVACIDADE

Em atendimento à Lei nº 13.709/2018 (LGPD) e à ABNT NBR ISO/IEC 27701:2019, a Fenox Tecnologia Ltda. formaliza a designação do Encarregado pelo Tratamento de Dados Pessoais (DPO) e a instituição do Comitê de Segurança e Privacidade, conforme o Ato de Designação nº (segue número da política), documento controlado no SGI-Fenox.

Este ato estabelece papéis, responsabilidades e instâncias de deliberação que asseguram a governança e a conformidade da empresa com os requisitos legais e normativos aplicáveis à proteção de dados pessoais e segurança da informação.

26.2 ENCARREGADO DE DADOS (DPO)

A Fenox adota o modelo de DPO compartilhado, distribuindo as funções entre a Gerência e a Qualidade, de forma a garantir independência, competência técnica e rastreabilidade operacional.

Função	Nome	Atribuições	Observação
DPO Institucional (Gerente da Empresa)	Andrea Moreira Monteiro	Representar oficialmente a Fenox perante a ANPD, clientes e parceiros; aprovar políticas e decisões estratégicas; responder comunicações externas e relatórios formais de conformidade.	Responsável final perante autoridades.
DPO Técnico / Operacional (Analista de Qualidade)	Leonardo Raimundo Machado Alves	Supervisionar o SGPI, manter RoPA, DPIA e registros de auditoria; coordenar o Comitê de Segurança e Privacidade; ministrar treinamentos e acompanhar auditorias internas.	Responsável pela operação e conformidade documental.

Contato do DPO Institucional:
andrea.monteiro@fenoxtec.com.br
(11) 98198-7976

26.3 COMITÊ DE SEGURANÇA E PRIVACIDADE

A Direção da Fenox institui formalmente o Comitê de Segurança e Privacidade, órgão de apoio consultivo e deliberativo responsável pela gestão integrada de privacidade, segurança da informação e conformidade normativa.

26.4 COMPOSIÇÃO DO COMITÊ

Área	Representante	Atribuição
Direção	Andrea Monteiro	Representação institucional e deliberação executiva.
DPO / Privacidade	Andrea / Leonardo	Coordenação técnica e acompanhamento da conformidade.
Jurídico	Milena Cardoso	Assessoria legal e adequação normativa.
Tecnologia da Informação	Janaina Sousa	Segurança de sistemas e infraestrutura tecnológica.
Qualidade / SGI	Leonardo Machado	Apoio em auditorias e registros de evidências.
Recursos Humanos	Graziele Martins	Privacidade de colaboradores e gestão de consentimentos.
Infraestrutura	Gabriel Souza	Apoio operacional e continuidade de serviços.
Desenvolvimento	Victor Corrêia	Segurança no ciclo de vida do desenvolvimento (SSDLC) e práticas de *Privacy by Design*.

26.5 COMPETÊNCIAS DO COMITÊ

Supervisionar a aplicação das políticas e procedimentos de privacidade e segurança da informação;
- Propor melhorias e revisar periodicamente documentos e controles do SGPI;
- Avaliar e deliberar sobre incidentes de segurança e violações de dados pessoais;
- Apoiar a Direção na tomada de decisões estratégicas sobre conformidade e riscos;
- Promover a cultura de proteção de dados em todos os níveis organizacionais;
- Monitorar o desempenho dos controles e indicadores de privacidade.

26.6 VIGÊNCIA E REVISÃO

Este ato entra em vigor na data de sua assinatura e permanecerá válido até nova deliberação da Direção. A composição e as atribuições poderão ser revistas conforme mudanças organizacionais, legais ou normativas.

27 PERIODICIDADE DE REVISÃO

A Política de Privacidade e Proteção de Dados Pessoais, o RoPA e o DPIA são revisados periodicamente, ou sempre que houver alteração relevante em processos, tecnologias, requisitos legais/regulatórios ou nas atividades de tratamento de dados pessoais. As revisões são registradas formalmente, com controle de versão**,** data e validação pelas instâncias responsáveis pela governança de privacidade.