



MA-004 - Manual de Proteção de Dados (LGPD)



Controle de Versões do Documento

Versão	Data	Elaborador	Revisor	Observações
1.0	02/03/2026	Comitê Multidisciplinar	Diretoria	Criação inicial do documento.

Informações sobre a Utilização e Controle do Documento

Este documento, quando impresso, é considerado uma cópia não controlada. Para garantir o uso das versões corretas e atualizadas, todos os documentos oficiais devem ser consultados exclusivamente no canal oficial da 1 IT, disponível no Enterprise Content Manager — ECM, Sistema de Gestão de Conteúdo. Recomenda-se que os usuários estejam atentos às versões em uso e verifiquem regularmente o sistema para assegurar a conformidade e a validade das informações.

Lista de documentos relacionados

- MA-001 - Manual de Funções da 1 IT.
- MA-002 - Manual de Segurança da Informação / PSI.
- MA-003 - Manual de Anticorrupção e Compliance.
- MA-004 - Manual de Proteção de Dados (LGPD).
- POs e ITs específicos de atendimento a titulares, resposta a incidentes, gestão de acessos, desenvolvimento seguro, backup, retenção e descarte, quando formalizados.

- Contratos, DPAs, termos de confidencialidade, avisos de privacidade e registros de treinamento.

Critério de completude: A estrutura deste Manual segue os capítulos 4 a 10 da norma, os objetivos e controles do Anexo A, as orientações de implementação do Anexo B, os mapeamentos informativos dos anexos C, D, E e F e o mapeamento nacional com a LGPD do Anexo NA, adaptados ao contexto operacional da 1 IT.

1. Finalidade, Escopo e Premissas

Este Manual estabelece as diretrizes, responsabilidades, controles, procedimentos e evidências mínimas para a proteção de dados pessoais tratados pela 1 IT, empresa em estruturação para atuação como registradora de contratos de veículos. O documento abrange atividades de recepção, validação, registro, transmissão, guarda, consulta, suporte, atendimento, relacionamento, segurança, auditoria e prestação de contas envolvendo dados pessoais.

O Manual foi estruturado para funcionar como instrumento central do Sistema de Gestão da Privacidade da Informação (SGPI), articulando governança, riscos, segurança da informação, privacidade por design, direitos dos titulares, contratos com operadores e suboperadores, gestão de incidentes, retenção, descarte e auditoria interna.

1.1 Objetivos específicos

- Formalizar a política institucional de privacidade e proteção de dados da 1 IT.
- Definir o escopo, os papéis e as responsabilidades do SGPI.
- Padronizar o inventário de dados pessoais, as bases legais, a finalidade, a retenção e o descarte.
- Estabelecer procedimentos para direitos dos titulares, incidentes de segurança, comunicações regulatórias e relacionamento com a ANPD.
- Integrar privacidade aos processos de tecnologia, segurança, desenvolvimento, suporte, fornecedores, contratos, operações e governança.
- Estabelecer evidências objetivas para auditorias internas, due diligence de clientes, processos de credenciamento e certificações.

1.2 Escopo organizacional e tecnológico

Dimensão	Abrangência
Organizacional	Alta Direção, governança, operações de registro, tecnologia, segurança da informação, jurídico/compliance, comercial,

	atendimento, ouvidoria, RH/DP, financeiro e gestão de fornecedores.
Processos finalísticos	Processos relacionados à recepção, validação, registro, consulta, manutenção, suporte e evidência de contratos de veículos e suas integrações.
Tecnologia	Aplicações web, APIs, bancos de dados, filas, logs, armazenamento, backups, cloud/datacenter, redes, WAF/firewall, IAM, SIEM/monitoramento, ambientes de desenvolvimento, homologação e produção.
Terceiros	Fornecedores de infraestrutura, nuvem, hospedagem, desenvolvimento, suporte, segurança, assinatura eletrônica, atendimento, comunicação, auditoria, consultoria e demais operadores/suboperadores.
Titulares	Pessoas naturais vinculadas a contratos, representantes de clientes e parceiros, usuários, colaboradores, candidatos, visitantes, fornecedores, manifestantes e solicitantes de direitos LGPD.

1.3 Premissas de aplicação

- A 1 IT pode atuar como controladora, operadora ou controladora conjunta conforme o processo, o contrato, a autonomia decisória e a determinação das finalidades e meios de tratamento.
- A definição de papel de agente de tratamento deve ser realizada por fluxo de dados e por relação contratual, evitando classificação genérica de toda a organização.
- Dados de contratos, veículos, garantias, representantes, usuários, logs, documentos e comunicações podem ser dados pessoais quando vinculados ou vinculáveis a pessoa natural identificada ou identificável.
- O tratamento deve ser demonstrável por evidências: ROPA, bases legais, logs, contratos, treinamentos, auditorias, AIPD/RIPD, indicadores, atas e registros de incidentes.
- Privacidade e segurança devem ser incorporadas por design e por default nos sistemas, integrações, APIs, cadastros, consultas, relatórios e exports.

2. Referências Legais, Regulatórias e Normativas

Referência	Aplicação no Manual

Lei nº 13.709/2018 - Lei Geral de Proteção de Dados Pessoais (LGPD)	Base legal central para princípios, hipóteses de tratamento, direitos dos titulares, agentes de tratamento, segurança, incidentes, governança e sanções.
Lei nº 13.853/2019	Altera a LGPD e estrutura a Autoridade Nacional de Proteção de Dados.
Regulamentações da ANPD vigentes	Complementam temas como atuação do encarregado, comunicação de incidentes, dosimetria, fiscalização e agentes de tratamento de pequeno porte.
ABNT NBR ISO/IEC 27701:2026	Requisitos e orientações para estabelecer, implementar, manter e melhorar continuamente o SGPI.
ABNT NBR ISO/IEC 27001 e família 27000	Referência de integração com SGSI, controles de segurança, riscos e declaração de aplicabilidade.
ABNT NBR ISO/IEC 29100	Estrutura e princípios de privacidade relacionados ao tratamento de dados pessoais.
ABNT NBR ISO/IEC 27018 e 29151	Boas práticas adicionais para proteção de dados pessoais em nuvem pública e para controles de proteção de dados pessoais.
Normativos setoriais e exigências de órgãos competentes	Aplicáveis ao credenciamento, operação, segurança, disponibilidade e rastreabilidade de registradora de contratos de veículos.
Contratos, DPAs, SLAs e políticas internas	Requisitos contratuais e organizacionais complementares a serem controlados no SGPI.

Hierarquia de requisitos: Em caso de conflito, prevalecem a legislação e os regulamentos aplicáveis. As normas técnicas e políticas internas complementam a governança e devem ser usadas como critérios de evidência, sem reduzir obrigações legais ou contratuais.

3. Termos, Definições e Critérios de Interpretação

Termo	Definição operacional para a 1 IT
Dado pessoal (DP)	Informação relacionada a pessoa natural identificada ou identificável, incluindo dados cadastrais, contratuais, identificadores, logs, credenciais, documentos e dados

	vinculados a veículo/contrato quando relacionados a pessoa natural.
Dado pessoal sensível	Dado sobre origem racial/étnica, convicção religiosa, opinião política, filiação, saúde, vida sexual, genética ou biometria. Não é esperado no processo fim, salvo hipóteses excepcionais, RH, identificação, incidentes ou obrigações legais.
Tratamento	Toda operação com DP: coleta, recepção, validação, classificação, uso, acesso, reprodução, transmissão, armazenamento, compartilhamento, eliminação, avaliação, controle e auditoria.
Controlador	Agente que decide finalidades e meios essenciais do tratamento.
Operador	Agente que trata DP em nome e sob instruções do controlador.
Controlador conjunto	Situação em que a 1 IT e outra organização determinam conjuntamente finalidades e meios do tratamento.
Titular	Pessoa natural a quem se referem os dados pessoais tratados.
Encarregado/DPO	Pessoa indicada para atuar como canal entre titular, agente de tratamento e ANPD, além de orientar internamente boas práticas.
SGPI	Sistema de gestão da privacidade da informação: conjunto de políticas, processos, controles, registros, responsabilidades, riscos e melhoria contínua para proteção de dados pessoais.
ROPA	Registro das operações de tratamento de dados pessoais, incluindo finalidades, bases legais, titulares, dados, sistemas, compartilhamentos, retenção, riscos e controles.
AIPD/RIPD	Avaliação/Relatório de Impacto à Proteção de Dados Pessoais para tratamentos de maior risco.
Suboperador	Fornecedor contratado por operador para apoiar tratamento de DP em nome do controlador.

4. Contexto da Organização e Escopo do SGPI

4.1 Entendendo a organização e seu contexto

A 1 IT deve determinar as questões internas e externas que afetam sua capacidade de alcançar os resultados pretendidos do SGPI. A análise deve considerar o contexto regulatório de registradora de contratos de veículos, o uso intensivo de tecnologia, a

dependência de integração com clientes e terceiros, os requisitos de disponibilidade, segurança, rastreabilidade e preservação de evidências, bem como a expectativa de transparência e proteção de titulares.

Questão	Impacto no SGPI	Controle mínimo
Regulação e credenciamento	Exigência de segurança, governança, rastreabilidade, disponibilidade e atendimento a requisitos de órgãos competentes.	Matriz regulatória e evidências de conformidade.
Operação tecnológica integrada	Risco de falhas em APIs, logs, bancos, filas, integrações e troca de arquivos.	Arquitetura segura, gestão de mudanças, monitoramento e testes.
Volume e criticidade de dados	Tratamentos podem envolver dados cadastrais, financeiros, contratuais, identificação e logs.	ROPA, minimização, criptografia, controle de acesso e retenção.
Terceiros e suboperadores	Dependência de cloud, datacenter, suporte, desenvolvimento e ferramentas de comunicação.	Due diligence, DPA, revisão de suboperadores e SLA de incidente.
Ameaças cibernéticas	Risco de vazamento, ransomware, exfiltração, uso indevido e indisponibilidade.	SGSI, backups, SIEM, EDR, MFA, hardening e resposta a incidentes.
Mudanças societárias e de razão social	Necessidade de manter rastreabilidade documental e continuidade de obrigações.	Controle documental e atualização de contratos/políticas.

4.2 Necessidades e expectativas das partes interessadas

Parte interessada	Necessidade/expectativa	Como atender
Titulares de dados	Transparência, segurança, atendimento de direitos e prevenção de danos.	Aviso de privacidade, canal LGPD, segurança e registro de solicitações.
Clientes e instituições parceiras	Conformidade, disponibilidade, integridade, sigilo, rastreabilidade e suporte.	Contratos, SLAs, evidências, auditorias e relatórios.

Órgãos reguladores/competentes	Cumprimento de requisitos setoriais, segurança e prestação de contas.	Matriz regulatória e dossiê de conformidade.
ANPD	Conformidade com LGPD, cooperação, governança e resposta a incidentes.	DPO, registros, ROPA, RIPD, comunicação e evidências.
Colaboradores e prestadores	Orientação clara, treinamento, acesso adequado e proteção de dados profissionais.	Políticas, termos, treinamentos e controles de RH.
Fornecedores/suboperadores	Instruções claras, escopo de tratamento e requisitos contratuais.	DPA, matriz de instruções e due diligence.
Alta Direção e sócios	Redução de risco, reputação, continuidade operacional e atendimento a credenciamentos.	Indicadores, auditorias, análise crítica e plano de melhoria.

4.3 Determinando o escopo do SGPI

O escopo do SGPI inclui os tratamentos de dados pessoais executados pela 1 IT nos processos finalísticos e de suporte. A delimitação deve estar documentada e revisada sempre que houver mudança relevante de processo, sistema, fornecedor, contrato, órgão de relacionamento, escopo de credenciamento ou categoria de dados.

Incluído no escopo	Exemplo de tratamento
Operação de registro de contratos de veículos	Recepção de dados, validação, registro, consulta, manutenção, evidências e comunicações associadas.
Gestão de clientes e usuários	Cadastro de representantes, credenciais, perfis, logs de acesso, tickets e comunicações.
Tecnologia e segurança	Logs, monitoramento, backups, incidentes, controle de acesso, ambientes e desenvolvimento.
Atendimento, ouvidoria e LGPD	Solicitações de titulares, reclamações, consultas, protocolos e respostas.
RH, fornecedores e administração	Dados de colaboradores, candidatos, prestadores, representantes, faturamento e contratos.

4.4 Sistema de Gestão da Privacidade da Informação

A 1 IT deve estabelecer, implementar, manter e melhorar continuamente o SGPI, incluindo políticas, processos, responsabilidades, controles, avaliação de riscos, tratamento de riscos, indicadores, auditoria interna e análise crítica. O SGPI deve interagir com o SGSI e com a governança corporativa, jurídica, operacional e de fornecedores.

4.4.1 Macroprocesso do SGPI

- Planejar: definir contexto, escopo, partes interessadas, política, objetivos, riscos e controles.
- Implementar: estabelecer procedimentos, controles técnicos, contratos, ROPA, AIPD/RIPD, canais e treinamento.
- Operar: executar tratamentos, atender titulares, registrar evidências, monitorar segurança e gerenciar fornecedores.
- Verificar: medir indicadores, auditar, revisar incidentes, avaliar riscos e analisar conformidade.
- Melhorar: tratar não conformidades, causas, ações corretivas, mudanças e lições aprendidas.

5. Liderança

5.1 Liderança e comprometimento

A Alta Direção deve demonstrar comprometimento com o SGPI mediante aprovação de políticas e objetivos, provisão de recursos, patrocínio à cultura de privacidade, integração dos requisitos aos processos de negócio, apoio ao DPO, análise de riscos e participação na análise crítica.

Obrigaç�o da lideran�a	Evid�ncia m�nima
Aprovar pol�tica e objetivos de privacidade.	Pol�tica aprovada, comunica��o interna e metas.
Integrar SGPI aos processos de neg�cio.	Mapeamento de processos, procedimentos e ROPA.
Disponibilizar recursos.	Or�amento, ferramentas, equipe, consultoria, treinamento.
Comunicar import�ncia da privacidade.	Comunicados, campanhas, participa��o em comit�s.
Garantir resultados pretendidos.	Indicadores, auditorias, planos de a��o.
Promover melhoria cont�nuas.	Atas, revis�o de riscos, backlog de melhorias.

5.2 Política de privacidade

A política de privacidade da 1 IT deve ser apropriada ao propósito da organização, compatível com a estratégia, incluir compromissos de atendimento a requisitos legais e de melhoria contínua, ser documentada, comunicada internamente e disponibilizada às partes interessadas pertinentes quando adequado.

5.2.1 Declaração de política

Política institucional: A 1 IT compromete-se a tratar dados pessoais de forma lícita, transparente, segura, proporcional e rastreável, observando a LGPD, requisitos regulatórios, contratuais e normativos aplicáveis, adotando privacidade por design e por default, proteção contra incidentes, atendimento aos direitos dos titulares, governança por riscos, melhoria contínua e prestação de contas.

5.3 Papéis, responsabilidades e autoridades

Papel	Responsabilidades
Alta Direção	Aprovar SGPI, política, objetivos, recursos, riscos residuais relevantes, respostas a incidentes críticos e análise crítica.
Encarregado/DPO	Atuar como canal com titulares e ANPD, orientar internamente, apoiar AIPD/RIPD, acompanhar solicitações, incidentes, treinamentos e indicadores.
Comitê de Privacidade e Segurança	Avaliar riscos, mudanças, fornecedores, incidentes, não conformidades, políticas, indicadores e prioridades.
TI/Segurança da Informação	Implementar controles de segurança, IAM, logs, backup, criptografia, monitoramento, resposta técnica a incidentes e desenvolvimento seguro.
Jurídico/Compliance	Avaliar bases legais, contratos, DPAs, respostas regulatórias, litígios, termos, avisos e obrigações legais.
Operações de Registro	Executar tratamentos conforme procedimento, validar dados, manter evidências, preservar sigilo e reportar desvios.
RH/DP	Proteger dados de candidatos, colaboradores, dependentes, benefícios, folha, saúde ocupacional e treinamento.
Gestores de processo	Manter ROPA, aprovar fluxos, validar acessos, treinar equipes e acompanhar riscos.

Colaboradores e terceiros	Cumprir políticas, proteger dados, reportar incidentes e usar dados apenas para finalidade autorizada.
---------------------------	--

6. Planejamento

6.1 Ações para abordar riscos e oportunidades

O planejamento do SGPI deve considerar riscos e oportunidades capazes de afetar a conformidade legal, a privacidade dos titulares, a confiança de clientes, a segurança operacional, a continuidade do negócio e a capacidade de demonstrar prestação de contas.

6.1.1 Geral

- Prevenir ou reduzir efeitos indesejados sobre titulares e sobre a organização.
- Aumentar efeitos desejáveis como confiança, conformidade, rastreabilidade, segurança e eficiência operacional.
- Integrar ações aos processos do SGPI e avaliar a eficácia dessas ações.
- Considerar risco aos direitos e liberdades dos titulares, risco regulatório, risco contratual, risco cibernético e risco reputacional.

6.1.2 Avaliação de riscos de privacidade

Etapa	Descrição	Registro
Identificação	Identificar eventos de risco, ameaças, vulnerabilidades, ativos, titulares, dados e processos afetados.	Registro de riscos e ROPA.
Análise	Avaliar probabilidade, impacto ao titular, impacto à 1 IT, volume, sensibilidade, exposição, dependência de terceiros e controles existentes.	Matriz de risco inerente.
Avaliação	Comparar com critérios de aceitação e priorizar tratamento.	Risco residual e decisão.
AIPD/RIPD	Elaborar avaliação de impacto para tratamentos de alto risco ou quando requerido.	Relatório de impacto e plano.
Revisão	Reavaliar por mudança relevante, incidente, auditoria, novo fornecedor, nova finalidade ou novo dado.	Histórico de revisão.

6.1.3 Tratamento de riscos de privacidade

Resposta	Quando aplicar	Evidência
Mitigar	Risco alto ou médio com controles viáveis.	Plano de tratamento e comprovação.
Evitar	Tratamento desnecessário, desproporcional ou sem base legal.	Decisão formal de não tratar.
Transferir/compartilhar	Risco associado a fornecedor/seguro/contrato, sem eliminar responsabilidade legal.	Contrato, DPA, seguro, SLA.
Aceitar	Risco residual dentro do apetite definido e aprovado.	Aceite formal por autoridade competente.

6.2 Objetivos de privacidade e planejamento para alcançá-los

Objetivo	Indicador	Meta inicial	Responsável
Manter ROPA atualizado.	% de tratamentos revisados no trimestre.	>= 95%	DPO + Gestores.
Atender direitos de titulares dentro do prazo.	% de solicitações respondidas no SLA.	100%	DPO + Área responsável.
Reduzir risco de acesso indevido.	% de acessos recertificados.	>= 95% trimestral.	TI/SI + Gestores.
Treinar equipe em LGPD e segurança.	% de colaboradores treinados.	100% admissional e anual.	RH + DPO.
Gerenciar incidentes com dados pessoais.	Tempo de triagem e classificação.	Triagem em até 24h úteis.	SI + DPO.
Controlar fornecedores críticos.	% de fornecedores com DPA/due diligence.	100% críticos.	Compras/Jurídico/DPO.

6.3 Planejamento de mudanças

Toda mudança relevante deve ser avaliada antes da implantação para identificar impacto em privacidade, segurança, bases legais, titulares, terceiros, retenção, contrato e requisitos regulatórios.

Tipo de mudança	Avaliação obrigatória
Novo sistema, API ou integração	ROPA, base legal, segurança, minimização, logs, acesso, testes, fornecedor e AIPD quando necessário.
Nova finalidade de uso de dados	Compatibilidade, base legal, transparência, retenção e comunicação ao titular.
Novo fornecedor/suboperador	Due diligence, contrato/DPA, localidade, incidente, subcontratação e segurança.
Mudança de arquitetura/hospedagem	Transferência internacional, criptografia, backup, continuidade, IAM e segregação.
Mudança societária/razão social	Atualização de contratos, avisos, cadastros regulatórios e controle documental.

7. Apoio

7.1 Recursos

A 1 IT deve prover recursos adequados para operar o SGPI, incluindo pessoas, ferramentas, infraestrutura, consultoria, treinamento, gestão documental, canais de atendimento, segurança, monitoramento e auditoria.

7.2 Competência

Função	Competência mínima
DPO/Encarregado	LGPD, gestão de privacidade, direitos dos titulares, incidentes, ROPA, AIPD/RIPD, comunicação com ANPD e governança.
TI/SI	Segurança de aplicações, IAM, logs, criptografia, backup, resposta a incidentes, hardening, cloud/datacenter e SDLC seguro.
Operações	Finalidade, minimização, sigilo, uso correto do sistema, registro de evidências e escalonamento de incidentes.
Jurídico/Compliance	Bases legais, contratos, DPAs, sanções, regulamentos, riscos e comunicações formais.

RH/DP	Tratamento de dados trabalhistas, sensíveis, retenção, confidencialidade e atendimento interno.
Atendimento/Ouvidoria	Identificação de demandas LGPD, proteção de dados no atendimento e comunicação clara.

7.3 Conscientização

- Todos devem conhecer a política de privacidade, consequências de não conformidade, canais de reporte, práticas de mesa limpa/tela limpa e regras de compartilhamento.
- Treinamentos devem ser admissionais, anuais e por mudança relevante; terceiros críticos devem receber orientações proporcionais ao risco.
- Campanhas devem abordar phishing, senhas, MFA, manipulação de planilhas, envio por e-mail, uso de nuvem, incidentes, atendimento a titulares e retenção.

7.4 Comunicação

Comunicação	Público	Canal	Periodicidade
Política de privacidade interna	Colaboradores e prestadores	Repositório, e-mail, treinamento	Admissão e revisão.
Aviso de privacidade externo	Titulares e partes externas	Site/portal/canal de atendimento	Sempre disponível.
Indicadores do SGPI	Alta Direção e Comitê	Relatório/ata	Mensal ou trimestral.
Solicitações LGPD	Titulares	Canal LGPD/e-mail/ticket	Sob demanda.
Incidentes relevantes	ANPD/titulares/clientes	Procedimento CIS e comunicação formal	Conforme gravidade/prazo legal.
Mudanças de privacidade	Áreas impactadas	Comitê/e-mail/repositório	Antes da implantação.

7.5 Informação documentada

7.5.1 Geral

A 1 IT deve manter documentos e registros necessários para a operação efetiva do SGPI e para demonstrar conformidade com LGPD, contratos e requisitos da norma.

7.5.2 Criação e atualização

Todo documento deve possuir identificação, versão, responsável, aprovador, classificação, data, histórico de alteração, local de guarda e periodicidade de revisão.

7.5.3 Controle da informação documentada

Tipo de informação	Controle
Políticas e manuais	Aprovação formal, versão, publicação controlada e revisão anual.
Registros de tratamento	ROPA, logs, trilhas e evidências protegidos contra alteração indevida.
AIPD/RIPD	Guarda restrita, revisão por mudança e aprovação do plano de tratamento.
Solicitações de titulares	Protocolo, validação de identidade, resposta, prazo e retenção.
Incidentes	Registro por no mínimo 5 anos, evidências técnicas, decisões e comunicações.
Contratos e DPAs	Controle por fornecedor/cliente, cláusulas de privacidade e revisão periódica.

8. Operação

8.1 Planejamento e controle operacional

A operação do SGPI deve ocorrer mediante critérios planejados, procedimentos, controles técnicos e administrativos, responsabilidades definidas e evidências. Processos terceirizados devem ser controlados conforme requisitos contratuais, de segurança e de privacidade.

8.2 Avaliação de riscos de privacidade

A avaliação de riscos deve ser realizada no início do tratamento, revisada periodicamente e atualizada em mudanças relevantes. Tratamentos de alto risco devem ser submetidos a AIPD/RIPD.

8.3 Tratamento de riscos de privacidade

O tratamento dos riscos deve ser acompanhado até conclusão, com responsáveis, prazos, recursos, evidências, aceitação do risco residual e reporte ao Comitê quando relevante.

Registro operacional obrigatório	Finalidade	Responsável
ROPA / Mapa de Dados	Controlar operações de tratamento.	DPO + Gestores.
Matriz de bases legais	Justificar licitude do tratamento.	Jurídico/Compliance + DPO.
Matriz de riscos de privacidade	Priorizar mitigação.	DPO + SI.
AIPD/RIPD	Avaliar alto risco e mitigação.	DPO + Área + SI + Jurídico.
Registro de solicitações LGPD	Atender direitos e evidenciar prazos.	DPO + Atendimento.
Registro de incidentes	Tratar eventos e cumprir comunicação.	SI + DPO.
Due diligence de fornecedores	Validar operadores/suboperadores.	Compras + Jurídico + DPO + SI.

9. Avaliação de Desempenho

9.1 Monitoramento, medição, análise e avaliação

Indicador	Fórmula/Fonte	Meta	Frequência
Cobertura do ROPA	Tratamentos registrados / tratamentos conhecidos.	>= 95%	Trimestral.
SLA de titulares	Solicitações respondidas no prazo / total.	100%	Mensal.
Treinamento LGPD/SI	Pessoas treinadas / público obrigatório.	100%	Mensal/Anual.
Acessos recertificados	Perfis revisados / perfis ativos.	>= 95%	Trimestral.
Fornecedores críticos avaliados	Fornecedores com due diligence/DPA / total críticos.	100%	Semestral.
Incidentes triados no prazo	Incidentes triados em até 24h úteis / total.	>= 95%	Mensal.

Planos de ação vencidos	Ações vencidas / ações abertas.	<= 5%	Mensal.
-------------------------	---------------------------------	-------	---------

9.2 Auditoria interna

9.2.1 Geral

A auditoria interna deve verificar se o SGPI atende aos requisitos da LGPD, da política interna, da norma de referência, dos contratos e dos procedimentos. A auditoria deve ser independente em relação à atividade auditada, proporcional ao risco e documentada.

9.2.2 Programa de auditoria interna

Etapa	Descrição
Planejamento	Definir escopo, critérios, auditores, áreas, documentos e cronograma.
Execução	Entrevistas, amostragem de registros, teste de controles, análise de evidências e inspeção de sistemas.
Relatório	Registrar conformidades, não conformidades, oportunidades de melhoria, riscos e recomendações.
Plano de ação	Definir causa raiz, ação corretiva, responsável, prazo e evidência esperada.
Verificação de eficácia	Confirmar se a ação eliminou causa e reduziu risco.

9.3 Análise crítica pela direção

9.3.1 Geral

A Alta Direção deve realizar análise crítica do SGPI em intervalos planejados para assegurar sua adequação, suficiência, eficácia e alinhamento estratégico.

9.3.2 Entradas para análise crítica

- Mudanças internas e externas relevantes.
- Resultados de auditorias e monitoramento.
- Indicadores e metas de privacidade.
- Status de não conformidades e ações corretivas.
- Incidentes, solicitações de titulares e reclamações.
- Riscos, oportunidades e eficácia dos planos de tratamento.

- Desempenho de fornecedores críticos.
- Necessidade de recursos e mudanças no SGPI.

9.3.3 Resultados da análise crítica

- Decisões de melhoria do SGPI.
- Mudanças em políticas, processos, objetivos, controles e recursos.
- Aprovação ou rejeição de riscos residuais relevantes.
- Priorização de ações, investimentos, auditorias e treinamentos.
- Encaminhamentos a responsáveis e prazos.

10. Melhoria

10.1 Melhoria contínua

A 1 IT deve melhorar continuamente a adequação, suficiência e eficácia do SGPI, com base em resultados de auditorias, indicadores, incidentes, reclamações, mudanças legais, avaliações de fornecedores, testes de segurança, análise crítica e lições aprendidas.

10.2 Não conformidade e ação corretiva

Fase	Atividade
Registro	Registrar não conformidade, requisito afetado, evidência e impacto.
Contenção	Aplicar ação imediata para reduzir dano ou exposição.
Causa raiz	Analisar causa usando método adequado, como 5 porquês ou Ishikawa.
Ação corretiva	Definir ação para eliminar causa e prevenir recorrência.
Eficácia	Verificar se a ação funcionou e registrar evidência.
Aprendizado	Atualizar políticas, treinamentos, controles e riscos.

11. Matriz de Cobertura Integral da ABNT NBR ISO/IEC 27701:2026

A matriz abaixo demonstra como os tópicos estruturais da norma foram considerados no MA-004 e quais evidências devem ser mantidas pela 1 IT. Ela deve ser usada como

roteiro de auditoria interna, preparação para certificação e acompanhamento de implantação do SGPI.

Item da norma	Tema	Implementação no MA-004 / SGPI	Evidências esperadas
0.1	Introdução e justificativa do SGPI	Integração entre privacidade, segurança, LGPD, evidências e prestação de contas.	Política, ROPA, AIPD/RIPD, matriz de riscos, indicadores.
0.2	Compatibilidade com outros sistemas de gestão	Alinhamento com SGSI, compliance, gestão de riscos, qualidade e continuidade.	Mapa de integração, atas do comitê, auditorias integradas.
1	Escopo	Aplicação a controladores e operadores de dados pessoais, com foco na 1 IT.	Escopo formal, limites, processos e papéis.
2	Referência normativa	Considera estrutura de privacidade e demais normas complementares aplicáveis.	Lista de referências e controle documental.
3	Termos e definições	Padronização de termos como SGPI, controlador, operador, titular, risco e informação documentada.	Glossário interno e treinamentos.
4.1	Entendendo a organização e seu contexto	Determinação de questões internas/externas, legais, regulatórias, contratuais e tecnológicas.	Matriz de contexto e riscos.
4.2	Partes interessadas	Identificação de titulares, clientes, órgãos, parceiros, fornecedores, ANPD, colaboradores e acionistas.	Matriz de partes interessadas.
4.3	Escopo do SGPI	Determinação dos limites, tratamentos, unidades, sistemas e processos cobertos.	Declaração de escopo e mapa de processos.

4.4	Sistema de gestão da privacidade da informação	Processos necessários, interações, responsabilidades e melhoria contínua.	Manual, procedimentos e indicadores.
5.1	Liderança e comprometimento	Alta direção provê recursos, aprova políticas, promove cultura e participa da análise crítica.	Ata de aprovação, objetivos, recursos e análises críticas.
5.2	Política de privacidade	Política compatível com direção estratégica e requisitos de privacidade.	Política publicada e comunicada.
5.3	Papéis, responsabilidades e autoridades	Atribuições de DPO, gestores, TI/SI, jurídico/compliance, operações e terceiros.	Matriz RACI, nomeações e descrições de função.
6.1.1	Riscos e oportunidades - geral	Planejamento para prevenir efeitos indesejados e alcançar resultados pretendidos.	Metodologia de riscos e plano de tratamento.
6.1.2	Avaliação de riscos de privacidade	Critérios, identificação, análise, avaliação, impactos aos titulares e risco residual.	Registro de riscos e AIPD/RIPD.
6.1.3	Tratamento de riscos de privacidade	Seleção de controles, plano de tratamento, aprovação e aceitação de riscos residuais.	Plano de tratamento e declaração de aplicabilidade.
6.2	Objetivos de privacidade	Objetivos mensuráveis, monitorados, comunicados e revisados.	Indicadores e metas.
6.3	Planejamento de mudanças	Avaliação formal de impactos de mudanças no SGPI.	Formulário de mudança e análise de impacto.
7.1	Recursos	Recursos humanos, tecnológicos, financeiros e documentais.	Plano orçamentário e recursos aprovados.
7.2	Competência	Competências de privacidade por papel.	Matriz de competência e

			registros de treinamento.
7.3	Conscientização	Conhecimento da política, riscos, consequências e deveres.	Campanhas, EAD e aceite de políticas.
7.4	Comunicação	Comunicação interna/externa, canais, responsáveis e periodicidade.	Plano de comunicação.
7.5.1	Informação documentada - geral	Documentos e registros necessários ao SGPI.	Lista mestra de documentos.
7.5.2	Criação e atualização	Identificação, descrição, formato, revisão e aprovação.	Fluxo de controle documental.
7.5.3	Controle da informação documentada	Disponibilidade, proteção, distribuição, acesso, retenção e descarte.	Repositório controlado e trilhas de revisão.
8.1	Planejamento e controle operacional	Execução de processos conforme critérios, controles e evidências.	POPs, logs e registros operacionais.
8.2	Avaliação de riscos de privacidade em operação	Reavaliação periódica e por mudanças relevantes.	Registro de riscos atualizado.
8.3	Tratamento de riscos em operação	Implementação e monitoramento dos planos de tratamento.	Plano de ação e evidências.
9.1	Monitoramento, medição, análise e avaliação	Indicadores de privacidade, segurança e conformidade.	Painel de indicadores.
9.2.1	Auditoria interna - geral	Auditorias planejadas para verificar conformidade do SGPI.	Plano, checklist e relatório.
9.2.2	Programa de auditoria interna	Critérios, escopo, frequência, independência e ações.	Programa anual de auditoria.
9.3.1	Análise crítica - geral	Avaliação periódica pela direção.	Ata de análise crítica.

9.3.2	Entradas da análise crítica	Mudanças, resultados, não conformidades, indicadores, auditorias, riscos, oportunidades.	Dossiê de entradas.
9.3.3	Resultados da análise crítica	Decisões sobre melhoria, recursos, mudanças e prioridades.	Plano de ação aprovado.
10.1	Melhoria contínua	Aperfeiçoamento sistemático do SGPI.	Backlog de melhorias e indicadores.
10.2	Não conformidade e ação corretiva	Tratamento de NCs, causas, ações, eficácia e registros.	Formulário de NC e ação corretiva.

11.1 Matriz consolidada dos controles normativos

Item	Aplicação	Controle	Diretriz operacional	Evidência
B.1.2.2	Controlador	Identificação e documentação do propósito	Documentar finalidade, compatibilidade com o negócio e limites de uso antes de iniciar o tratamento.	ROPA, matriz finalidade/base legal, especificação funcional.
B.1.2.3	Controlador	Identificação de bases legais	Registrar a hipótese legal de cada operação de tratamento e sua justificativa.	Matriz de bases legais, parecer jurídico quando necessário.
B.1.2.4	Controlador	Quando e como obter consentimento	Usar consentimento apenas quando adequado; garantir destaque, granularidade e possibilidade de revogação.	Termo de consentimento, tel de aceite, registro de origem.

B.1.2.5	Controlador	Obtenção e registro do consentimento	Manter evidência de quem consentiu, quando, para que finalidade, por qual canal e versão do texto.	Log de consentimento e histórico de versões
B.1.2.6	Controlador	Avaliação de impacto de privacidade	Realizar AIPD/RIPD para alto risco, larga escala, dados sensíveis, decisão automatizada ou mudanças relevantes.	Relatório de impacto, plano de mitigação e aprovação.
B.1.2.7	Controlador	Contratos com operadores de DP	Contratar operadores com cláusulas de instrução, segurança, sigilo, suboperadores, incidente e devolução/descarte.	Contrato, DPA, due diligence, SLA de incidente.
B.1.2.8	Controlador	Controlador conjunto de DP	Definir responsabilidades entre controladores quando houver decisão conjunta sobre finalidades e meios.	Acordo de controladoria conjunta e matriz de responsabilidades.
B.1.2.9	Controlador	Registros relacionados ao tratamento de DP	Manter registros completos e auditáveis das operações de tratamento.	ROPA, logs, evidências de tratamento e revisões
B.1.3.2	Controlador	Obrigações perante titulares	Mapear e cumprir direitos de titulares conforme LGPD.	Procedimento de direitos, SLA e registros de atendimento.
B.1.3.3	Controlador	Informações para titulares	Definir conteúdo mínimo de transparência, incluindo finalidade, base legal, compartilhamento,	Aviso de privacidade e respostas-padrão

			retenção e contato do DPO.	
B.1.3.4	Controlador	Fornecimento de informações aos titulares	Disponibilizar informações claras, acessíveis, atualizadas e em linguagem adequada.	Portal/canal LGPD, FAQ, política publicada.
B.1.3.5	Controlador	Modificar ou retirar consentimento	Disponibilizar mecanismo para retirada de consentimento e atualização de preferências.	Registro de revogação e bloqueio de uso.
B.1.3.6	Controlador	Oposição ao tratamento	Permitir oposição a tratamento irregular ou baseado em hipóteses que admitam contestação.	Fluxo de objeção, decisão fundamentada e resposta.
B.1.3.7	Controlador	Acesso, correção ou exclusão	Atender pedidos de confirmação, acesso, correção, anonimização, bloqueio, eliminação e portabilidade quando cabível.	Protocolo, evidências de validação de identidade e resposta.
B.1.3.8	Controlador	Informar terceiros	Comunicar correções, eliminações ou restrições a terceiros com quem os dados foram compartilhados quando cabível.	Registro de destinatários e comunicações.
B.1.3.9	Controlador	Cópia de DP tratados	Fornecer cópia ou extrato dos dados pessoais em formato seguro e adequado.	Arquivo de resposta, trilha de entrega e comprovante.
B.1.3.10	Controlador	Tratamento de solicitações	Registrar, triagem, validar identidade, classificar, responder	Sistema de tickets LGPD e SLA.

			e reter evidência das solicitações.	
B.1.3.11	Controlador	Tomada de decisão automatizada	Mapear decisões automatizadas, critérios, revisão humana e explicabilidade quando aplicável.	Inventário de algoritmos/regras, logs e revisão.
B.1.4.2	Controlador	Limitação da coleta	Coletar somente dados necessários à finalidade declarada.	Revisão de campo minimização de AF e formulários.
B.1.4.3	Controlador	Limitação do tratamento	Usar dados apenas nas finalidades autorizadas e compatíveis.	Controle de finalidade, segregação de bases e logs.
B.1.4.4	Controlador	Precisão e qualidade	Manter dados exatos, completos e atualizados quando necessário.	Validações, correções e trilhas de atualização.
B.1.4.5	Controlador	Objetivos de minimização de DP	Definir metas para reduzir volume, exposição e retenção de dados pessoais.	Indicadores de minimização e revisão de cadastr
B.1.4.6	Controlador	Desidentificação e exclusão ao final do tratamento	Anonimizar, pseudonimizar ou eliminar dados ao fim da finalidade e prazo de retenção.	Rotina de descarte evidência técnica.
B.1.4.7	Controlador	Arquivos temporários	Controlar, expirar e eliminar arquivos temporários, caches, exports e bases de teste.	Política de temporários, varreduras e logs e limpeza.
B.1.4.8	Controlador	Retenção	Definir prazos por base legal, contrato, regulação e necessidade operacional.	Tabela de temporalidade e revisão periódica.
B.1.4.9	Controlador	Descarte	Executar descarte seguro e	Certificado/registo de descarte e

			documentado de dados e mídias.	aprovação.
B.1.4.10	Controlador	Controles de transmissão de DP	Proteger dados em trânsito por criptografia, autenticação, integridade e canal autorizado.	TLS, VPN, chaves, logs e testes.
B.1.5.2	Controlador	Bases para transferências entre jurisdições	Avaliar base legal e salvaguardas para transferência internacional.	Registro de transferência e cláusulas contratuais.
B.1.5.3	Controlador	Países/organizações de destino	Documentar países, provedores e organizações internacionais que recebem DP.	Inventário de fornecedores e localidade de dados
B.1.5.4	Controlador	Registros de transferência de DP	Manter registros de transferências, finalidade, destinatário, base e salvaguarda.	Registro de transferência e revisão.
B.1.5.5	Controlador	Registros de divulgação a terceiros	Registrar divulgações pontuais, obrigatórias ou contratuais a terceiros.	Log de divulgação autorização.
B.2.2.2	Operador	Acordo com o cliente	Tratar DP conforme contrato e instruções documentadas do controlador.	Contrato, ordem de serviço, matriz de instruções.
B.2.2.3	Operador	Propósitos da organização	Não usar dados do cliente para finalidades próprias incompatíveis.	Política interna e segregação lógica
B.2.2.4	Operador	Uso para marketing e propaganda	Vedado uso de DP tratados como operadora para marketing próprio sem autorização válida.	Cláusula contratual e bloqueios de uso

B.2.2.5	Operador	Instruções infradoras	Alertar o controlador quando instrução aparentar violar lei, contrato ou política.	Registro de alerta e decisão do cliente.
B.2.2.6	Operador	Obrigações do cliente	Definir obrigações do controlador em instruções, bases legais, titulares e informações necessárias.	DPA, matriz de responsabilidades SLA.
B.2.2.7	Operador	Registros relativos ao tratamento	Manter registros das operações executadas em nome do controlador.	Logs, ROPA como operadora e evidências.
B.2.3.2	Operador	Compliance com obrigações perante titulares	Apoiar o controlador no atendimento aos direitos de titulares dentro de prazo contratual.	Ticket de apoio, log e retorno ao controlador.
B.2.4.2	Operador	Arquivos temporários	Remover arquivos temporários criados em suporte, migração, teste ou incidente.	Registro de limpeza e controles de acesso.
B.2.4.3	Operador	Devolução, transferência ou descarte de DP	Ao término do contrato, devolver, transferir, bloquear ou descartar dados conforme instrução.	Termo de devolução/descarte e evidências.
B.2.4.4	Operador	Controles de transmissão de DP	Utilizar canais seguros para troca de dados do controlador.	TLS, SFTP, VPN, criptografia e logs.
B.2.5.2	Operador	Fundamentação para transferência entre jurisdições	Transferir dados apenas mediante autorização/instrução e salvaguardas.	Contrato, localidade de hospedagem e avaliação.
B.2.5.3	Operador	Países/organizações de destino	Informar ao controlador a localidade de	Lista de suboperadores e regiões de cloud.

			processamento e suboperadores.	
B.2.5.4	Operador	Registros de divulgações a terceiros	Manter registro de divulgações autorizadas ou obrigatórias.	Log de divulgação base e aprovador.
B.2.5.5	Operador	Notificação de solicitações de divulgação de DP	Informar ao controlador solicitações legais/administrativas quando permitido.	Registro de solicitação e comunicação.
B.2.5.6	Operador	Divulgações legalmente obrigatórias	Cumprir obrigação legal preservando sigilo e mínima divulgação.	Parecer jurídico e protocolo.
B.2.5.7	Operador	Divulgação de subcontratados	Disponibilizar lista de suboperadores e serviços envolvidos.	Catálogo de suboperadores.
B.2.5.8	Operador	Envolvimento de subcontratado	Obter autorização e impor obrigações equivalentes ao suboperador.	Contrato com suboperador e due diligence.
B.2.5.9	Operador	Troca de subcontratado	Comunicar troca e permitir objeção quando contratualmente previsto.	Notificação, avaliação e aceite.
B.3.3	Comum	Políticas de segurança da informação	Manter políticas integradas de SI e privacidade.	PSI, política de privacidade, revisão anual.
B.3.4	Comum	Papéis e responsabilidades em segurança da informação	Definir responsabilidades de SI relacionadas a DP.	Matriz RACI, nomeações e descrições.
B.3.5	Comum	Classificação da informação	Classificar dados pessoais por criticidade, sensibilidade e restrição.	Matriz de classificação e etiquetas.

B.3.6	Comum	Rotulagem da informação	Aplicar rótulos em documentos, bases, exports e repositórios.	Etiquetas e configuração DLP.
B.3.7	Comum	Transferência de informação	Formalizar meios seguros de transferência interna e externa.	Procedimento de transferência segura
B.3.8	Comum	Gestão de identidade	Controlar identidades humanas, técnicas, administrativas e de serviço.	IAM, MFA, revisão de contas.
B.3.9	Comum	Direitos de acesso	Aplicar menor privilégio, segregação, aprovação e revisão periódica.	Matriz de acesso, logs, recertificação
B.3.10	Comum	Segurança em contratos de fornecedores	Incluir requisitos de SI, privacidade, auditoria, incidente e subcontratação.	Cláusulas, DPA e due diligence.
B.3.11	Comum	Planejamento e preparação para incidentes	Definir playbooks, equipe, canais, critérios e simulações.	Plano de resposta a incidentes.
B.3.12	Comum	Resposta a incidentes de segurança	Detectar, conter, erradicar, recuperar, comunicar e registrar incidentes.	Registro de incidente e lições aprendidas.
B.3.13	Comum	Requisitos legais, estatutários, regulatórios e contratuais	Manter matriz de requisitos aplicáveis à privacidade e ao negócio.	Matriz legal e revisão.
B.3.14	Comum	Proteção de registros	Proteger registros contra perda, alteração indevida e acesso não autorizado.	Controle de retenção, backup e assinatura.

B.3.15	Comum	Análise crítica independente da segurança	Realizar avaliações independentes, auditorias e testes.	Relatórios de auditoria/pentest.
B.3.16	Comum	Compliance com políticas, regras e normas	Monitorar adesão às políticas e tratar exceções.	Checklist de conformidade e ações.
B.3.17	Comum	Conscientização, educação e treinamento	Treinar colaboradores e terceiros por perfil de risco.	Trilha EAD, listas e certificados.
B.3.18	Comum	Acordos de confidencialidade ou não divulgação	Formalizar NDA/termo de sigilo para acesso a DP.	Termos assinados controle.
B.3.19	Comum	Mesa limpa e tela limpa	Reduzir exposição física e visual de DP.	Política e inspeção
B.3.20	Comum	Mídias de armazenamento	Controlar mídias removíveis, criptografia, inventário e descarte.	Registro de mídia e bloqueios.
B.3.21	Comum	Descarte seguro ou reutilização de equipamentos	Sanitizar ativos antes de descarte, manutenção ou reutilização.	Termo de sanitização/descarte
B.3.22	Comum	Dispositivos endpoint do usuário	Proteger notebooks, estações e dispositivos móveis.	EDR/antivírus, MDI criptografia.
B.3.23	Comum	Autenticação segura	MFA, senhas robustas, tokens, cofre de credenciais e segregação.	Política de autenticação e log
B.3.24	Comum	Backup das informações	Executar backups, testes de restauração e retenção compatível.	Plano de backup, testes e relatórios.
B.3.25	Comum	Log	Registrar eventos relevantes, proteger logs e monitorar anomalias.	SIEM, trilhas de auditoria e alertas.

B.3.26	Comum	Uso de criptografia	Criptografar dados em trânsito e em repouso quando aplicável.	Inventário criptográfico e TLS
B.3.27	Comum	Ciclo de vida de desenvolvimento seguro	Integrar privacidade e segurança ao SDLC.	Requisitos, code review, SAST/DAST
B.3.28	Comum	Requisitos de segurança da aplicação	Definir requisitos de autenticação, autorização, logs, validação e proteção de dados.	Backlog, user stories e testes.
B.3.29	Comum	Princípios de arquitetura e engenharia seguras	Usar segmentação, defesa em profundidade, segregação e hardening.	Arquitetura, diagramas e revisões
B.3.30	Comum	Desenvolvimento terceirizado	Controlar fornecedores de desenvolvimento e entrega de código.	Contrato, revisão de código e aceite seguro.
B.3.31	Comum	Informações de teste	Evitar dados pessoais reais em testes; mascarar, anonimizar ou sintetizar.	Base mascarada, procedimento e evidência.

12. Controles para Controladores de Dados Pessoais

Esta seção aplica-se aos tratamentos em que a 1 IT determina as finalidades e meios essenciais de tratamento, inclusive em processos administrativos, comerciais, operacionais próprios, atendimento, gestão de usuários e situações em que assuma controle sobre dados pessoais. Em cada tratamento, a classificação deve ser confirmada no ROPA.

12.1 B.1.2 - Condições para coleta e tratamento

B.1.2.2 - Identificação e documentação do propósito

Documentar finalidade, compatibilidade com o negócio e limites de uso antes de iniciar o tratamento.

- Evidência mínima: ROPA, matriz finalidade/base legal, especificação funcional.

B.1.2.3 - Identificação de bases legais

Registrar a hipótese legal de cada operação de tratamento e sua justificativa.

- Evidência mínima: Matriz de bases legais, parecer jurídico quando necessário.

B.1.2.4 - Quando e como obter consentimento

Usar consentimento apenas quando adequado; garantir destaque, granularidade e possibilidade de revogação.

- Evidência mínima: Termo de consentimento, tela de aceite, registro de origem.

B.1.2.5 - Obtenção e registro do consentimento

Manter evidência de quem consentiu, quando, para que finalidade, por qual canal e versão do texto.

- Evidência mínima: Log de consentimento e histórico de versão.

B.1.2.6 - Avaliação de impacto de privacidade

Realizar AIPD/RIPD para alto risco, larga escala, dados sensíveis, decisão automatizada ou mudanças relevantes.

- Evidência mínima: Relatório de impacto, plano de mitigação e aprovação.

B.1.2.7 - Contratos com operadores de DP

Contratar operadores com cláusulas de instrução, segurança, sigilo, suboperadores, incidente e devolução/descarte.

- Evidência mínima: Contrato, DPA, due diligence, SLA de incidente.

B.1.2.8 - Controlador conjunto de DP

Definir responsabilidades entre controladores quando houver decisão conjunta sobre finalidades e meios.

- Evidência mínima: Acordo de controladoria conjunta e matriz de responsabilidades.

B.1.2.9 - Registros relacionados ao tratamento de DP

Manter registros completos e auditáveis das operações de tratamento.

- Evidência mínima: ROPA, logs, evidências de tratamento e revisão.

12.2 B.1.3 - Obrigações para com os titulares de dados pessoais

B.1.3.2 - Obrigações perante titulares

Mapear e cumprir direitos de titulares conforme LGPD.

- Evidência mínima: Procedimento de direitos, SLA e registros de atendimento.

B.1.3.3 - Informações para titulares

Definir conteúdo mínimo de transparência, incluindo finalidade, base legal, compartilhamento, retenção e contato do DPO.

- Evidência mínima: Aviso de privacidade e respostas-padrão.

B.1.3.4 - Fornecimento de informações aos titulares

Disponibilizar informações claras, acessíveis, atualizadas e em linguagem adequada.

- Evidência mínima: Portal/canal LGPD, FAQ, política publicada.

B.1.3.5 - Modificar ou retirar consentimento

Disponibilizar mecanismo para retirada de consentimento e atualização de preferências.

- Evidência mínima: Registro de revogação e bloqueio de uso.

B.1.3.6 - Oposição ao tratamento

Permitir oposição a tratamento irregular ou baseado em hipóteses que admitam contestação.

- Evidência mínima: Fluxo de objeção, decisão fundamentada e resposta.

B.1.3.7 - Acesso, correção ou exclusão

Atender pedidos de confirmação, acesso, correção, anonimização, bloqueio, eliminação e portabilidade quando cabível.

- Evidência mínima: Protocolo, evidências de validação de identidade e resposta.

B.1.3.8 - Informar terceiros

Comunicar correções, eliminações ou restrições a terceiros com quem os dados foram compartilhados quando cabível.

- Evidência mínima: Registro de destinatários e comunicações.

B.1.3.9 - Cópia de DP tratados

Fornecer cópia ou extrato dos dados pessoais em formato seguro e adequado.

- Evidência mínima: Arquivo de resposta, trilha de entrega e comprovante.

B.1.3.10 - Tratamento de solicitações

Registrar, triagem, validar identidade, classificar, responder e reter evidência das solicitações.

- Evidência mínima: Sistema de tickets LGPD e SLA.

B.1.3.11 - Tomada de decisão automatizada

Mapear decisões automatizadas, critérios, revisão humana e explicabilidade quando aplicável.

- Evidência mínima: Inventário de algoritmos/regras, logs e revisão.

12.3 B.1.4 - Privacidade por design e por default

B.1.4.2 - Limitação da coleta

Coletar somente dados necessários à finalidade declarada.

- Evidência mínima: Revisão de campos, minimização de API e formulários.

B.1.4.3 - Limitação do tratamento

Usar dados apenas nas finalidades autorizadas e compatíveis.

- Evidência mínima: Controle de finalidade, segregação de bases e logs.

B.1.4.4 - Precisão e qualidade

Manter dados exatos, completos e atualizados quando necessário.

- Evidência mínima: Validações, correções e trilhas de atualização.

B.1.4.5 - Objetivos de minimização de DP

Definir metas para reduzir volume, exposição e retenção de dados pessoais.

- Evidência mínima: Indicadores de minimização e revisão de cadastros.

B.1.4.6 - Desidentificação e exclusão ao final do tratamento

Anonimizar, pseudonimizar ou eliminar dados ao fim da finalidade e prazo de retenção.

- Evidência mínima: Rotina de descarte e evidência técnica.

B.1.4.7 - Arquivos temporários

Controlar, expirar e eliminar arquivos temporários, caches, exports e bases de teste.

- Evidência mínima: Política de temporários, varreduras e logs de limpeza.

B.1.4.8 - Retenção

Definir prazos por base legal, contrato, regulação e necessidade operacional.

- Evidência mínima: Tabela de temporalidade e revisão periódica.

B.1.4.9 - Descarte

Executar descarte seguro e documentado de dados e mídias.

- Evidência mínima: Certificado/registro de descarte e aprovação.

B.1.4.10 - Controles de transmissão de DP

Proteger dados em trânsito por criptografia, autenticação, integridade e canal autorizado.

- Evidência mínima: TLS, VPN, chaves, logs e testes.

B.1.5.2 - Bases para transferências entre jurisdições

Avaliar base legal e salvaguardas para transferência internacional.

- Evidência mínima: Registro de transferência e cláusulas contratuais.

12.4 B.1.5 - Compartilhamento, transferência e divulgação

B.1.5.3 - Países/organizações de destino

Documentar países, provedores e organizações internacionais que recebem DP.

- Evidência mínima: Inventário de fornecedores e localidade de dados.

B.1.5.4 - Registros de transferência de DP

Manter registros de transferências, finalidade, destinatário, base e salvaguarda.

- Evidência mínima: Registro de transferência e revisão.

B.1.5.5 - Registros de divulgação a terceiros

Registrar divulgações pontuais, obrigatórias ou contratuais a terceiros.

- Evidência mínima: Log de divulgação e autorização.

13. Controles para Operadores de Dados Pessoais

Esta seção aplica-se aos tratamentos em que a 1 IT atua sob instruções de um controlador, realizando operações técnicas, operacionais ou de suporte em nome do cliente. Nessa hipótese, a 1 IT deve observar estritamente o contrato, o DPA, as instruções documentadas, os requisitos de segurança e os prazos de comunicação.

13.1 B.2.2 - Condições para coleta e tratamento como operadora

B.2.2.2 - Acordo com o cliente

Tratar DP conforme contrato e instruções documentadas do controlador.

- Evidência mínima: Contrato, ordem de serviço, matriz de instruções.

B.2.2.3 - Propósitos da organização

Não usar dados do cliente para finalidades próprias incompatíveis.

- Evidência mínima: Política interna e segregação lógica.

B.2.2.4 - Uso para marketing e propaganda

Vedado uso de DP tratados como operadora para marketing próprio sem autorização válida.

- Evidência mínima: Cláusula contratual e bloqueios de uso.

B.2.2.5 - Instruções infratoras

Alertar o controlador quando instrução aparentar violar lei, contrato ou política.

- Evidência mínima: Registro de alerta e decisão do cliente.

B.2.2.6 - Obrigações do cliente

Definir obrigações do controlador em instruções, bases legais, titulares e informações necessárias.

- Evidência mínima: DPA, matriz de responsabilidades e SLA.

B.2.2.7 - Registros relativos ao tratamento

Manter registros das operações executadas em nome do controlador.

- Evidência mínima: Logs, ROPA como operadora e evidências.

13.2 B.2.3 - Obrigações para com os titulares

B.2.3.2 - Compliance com obrigações perante titulares

Apoiar o controlador no atendimento aos direitos de titulares dentro de prazo contratual.

- Evidência mínima: Ticket de apoio, logs e retorno ao controlador.

13.3 B.2.4 - Privacidade por design e por default como operadora

B.2.4.2 - Arquivos temporários

Remover arquivos temporários criados em suporte, migração, teste ou incidente.

- Evidência mínima: Registro de limpeza e controles de acesso.

B.2.4.3 - Devolução, transferência ou descarte de DP

Ao término do contrato, devolver, transferir, bloquear ou descartar dados conforme instrução.

- Evidência mínima: Termo de devolução/descarte e evidências.

B.2.4.4 - Controles de transmissão de DP

Utilizar canais seguros para troca de dados do controlador.

- Evidência mínima: TLS, SFTP, VPN, criptografia e logs.

13.4 B.2.5 - Compartilhamento, transferência e divulgação como operadora

B.2.5.2 - Fundamentação para transferência entre jurisdições

Transferir dados apenas mediante autorização/instrução e salvaguardas.

- Evidência mínima: Contrato, localidade de hospedagem e avaliação.

B.2.5.3 - Países/organizações de destino

Informar ao controlador a localidade de processamento e suboperadores.

- Evidência mínima: Lista de suboperadores e regiões de cloud.

B.2.5.4 - Registros de divulgações a terceiros

Manter registro de divulgações autorizadas ou obrigatórias.

- Evidência mínima: Log de divulgação, base e aprovador.

B.2.5.5 - Notificação de solicitações de divulgação de DP

Informar ao controlador solicitações legais/administrativas quando permitido.

- Evidência mínima: Registro de solicitação e comunicação.

B.2.5.6 - Divulgações legalmente obrigatórias

Cumprir obrigação legal preservando sigilo e mínima divulgação.

- Evidência mínima: Parecer jurídico e protocolo.

B.2.5.7 - Divulgação de subcontratados

Disponibilizar lista de suboperadores e serviços envolvidos.

- Evidência mínima: Catálogo de suboperadores.

B.2.5.8 - Envolvimento de subcontratado

Obter autorização e impor obrigações equivalentes ao suboperador.

- Evidência mínima: Contrato com suboperador e due diligence.

B.2.5.9 - Troca de subcontratado

Comunicar troca e permitir objeção quando contratualmente previsto.

- Evidência mínima: Notificação, avaliação e aceite.

14. Controles Comuns para Controladores e Operadores

Os controles comuns devem ser aplicados independentemente do papel da 1 IT, pois representam a base mínima de segurança, governança e evidência para qualquer tratamento de dados pessoais.

14.1 Governança, classificação e transferência

B.3.3 - Políticas de segurança da informação

Manter políticas integradas de SI e privacidade.

- Evidência mínima: PSI, política de privacidade, revisão anual.

B.3.4 - Papéis e responsabilidades em segurança da informação

Definir responsabilidades de SI relacionadas a DP.

- Evidência mínima: Matriz RACI, nomeações e descrições.

B.3.5 - Classificação da informação

Classificar dados pessoais por criticidade, sensibilidade e restrição.

- Evidência mínima: Matriz de classificação e etiquetas.

B.3.6 - Rotulagem da informação

Aplicar rótulos em documentos, bases, exports e repositórios.

- Evidência mínima: Etiquetas e configuração DLP.

B.3.7 - Transferência de informação

Formalizar meios seguros de transferência interna e externa.

- Evidência mínima: Procedimento de transferência segura.

14.2 Identidade, acesso e fornecedores

B.3.8 - Gestão de identidade

Controlar identidades humanas, técnicas, administrativas e de serviço.

- Evidência mínima: IAM, MFA, revisão de contas.

B.3.9 - Direitos de acesso

Aplicar menor privilégio, segregação, aprovação e revisão periódica.

- Evidência mínima: Matriz de acesso, logs, recertificação.

B.3.10 - Segurança em contratos de fornecedores

Incluir requisitos de SI, privacidade, auditoria, incidente e subcontratação.

- Evidência mínima: Cláusulas, DPA e due diligence.

14.3 Incidentes, requisitos e registros

B.3.11 - Planejamento e preparação para incidentes

Definir playbooks, equipe, canais, critérios e simulações.

- Evidência mínima: Plano de resposta e exercícios.

B.3.12 - Resposta a incidentes de segurança

Detectar, conter, erradicar, recuperar, comunicar e registrar incidentes.

- Evidência mínima: Registro de incidente e lições aprendidas.

B.3.13 - Requisitos legais, estatutários, regulatórios e contratuais

Manter matriz de requisitos aplicáveis à privacidade e ao negócio.

- Evidência mínima: Matriz legal e revisão.

B.3.14 - Proteção de registros

Proteger registros contra perda, alteração indevida e acesso não autorizado.

- Evidência mínima: Controle de retenção, backup e assinatura.

14.4 Auditoria, conformidade, treinamento e sigilo

B.3.15 - Análise crítica independente da segurança

Realizar avaliações independentes, auditorias e testes.

- Evidência mínima: Relatórios de auditoria/pentest.

B.3.16 - Compliance com políticas, regras e normas

Monitorar adesão às políticas e tratar exceções.

- Evidência mínima: Checklist de conformidade e ações.

B.3.17 - Conscientização, educação e treinamento

Treinar colaboradores e terceiros por perfil de risco.

- Evidência mínima: Trilha EAD, listas e certificados.

B.3.18 - Acordos de confidencialidade ou não divulgação

Formalizar NDA/termo de sigilo para acesso a DP.

- Evidência mínima: Termos assinados e controle.

14.5 Controles físicos, endpoints e mídias

B.3.19 - Mesa limpa e tela limpa

Reduzir exposição física e visual de DP.

- Evidência mínima: Política e inspeções.

B.3.20 - Mídias de armazenamento

Controlar mídias removíveis, criptografia, inventário e descarte.

- Evidência mínima: Registro de mídia e bloqueios.

B.3.21 - Descarte seguro ou reutilização de equipamentos

Sanitizar ativos antes de descarte, manutenção ou reutilização.

- Evidência mínima: Termo de sanitização/descarte.

B.3.22 - Dispositivos endpoint do usuário

Proteger notebooks, estações e dispositivos móveis.

- Evidência mínima: EDR/antivírus, MDM, criptografia.

14.6 Autenticação, backup, logs e criptografia

B.3.23 - Autenticação segura

MFA, senhas robustas, tokens, cofre de credenciais e segregação.

- Evidência mínima: Política de autenticação e logs.

B.3.24 - Backup das informações

Executar backups, testes de restauração e retenção compatível.

- Evidência mínima: Plano de backup, testes e relatórios.

B.3.25 - Log

Registrar eventos relevantes, proteger logs e monitorar anomalias.

- Evidência mínima: SIEM, trilhas de auditoria e alertas.

B.3.26 - Uso de criptografia

Criptografar dados em trânsito e em repouso quando aplicável.

- Evidência mínima: Inventário criptográfico e TLS.

14.7 Desenvolvimento seguro, aplicações, arquitetura e testes

B.3.27 - Ciclo de vida de desenvolvimento seguro

Integrar privacidade e segurança ao SDLC.

- Evidência mínima: Requisitos, code review, SAST/DAST.

B.3.28 - Requisitos de segurança da aplicação

Definir requisitos de autenticação, autorização, logs, validação e proteção de dados.

- Evidência mínima: Backlog, user stories e testes.

B.3.29 - Princípios de arquitetura e engenharia seguras

Usar segmentação, defesa em profundidade, segregação e hardening.

- Evidência mínima: Arquitetura, diagramas e revisão.

B.3.30 - Desenvolvimento terceirizado

Controlar fornecedores de desenvolvimento e entrega de código.

- Evidência mínima: Contrato, revisão de código e aceite seguro.

B.3.31 - Informações de teste

Evitar dados pessoais reais em testes; mascarar, anonimizar ou sintetizar.

- Evidência mínima: Base mascarada, procedimento e evidência.

15. Aplicação Operacional da LGPD na 1 IT

15.1 Princípios da LGPD aplicados aos processos

Princípio	Aplicação prática	Evidência
Finalidade	Todo tratamento deve possuir finalidade específica, legítima, documentada e compatível com o serviço.	ROPA e matriz de finalidade.
Adequação	Dados usados apenas de forma compatível com o contexto informado/contratado.	Revisão de processos e contratos.
Necessidade	Coleta mínima e campos obrigatórios justificados.	Revisão de formulários, APIs e cadastros.
Livre acesso	Canal para consulta e confirmação do tratamento.	Canal LGPD e registros.
Qualidade dos dados	Correção e atualização quando necessário à finalidade.	Trilhas de alteração e validação.
Transparência	Informações claras sobre tratamento, compartilhamento, retenção e DPO.	Avisos e política de privacidade.
Segurança	Controles técnicos e administrativos proporcionais ao risco.	IAM, logs, criptografia, backup, SIEM.
Prevenção	Riscos avaliados antes da implantação e mitigados continuamente.	AIPD/RIPD e plano de ação.
Não discriminação	Proibição de tratamento abusivo ou discriminatório.	Revisão de regras automatizadas.
Responsabilização	Demonstração de medidas eficazes de conformidade.	Auditorias, atas, indicadores e evidências.

15.2 Mapeamento LGPD x MA-004

Artigo	Tema	Aplicação	Evidência
Art. 1º e 3º	Âmbito e aplicação territorial	Aplicar LGPD a tratamentos realizados pela 1 IT ou relacionados a oferta/serviço no Brasil.	Escopo do SGPI, contratos e mapa de dados.
Art. 5º	Conceitos legais	Padronizar controlador, operador, titular, dado pessoal, dado sensível, anonimização e tratamento.	Glossário e treinamentos.
Art. 6º	Princípios	Operacionalizar finalidade, adequação, necessidade, transparência, segurança, prevenção e accountability.	Matriz de princípios e evidências.
Art. 7º	Bases legais para dados pessoais	Definir base legal por finalidade e macroprocesso.	Matriz de bases legais.
Art. 8º	Consentimento	Controlar consentimento apenas quando usado como base legal.	Registro de consentimento/revogação.
Art. 9º	Transparência ao titular	Disponibilizar informações claras sobre tratamento.	Avisos e política de privacidade.
Art. 10	Legítimo interesse	Realizar teste de balanceamento quando aplicável.	LIA/avaliação de legítimo interesse.
Art. 11	Dados pessoais sensíveis	Evitar sensíveis no processo fim; controlar RH, biometria ou situações excepcionais.	ROPA e AIPD.
Art. 12 e 13	Anonimização e estudos	Validar anonimização e evitar reversão quando usada.	Procedimento de anonimização.
Art. 14	Crianças e adolescentes	Não tratar no processo fim salvo exceção	Triagem de tratamento e bloqueio.

		justificada; reforçar cuidado em canais e RH.	
Art. 15 e 16	Término, conservação e eliminação	Definir retenção por finalidade e descarte seguro.	Tabela de temporalidade.
Art. 17 a 22	Direitos dos titulares	Atender confirmação, acesso, correção, anonimização, eliminação, portabilidade, informação e revisão.	Canal LGPD e protocolo.
Art. 20	Decisão automatizada	Mapear e permitir revisão quando houver decisão baseada exclusivamente em tratamento automatizado.	Inventário e procedimento.
Art. 23 a 30	Poder público e compartilhamento	Controlar compartilhamentos com órgãos e clientes públicos quando houver.	Registro de compartilhamento.
Art. 31 a 36	Transferência internacional	Registrar países, bases e salvaguardas quando houver cloud ou suboperador internacional.	Matriz de transferência.
Art. 37	Registro das operações	Manter ROPA atualizado.	ROPA.
Art. 38	Relatório de impacto	Elaborar RIPD/AIPD quando necessário ou requisitado.	RIPD/AIPD.
Art. 39	Operador	Operador deve realizar tratamento segundo instruções do controlador.	DPA e matriz de instruções.
Art. 40	Padrões de interoperabilidade e segurança	Aplicar padrões técnicos quando definidos pela ANPD ou setor.	Arquitetura e requisitos técnicos.
Art. 41	Encarregado	Indicar encarregado e divulgar	Nomeação e canal do DPO.

		identidade/contato conforme norma da ANPD.	
Art. 42 a 45	Responsabilidade e ressarcimento	Prevenir danos e demonstrar controles.	Gestão de riscos, auditorias, incidentes.
Art. 46 a 49	Segurança e boas práticas	Aplicar medidas técnicas/administrativas e segurança desde a concepção.	PSI, SDLC, logs, backup, criptografia.
Art. 48	Comunicação de incidente	Comunicar ANPD e titulares quando houver risco ou dano relevante.	Playbook CIS e registro de incidente.
Art. 50	Governança em privacidade	Implementar programa de governança, políticas, auditorias, treinamento e mitigação de riscos.	SGPI, comitê, indicadores.
Art. 52 a 54	Sanções administrativas	Gerenciar riscos de sanções e evidenciar boa-fé, cooperação e diligência.	Dossiê de conformidade e plano de ação.

15.3 Matriz de bases legais por macroprocesso

Macroprocesso	Papel provável	Dados típicos	Base legal principal	O
Registro de contratos de veículos	Operadora ou controladora, conforme contrato e credenciamento	Identificação, CPF, contrato, veículo, garantia, representante, logs e evidências.	Execução de contrato, obrigação legal/regulatória, exercício regular de direitos ou legítimo interesse, conforme caso.	Co pa cc RC
Cadastro de clientes e parceiros	Controladora	Representantes, contatos, documentos, credenciais e comunicações.	Execução de contrato, legítimo interesse e cumprimento de obrigação legal.	Us m e pe
Gestão de usuários e	Controladora/operadora	Nome, e-mail, CPF quando	Legítimo interesse, execução de contrato	M re

acessos		necessário, perfil, logs, IP, MFA.	e segurança/prevenção à fraude.	e
Suporte técnico e operacional	Operadora ou controladora	Dados do solicitante, ticket, logs, evidências e prints.	Execução de contrato, legítimo interesse e exercício regular de direitos.	Ev ex er pr
Atendimento LGPD	Controladora	Nome, contato, documento para validação, demanda, resposta e protocolo.	Cumprimento de obrigação legal.	Va id fo pr
Incidentes e segurança	Controladora/operadora	Logs, IPs, usuários, eventos, evidências técnicas e dados afetados.	Cumprimento de obrigação legal, legítimo interesse e segurança.	Re in nc ar er
RH e DP	Controladora	Dados cadastrais, trabalhistas, benefícios, folha, saúde ocupacional quando aplicável.	Obrigação legal/regulatória, contrato e tutela da saúde quando aplicável.	Co re pa se
Marketing institucional B2B	Controladora	Contato profissional, cargo, organização, histórico comercial.	Legítimo interesse ou consentimento quando aplicável.	Oj re or
Fornecedores	Controladora	Representantes, contatos, contratos, dados bancários e fiscais.	Execução de contrato, obrigação legal e legítimo interesse.	Co re ac

15.4 Tratamentos de alto risco e gatilhos de AIPD/RIPD

- Tratamento em larga escala de dados pessoais vinculados a contratos ou operações financeiras.
- Uso de dados sensíveis ou de crianças/adolescentes, ainda que incidental.
- Decisão automatizada com efeito relevante para titular.
- Compartilhamento amplo com terceiros, órgãos, suboperadores ou transferência internacional.
- Mudança relevante de arquitetura, cloud, banco de dados, API, finalidade, retenção ou base legal.
- Incidente de segurança relevante, recorrente ou com risco a direitos fundamentais.
- Uso de tecnologia nova ou integração com risco elevado de rastreamento, perfilamento, fraude ou exposição.

16. Procedimentos Operacionais de Privacidade

16.1 Procedimento de ROPA e Mapa de Dados

Passo	Atividade	Responsável	Evidência
1	Identificar processo, área, sistemas, dados, titulares e finalidade.	Gestor do processo	Ficha de tratamento.
2	Classificar papel da 1 IT: controladora, operadora ou conjunta.	DPO + Jurídico	Campo do ROPA.
3	Validar base legal e necessidade de transparência.	Jurídico + DPO	Matriz de base legal.
4	Mapear compartilhamentos, fornecedores, localidade, retenção e descarte.	Gestor + TI/SI	Mapa de dados.
5	Avaliar riscos, controles existentes e necessidade de AIPD/RIPD.	DPO + SI	Matriz de riscos.
6	Aprovar, publicar e revisar periodicamente.	Comitê	Ata e versão do ROPA.

16.2 Procedimento de atendimento aos titulares

Etapa	Controle mínimo

Recepção	Registrar solicitação com protocolo, data, canal, solicitante, tipo de direito e processo relacionado.
Validação de identidade	Aplicar validação proporcional, evitando coleta excessiva de documentos.
Classificação	Classificar direito solicitado: confirmação, acesso, correção, anonimização, eliminação, portabilidade, informação, revogação, oposição ou revisão.
Análise	Verificar papel da 1 IT, base legal, dados disponíveis, impedimentos legais, sigilo de terceiros e necessidade de consultar controlador.
Resposta	Responder em linguagem clara, segura e rastreável, dentro do prazo legal/contratual.
Execução	Aplicar correção, bloqueio, anonimização, eliminação, revogação ou encaminhamento quando cabível.
Encerramento	Registrar resposta, evidências, anexos, responsável e data de conclusão.

16.3 Procedimento de incidentes de segurança com dados pessoais

Fase	Ação	Responsáveis
Detecção	Identificar evento por alerta, usuário, fornecedor, cliente, log, monitoramento ou denúncia.	TI/SI, usuários, fornecedor.
Triagem	Verificar se envolve dados pessoais, sistemas, titulares, volume, sensibilidade e risco.	TI/SI + DPO.
Contenção	Bloquear acesso, revogar credenciais, isolar sistema, suspender integração, preservar evidência.	TI/SI.
Avaliação de risco	Avaliar risco ou dano relevante, categorias de dados, titulares, escala, mitigação e obrigação de comunicação.	DPO + Jurídico + SI.
Comunicação	Quando aplicável, comunicar ANPD e titulares no prazo legal, e clientes/controladores conforme contrato.	DPO + Jurídico + Alta Direção.

Recuperação	Restaurar serviço, corrigir vulnerabilidade, monitorar recorrência e validar integridade.	TI/SI + Operações.
Lições aprendidas	Atualizar riscos, controles, treinamento, contrato, playbook e plano de ação.	Comitê.

Prazo regulatório: Para incidentes com risco ou dano relevante, a comunicação à ANPD e aos titulares deve observar o prazo regulatório aplicável. O procedimento interno da 1 IT deve exigir triagem imediata e escalonamento ao DPO/Comitê, permitindo decisão tempestiva e comunicação preliminar quando as informações completas ainda não estiverem disponíveis.

16.4 Procedimento de fornecedores, operadores e suboperadores

Fase	Atividade
Classificação	Determinar se o fornecedor trata DP, qual papel exerce, criticidade, dados, sistemas e acesso.
Due diligence	Avaliar segurança, privacidade, certificações, localização de dados, suboperadores, incidentes e continuidade.
Contrato/DPA	Incluir instruções, confidencialidade, controles, subcontratação, incidente, auditoria, retenção e descarte.
Homologação técnica	Validar MFA, acesso mínimo, criptografia, logs, segregação, backup, suporte e integração.
Monitoramento	Revisar performance, incidentes, mudanças de suboperadores, certificados e conformidade.
Encerramento	Executar devolução, transferência, bloqueio ou descarte de DP com evidência.

16.5 Procedimento de retenção, descarte e anonimização

Etapa	Controle
Definição do prazo	Definir prazo por base legal, finalidade, contrato, regulação, prescrição e necessidade operacional.
Bloqueio/restrição	Ao fim da finalidade, restringir acesso quando a guarda for necessária apenas por obrigação legal ou defesa.

Descarte lógico	Eliminar com método seguro, logs de execução, aprovação e validação.
Descarte físico	Sanitizar mídias, destruir documentos e registrar certificado/termo.
Anonimização	Aplicar técnica irreversível ou com risco razoavelmente controlado de reidentificação.
Backups	Gerenciar expurgo conforme ciclo de backup, sem restauração indevida de dados eliminados.

16.6 Procedimento de desenvolvimento seguro e privacidade por design

Fase SDLC	Requisito de privacidade
Ideação	Identificar dados pessoais, finalidade, base legal, titulares, risco e necessidade de AIPD.
Requisitos	Incluir minimização, controle de acesso, logs, retenção, transparência, exportação segura, segregação e direitos de titulares.
Arquitetura	Aplicar segurança por camadas, criptografia, segregação de ambientes, gestão de segredos e isolamento.
Desenvolvimento	Evitar dados reais em teste; validar entradas; impedir exposição em logs; revisar permissões e APIs.
Testes	Executar SAST/DAST, teste de autorização, teste de sessão, revisão de logs e teste de mascaramento.
Deploy	Avaliar mudança, aprovar risco residual, revisar ROPA e atualizar documentação.
Operação	Monitorar anomalias, vulnerabilidades, incidentes, acessos e desempenho de controles.

17. Anexos Operacionais e Modelos de Registro

17.1 Modelo de ROPA / Registro de Operações de Tratamento

Campo	Preenchimento esperado
ID do tratamento	Código único.
Nome do processo	Ex.: Registro de contratos de veículos.

Área responsável	Gestor e área.
Papel da 1 IT	Controladora, operadora ou conjunta.
Finalidade	Descrição objetiva da finalidade.
Base legal	Hipótese LGPD e justificativa.
Titulares	Categorias de titulares.
Dados pessoais	Categorias de dados tratados.
Dados sensíveis	Indicar se há, justificar e controlar.
Origem dos dados	Titular, cliente, integração, órgão, fornecedor etc.
Operações	Coleta, validação, armazenamento, transmissão, consulta, descarte etc.
Sistemas/repositórios	Aplicação, banco, storage, log, e-mail, ticket.
Compartilhamentos	Destinatários e fundamento.
Transferência internacional	País, fornecedor, salvaguarda e contrato.
Retenção	Prazo, base e gatilho de eliminação.
Controles de segurança	Acesso, criptografia, logs, backup, mascaramento.
Riscos	Risco inerente/residual e plano de tratamento.
AIPD/RIPD	Obrigatório? Sim/Não. Justificativa.
Evidências	Documentos e registros associados.

17.2 Modelo de AIPD/RIPD

Seção	Conteúdo mínimo
1. Identificação	Processo, área, responsável, data, versão e gatilho da avaliação.
2. Descrição do tratamento	Finalidade, dados, titulares, sistemas, fluxo, origem, destino e tecnologia.
3. Necessidade e proporcionalidade	Justificativa de coleta, minimização, base legal e alternativas menos invasivas.
4. Avaliação de riscos	Ameaças, vulnerabilidades, probabilidade, impacto aos titulares e risco à organização.
5. Controles existentes	Controles técnicos, administrativos, contratuais e organizacionais.

6. Plano de mitigação	Ações, responsáveis, prazos, evidências e risco residual.
7. Consulta e aprovação	DPO, jurídico, SI, gestor do processo, alta direção quando necessário.
8. Revisão	Periodicidade, gatilhos de revisão e histórico de versões.

17.3 Formulário de solicitação de titular

Campo	Descrição
Protocolo	Número único da solicitação.
Data e canal	Data de recebimento e canal utilizado.
Solicitante	Nome e dados mínimos de contato.
Validação de identidade	Método usado e evidência proporcional.
Direito solicitado	Confirmação, acesso, correção, anonimização, bloqueio, eliminação, portabilidade, revogação, oposição, revisão ou informação.
Processo relacionado	Sistema, contrato, cliente ou área relacionada.
Análise	Base legal, papel da 1 IT, restrições, terceiros e decisão.
Resposta	Resumo da resposta enviada e data.
Execução	Ação tomada: correção, exclusão, bloqueio etc.
Encerramento	Responsável, data, evidências e retenção.

17.4 Registro de incidente de segurança com DP

Campo	Descrição
ID do incidente	Código único.
Data/hora de detecção	Quando o evento foi identificado.
Data/hora de conhecimento	Quando a 1 IT tomou conhecimento suficiente para triagem.
Origem do alerta	Monitoramento, usuário, fornecedor, cliente, ANPD, titular etc.

Descrição	Resumo técnico e executivo.
Dados afetados	Categorias de dados pessoais e sensíveis, se houver.
Titulares afetados	Quantidade estimada, grupos vulneráveis e identificação possível.
Risco ou dano relevante	Avaliação fundamentada.
Medidas de contenção	Ações imediatas.
Comunicação	ANPD, titulares, clientes/controladores, suboperadores e autoridades, se aplicável.
Evidências	Logs, prints, tickets, relatórios, hashes e cadeia de custódia.
Lições aprendidas	Causa raiz, ação corretiva e melhoria.
Retenção	Registro mantido por no mínimo 5 anos quando envolver DP, ou maior prazo aplicável.

17.5 Checklist de contratação de operador/suboperador

Item	Pergunta de verificação	Evidência
Papel	O fornecedor trata dados pessoais? Em qual papel?	Classificação e ROPA.
Dados	Quais dados, titulares, sistemas e finalidades estão envolvidos?	Escopo do serviço.
Localidade	Onde os dados serão armazenados/processados?	Região de cloud/datacenter.
Suboperadores	Há suboperadores? Foram informados e aprovados?	Lista e contratos.
Segurança	Há MFA, criptografia, logs, backup, segregação e gestão de vulnerabilidades?	Políticas e evidências.
Incidentes	O fornecedor notifica incidente sem demora injustificada?	Cláusula e SLA.
Retenção/descarte	Há procedimento de devolução, eliminação e comprovação?	Termo de descarte.
Auditoria	Há direito de auditoria ou fornecimento de evidências?	Cláusula contratual.

Confidencialidade	Equipe do fornecedor possui dever de sigilo?	NDA/contrato.
Encerramento	Há plano de saída e portabilidade?	Plano de encerramento.

17.6 Tabela de temporalidade inicial

Categoria	Prazo inicial recomendado	Observação
Dados de contratos e registros de veículos	Conforme obrigação legal/regulatória, contrato e prescrição aplicável.	Validar com jurídico e requisitos setoriais.
Logs de acesso e auditoria	Conforme requisitos de segurança, contrato e necessidade de investigação.	Definir retenção mínima compatível com risco.
Solicitações LGPD	Prazo necessário para comprovação do atendimento e exercício regular de direitos.	Acesso restrito ao DPO/Jurídico.
Incidentes de segurança com DP	Mínimo de 5 anos quando aplicável a incidente com dados pessoais.	Observar regulamento de comunicação de incidentes.
Dados de candidatos	Prazo informado no aviso de recrutamento ou até fim da finalidade.	Eliminar ou anonimizar após prazo.
Dados trabalhistas e previdenciários	Conforme legislação trabalhista, previdenciária, fiscal e prescrição.	Controle com RH/Jurídico.
Fornecedores e contratos	Prazo contratual, fiscal e prescricional aplicável.	Separar dados de representantes.
Backups	Ciclo técnico de backup definido e documentado.	Evitar restauração indevida de dados eliminados.

17.7 Checklist de auditoria interna do SGPI

Item	Tema	Evidência a verificar
0.1	Introdução e justificativa do SGPI	Política, ROPA, AIPD/RIPD, matriz de riscos, indicadores.

0.2	Compatibilidade com outros sistemas de gestão	Mapa de integração, atas do comitê, auditorias integradas.
1	Escopo	Escopo formal, limites, processos e papéis.
2	Referência normativa	Lista de referências e controle documental.
3	Termos e definições	Glossário interno e treinamentos.
4.1	Entendendo a organização e seu contexto	Matriz de contexto e riscos.
4.2	Partes interessadas	Matriz de partes interessadas.
4.3	Escopo do SGPI	Declaração de escopo e mapa de processos.
4.4	Sistema de gestão da privacidade da informação	Manual, procedimentos e indicadores.
5.1	Liderança e comprometimento	Ata de aprovação, objetivos, recursos e análises críticas.
5.2	Política de privacidade	Política publicada e comunicada.
5.3	Papéis, responsabilidades e autoridades	Matriz RACI, nomeações e descrições de função.
6.1.1	Riscos e oportunidades - geral	Metodologia de riscos e plano de tratamento.
6.1.2	Avaliação de riscos de privacidade	Registro de riscos e AIPD/RIPD.
6.1.3	Tratamento de riscos de privacidade	Plano de tratamento e declaração de aplicabilidade.
6.2	Objetivos de privacidade	Indicadores e metas.
6.3	Planejamento de mudanças	Formulário de mudança e análise de impacto.
7.1	Recursos	Plano orçamentário e recursos aprovados.
7.2	Competência	Matriz de competência e registros de treinamento.
7.3	Conscientização	Campanhas, EAD e aceite de políticas.
7.4	Comunicação	Plano de comunicação.
7.5.1	Informação documentada - geral	Lista mestra de documentos.
7.5.2	Criação e atualização	Fluxo de controle documental.

7.5.3	Controle da informação documentada	Repositório controlado e trilhas de revisão.
8.1	Planejamento e controle operacional	POPs, logs e registros operacionais.
8.2	Avaliação de riscos de privacidade em operação	Registro de riscos atualizado.
8.3	Tratamento de riscos em operação	Plano de ação e evidências.
9.1	Monitoramento, medição, análise e avaliação	Painel de indicadores.
9.2.1	Auditoria interna - geral	Plano, checklist e relatório.
9.2.2	Programa de auditoria interna	Programa anual de auditoria.
9.3.1	Análise crítica - geral	Ata de análise crítica.
9.3.2	Entradas da análise crítica	Dossiê de entradas.
9.3.3	Resultados da análise crítica	Plano de ação aprovado.
10.1	Melhoria contínua	Backlog de melhorias e indicadores.
10.2	Não conformidade e ação corretiva	Formulário de NC e ação corretiva.

17.8 Declaração de aplicabilidade simplificada do SGPI

17.8 Declaração de aplicabilidade simplificada do SGPI

Item	Controle	Aplicabilidade	Decisão de tratamento	Evidência
B.1.2.2	Identificação e documentação do propósito	Aplicável conforme papel/processo	Implementar e evidenciar	ROPA, matriz finalidade/base legal, especificação funcional.
B.1.2.3	Identificação de bases legais	Aplicável conforme papel/processo	Implementar e evidenciar	Matriz de bases legais, parecer jurídico quando necessário.
B.1.2.4	Quando e como obter consentimento	Aplicável conforme papel/processo	Implementar e evidenciar	Termo de consentimento, tela de aceite, registro de origem.

B.1.2.5	Obtenção e registro do consentimento	Aplicável conforme papel/processo	Implementar e evidenciar	Log de consentimento e histórico de versão.
B.1.2.6	Avaliação de impacto de privacidade	Aplicável conforme papel/processo	Implementar e evidenciar	Relatório de impacto, plano de mitigação e aprovação.
B.1.2.7	Contratos com operadores de DP	Aplicável conforme papel/processo	Implementar e evidenciar	Contrato, DPA, due diligence, SLA de incidente.
B.1.2.8	Controlador conjunto de DP	Aplicável conforme papel/processo	Implementar e evidenciar	Acordo de controladoria conjunta e matriz de responsabilidades.
B.1.2.9	Registros relacionados ao tratamento de DP	Aplicável conforme papel/processo	Implementar e evidenciar	ROPA, logs, evidências de tratamento e revisão.
B.1.3.2	Obrigações perante titulares	Aplicável conforme papel/processo	Implementar e evidenciar	Procedimento de direitos, SLA e registros de atendimento.
B.1.3.3	Informações para titulares	Aplicável conforme papel/processo	Implementar e evidenciar	Aviso de privacidade e respostas-padrão.
B.1.3.4	Fornecimento de informações aos titulares	Aplicável conforme papel/processo	Implementar e evidenciar	Portal/canal LGPD, FAQ, política publicada.
B.1.3.5	Modificar ou retirar consentimento	Aplicável conforme papel/processo	Implementar e evidenciar	Registro de revogação e bloqueio de uso.
B.1.3.6	Oposição ao tratamento	Aplicável conforme papel/processo	Implementar e evidenciar	Fluxo de objeção, decisão fundamentada e resposta.
B.1.3.7	Acesso, correção ou exclusão	Aplicável conforme papel/processo	Implementar e evidenciar	Protocolo, evidências de validação de identidade e resposta.

B.1.3.8	Informar terceiros	Aplicável conforme papel/processo	Implementar e evidenciar	Registro de destinatários e comunicações.
B.1.3.9	Cópia de DP tratados	Aplicável conforme papel/processo	Implementar e evidenciar	Arquivo de resposta, trilha de entrega e comprovante.
B.1.3.10	Tratamento de solicitações	Aplicável conforme papel/processo	Implementar e evidenciar	Sistema de tickets LGPD e SLA.
B.1.3.11	Tomada de decisão automatizada	Aplicável conforme papel/processo	Implementar e evidenciar	Inventário de algoritmos/regras, logs e revisão.
B.1.4.2	Limitação da coleta	Aplicável conforme papel/processo	Implementar e evidenciar	Revisão de campos, minimização de API e formulários.
B.1.4.3	Limitação do tratamento	Aplicável conforme papel/processo	Implementar e evidenciar	Controle de finalidade, segregação de bases e logs.
B.1.4.4	Precisão e qualidade	Aplicável conforme papel/processo	Implementar e evidenciar	Validações, correções e trilhas de atualização.
B.1.4.5	Objetivos de minimização de DP	Aplicável conforme papel/processo	Implementar e evidenciar	Indicadores de minimização e revisão de cadastros.
B.1.4.6	Desidentificação e exclusão ao final do tratamento	Aplicável conforme papel/processo	Implementar e evidenciar	Rotina de descarte e evidência técnica.
B.1.4.7	Arquivos temporários	Aplicável conforme papel/processo	Implementar e evidenciar	Política de temporários, varreduras e logs de limpeza.
B.1.4.8	Retenção	Aplicável conforme papel/processo	Implementar e evidenciar	Tabela de temporalidade e revisão periódica.
B.1.4.9	Descarte	Aplicável conforme papel/processo	Implementar e evidenciar	Certificado/registro de descarte e aprovação.

B.1.4.10	Controles de transmissão de DP	Aplicável conforme papel/processo	Implementar e evidenciar	TLS, VPN, chaves, logs e testes.
B.1.5.2	Bases para transferências entre jurisdições	Aplicável conforme papel/processo	Implementar e evidenciar	Registro de transferência e cláusulas contratuais.
B.1.5.3	Países/organizações de destino	Aplicável conforme papel/processo	Implementar e evidenciar	Inventário de fornecedores e localidade de dados.
B.1.5.4	Registros de transferência de DP	Aplicável conforme papel/processo	Implementar e evidenciar	Registro de transferência e revisão.
B.1.5.5	Registros de divulgação a terceiros	Aplicável conforme papel/processo	Implementar e evidenciar	Log de divulgação e autorização.
B.2.2.2	Acordo com o cliente	Aplicável conforme papel/processo	Implementar e evidenciar	Contrato, ordem de serviço, matriz de instruções.
B.2.2.3	Propósitos da organização	Aplicável conforme papel/processo	Implementar e evidenciar	Política interna e segregação lógica.
B.2.2.4	Uso para marketing e propaganda	Aplicável conforme papel/processo	Implementar e evidenciar	Cláusula contratual e bloqueios de uso.
B.2.2.5	Instruções infratoras	Aplicável conforme papel/processo	Implementar e evidenciar	Registro de alerta e decisão do cliente.
B.2.2.6	Obrigações do cliente	Aplicável conforme papel/processo	Implementar e evidenciar	DPA, matriz de responsabilidades e SLA.
B.2.2.7	Registros relativos ao tratamento	Aplicável conforme papel/processo	Implementar e evidenciar	Logs, ROPA como operadora e evidências.
B.2.3.2	Compliance com obrigações perante titulares	Aplicável conforme papel/processo	Implementar e evidenciar	Ticket de apoio, logs e retorno ao controlador.

B.2.4.2	Arquivos temporários	Aplicável conforme papel/processo	Implementar e evidenciar	Registro de limpeza e controles de acesso.
B.2.4.3	Devolução, transferência ou descarte de DP	Aplicável conforme papel/processo	Implementar e evidenciar	Termo de devolução/descarte e evidências.
B.2.4.4	Controles de transmissão de DP	Aplicável conforme papel/processo	Implementar e evidenciar	TLS, SFTP, VPN, criptografia e logs.
B.2.5.2	Fundamentação para transferência entre jurisdições	Aplicável conforme papel/processo	Implementar e evidenciar	Contrato, localidade de hospedagem e avaliação.
B.2.5.3	Países/organizações de destino	Aplicável conforme papel/processo	Implementar e evidenciar	Lista de suboperadores e regiões de cloud.
B.2.5.4	Registros de divulgações a terceiros	Aplicável conforme papel/processo	Implementar e evidenciar	Log de divulgação, base e aprovador.
B.2.5.5	Notificação de solicitações de divulgação de DP	Aplicável conforme papel/processo	Implementar e evidenciar	Registro de solicitação e comunicação.
B.2.5.6	Divulgações legalmente obrigatórias	Aplicável conforme papel/processo	Implementar e evidenciar	Parecer jurídico e protocolo.
B.2.5.7	Divulgação de subcontratados	Aplicável conforme papel/processo	Implementar e evidenciar	Catálogo de suboperadores.
B.2.5.8	Envolvimento de subcontratado	Aplicável conforme papel/processo	Implementar e evidenciar	Contrato com suboperador e due diligence.
B.2.5.9	Troca de subcontratado	Aplicável conforme papel/processo	Implementar e evidenciar	Notificação, avaliação e aceite.
B.3.3	Políticas de segurança da informação	Aplicável	Implementar e evidenciar	PSI, política de privacidade, revisão anual.
B.3.4	Papéis e responsabilidades	Aplicável	Implementar e evidenciar	Matriz RACI, nomeações e

	em segurança da informação			descrições.
B.3.5	Classificação da informação	Aplicável	Implementar e evidenciar	Matriz de classificação e etiquetas.
B.3.6	Rotulagem da informação	Aplicável	Implementar e evidenciar	Etiquetas e configuração DLP.
B.3.7	Transferência de informação	Aplicável	Implementar e evidenciar	Procedimento de transferência segura.
B.3.8	Gestão de identidade	Aplicável	Implementar e evidenciar	IAM, MFA, revisão de contas.
B.3.9	Direitos de acesso	Aplicável	Implementar e evidenciar	Matriz de acesso, logs, recertificação.
B.3.10	Segurança em contratos de fornecedores	Aplicável	Implementar e evidenciar	Cláusulas, DPA e due diligence.
B.3.11	Planejamento e preparação para incidentes	Aplicável	Implementar e evidenciar	Plano de resposta e exercícios.
B.3.12	Resposta a incidentes de segurança	Aplicável	Implementar e evidenciar	Registro de incidente e lições aprendidas.
B.3.13	Requisitos legais, estatutários, regulatórios e contratuais	Aplicável	Implementar e evidenciar	Matriz legal e revisão.
B.3.14	Proteção de registros	Aplicável	Implementar e evidenciar	Controle de retenção, backup e assinatura.
B.3.15	Análise crítica independente da segurança	Aplicável	Implementar e evidenciar	Relatórios de auditoria/pentest.
B.3.16	Compliance com políticas, regras e normas	Aplicável	Implementar e evidenciar	Checklist de conformidade e ações.
B.3.17	Conscientização, educação e treinamento	Aplicável	Implementar e evidenciar	Trilha EAD, listas e certificados.

B.3.18	Acordos de confidencialidade ou não divulgação	Aplicável	Implementar e evidenciar	Termos assinados e controle.
B.3.19	Mesa limpa e tela limpa	Aplicável	Implementar e evidenciar	Política e inspeções.
B.3.20	Mídias de armazenamento	Aplicável	Implementar e evidenciar	Registro de mídia e bloqueios.
B.3.21	Descarte seguro ou reutilização de equipamentos	Aplicável	Implementar e evidenciar	Termo de sanitização/descarte.
B.3.22	Dispositivos endpoint do usuário	Aplicável	Implementar e evidenciar	EDR/antivírus, MDM, criptografia.
B.3.23	Autenticação segura	Aplicável	Implementar e evidenciar	Política de autenticação e logs.
B.3.24	Backup das informações	Aplicável	Implementar e evidenciar	Plano de backup, testes e relatórios.
B.3.25	Log	Aplicável	Implementar e evidenciar	SIEM, trilhas de auditoria e alertas.
B.3.26	Uso de criptografia	Aplicável	Implementar e evidenciar	Inventário criptográfico e TLS.
B.3.27	Ciclo de vida de desenvolvimento seguro	Aplicável	Implementar e evidenciar	Requisitos, code review, SAST/DAST.
B.3.28	Requisitos de segurança da aplicação	Aplicável	Implementar e evidenciar	Backlog, user stories e testes.
B.3.29	Princípios de arquitetura e engenharia seguras	Aplicável	Implementar e evidenciar	Arquitetura, diagramas e revisão.
B.3.30	Desenvolvimento terceirizado	Aplicável	Implementar e evidenciar	Contrato, revisão de código e aceite seguro.
B.3.31	Informações de teste	Aplicável	Implementar e evidenciar	Base mascarada, procedimento e evidência.

18. Disposições Finais

Este Manual deve ser comunicado aos colaboradores e terceiros pertinentes, incorporado ao programa de treinamento e utilizado como critério de auditoria interna. A sua implementação deve ser acompanhada pelo Comitê de Privacidade e Segurança da Informação, com reporte periódico à Alta Direção.

Qualquer exceção a este Manual deve ser formalmente registrada, justificada, submetida a avaliação de risco e aprovada por autoridade competente, sem afastar obrigações legais, regulatórias ou contratuais.

18.1 Referências de apoio utilizadas na elaboração

- Lei nº 13.709/2018 - Lei Geral de Proteção de Dados Pessoais (LGPD), texto compilado.
- Lei nº 13.853/2019 - altera a LGPD e cria/estrutura a ANPD.
- Regulamentações e orientações oficiais da Autoridade Nacional de Proteção de Dados (ANPD), incluindo comunicação de incidentes, atuação do encarregado, dosimetria e agentes de tratamento de pequeno porte.
- ABNT NBR ISO/IEC 27701:2026 - Segurança da informação, segurança cibernética e proteção da privacidade - Sistemas de gestão da privacidade da informação - Requisitos e orientações.
- Normas complementares de segurança da informação, privacidade, desenvolvimento seguro, continuidade, gestão de riscos e requisitos contratuais aplicáveis.