CÓDIGO INSTITUCIONAL • VGF-PRI-001 • VERSÃO 2.0

Política de Privacidade e Proteção de Dados Pessoais

LGPD • ISO/IEC 27701:2025 • alinhamento ao GDPR

Compromisso público com tratamento lícito, transparente, seguro e responsável de dados pessoais em todas as atividades jurídicas, administrativas, digitais e de relacionamento.

ORGANIZAÇÃO	VOLK E GIFFONI FERREIRA SOCIEDADE DE ADVOGADOS — CNPJ 23.637.778/0001-01
ELABORAÇÃO	Time Técnico Operacional • 21 de outubro de 2025
APROVAÇÃO	Diretoria e Comitê multidisciplinar
SITUAÇÃO	Aprovado • uso institucional e comunicação ao mercado

Nota de integridade documental. Este instrumento estabelece compromissos e requisitos de governança. Alinhamento normativo não significa certificação, atestado de conformidade ou prova isolada de implementação.

1. Controle e identificação do documento

Campo	Informação
Título	Política de Privacidade e Proteção de Dados Pessoais
Código	VGF-PRI-001
Versão vigente	2.0
Data de elaboração/revisão	21 de outubro de 2025
Elaboração	Time Técnico Operacional
Aprovação	Diretoria e Comitê multidisciplinar
Periodicidade de revisão	Anual ou antes, diante de alteração legal, normativa, operacional, tecnológica ou de risco relevante
Classificação	Público institucional, ressalvados anexos e evidências operacionais classificados
Proprietário do documento	Encarregado (DPO), com apoio do Comitê multidisciplinar

1.1 Histórico de versões

Versão	Data	Síntese da alteração	Aprovação
1.0	3 de fevereiro de 2025	Emissão inicial e estruturação dos compromissos institucionais.	Diretoria
2.0	21 de outubro de 2025	Revisão integral; integração LGPD, GDPR, PIMS, transferências internacionais, incidentes, privacy by design e rastreabilidade aos formulários. Inclusão de fluxo executivo ilustrado e catálogo ampliado de requisitos, controles e evidências.	Diretoria e Comitê multidisciplinar

LEITURA CORRETA A versão 2.0 substitui versões anteriores. Cópias impressas são não controladas; a validade deve ser conferida no repositório oficial.

2. Objetivo, escopo e aplicação

Esta Política estabelece os princípios, responsabilidades e requisitos mínimos para o tratamento de dados pessoais pela VGF, como controladora, operadora ou agente em arranjos específicos, promovendo direitos fundamentais, sigilo profissional, responsabilização e melhoria contínua do Sistema de Gestão de Informações de Privacidade (PIMS).

Aplica-se à Diretoria, sócios, advogados, estagiários, empregados, prestadores, correspondentes, consultores, parceiros e terceiros que atuem em nome ou no interesse da VGF, observadas a natureza do vínculo, as responsabilidades contratuais e a legislação aplicável. Também orienta a relação com clientes, titulares de dados, fornecedores, autoridades, comunidade e demais partes interessadas.

- Abrange dados de clientes e seus representantes, partes, testemunhas, peritos, profissionais, candidatos, fornecedores, visitantes, usuários de canais digitais e demais pessoas naturais.
- Abrange coleta, acesso, consulta, organização, uso, compartilhamento, armazenamento, transmissão, arquivamento, anonimização, eliminação e demais operações, em meios físicos ou digitais.
- As obrigações do GDPR são adotadas como referência e aplicadas quando houver alcance territorial, estabelecimento, oferta ou monitoramento relevante no Espaço Econômico Europeu.

HIERARQUIA Em caso de conflito, prevalecem a lei, as normas profissionais da OAB, decisões de autoridade competente e obrigações contratuais mais protetivas. Dúvidas devem ser elevadas ao proprietário do documento antes da ação.

3. Fundamentos, princípios e responsabilidades

3.1 Fundamentos e princípios

A VGF interpreta a privacidade como requisito de confiança e de qualidade jurídica. O tratamento deve ser demonstravelmente compatível com a finalidade, o contexto, o risco e as expectativas legítimas do titular.

- finalidade, adequação, necessidade e minimização;
- livre acesso, qualidade, transparência e linguagem acessível;
- segurança, prevenção, privacidade desde a concepção e por padrão;
- não discriminação, respeito à autodeterminação informativa e equidade;
- responsabilização, prestação de contas, rastreabilidade e melhoria contínua;
- sigilo profissional, independência técnica e preservação de direitos em processos.

3.2 Estrutura de responsabilidades

Papel	Responsabilidades centrais	Prestação de contas
Diretoria	Aprovar o PIMS, recursos, apetite a risco e decisões relevantes.	Análise crítica, indicadores e planos.
Encarregado (DPO)	Sancle Albuquerque — Encarregado (DPO) externo, profissional DPO Practitioner; orientar, receber titulares e ANPD, monitorar e aconselhar.	Relatório de atividades, registros de atendimento e recomendações independentes.
Comitê multidisciplinar	Integrar privacidade a jurídico, tecnologia, pessoas, compliance, segurança e fornecedores.	RIPD, riscos, incidentes e deliberações.
Controladores de processo	Definir finalidade, base legal, dados, retenção, acessos, operadores e transparência.	ROPA/inventário, avisos, contratos, testes e revisões.
Operadores e terceiros	Tratar apenas sob instrução documentada e implementar medidas adequadas.	Contratos, suboperadores, logs, incidentes e devolução/eliminação.
Todos os profissionais	Usar dados pelo mínimo necessário, proteger sigilo e comunicar desvios.	Termos, treinamento e observância diária.

3.3 Fluxo executivo de aplicação

O fluxo abaixo resume a sequência decisória esperada. Ele não substitui os procedimentos específicos, mas orienta o leitor sobre quando registrar, consultar, controlar, escalar e aprender.

Figura 1 — Ciclo executivo do Sistema de Gestão de Informações de Privacidade.

4. Diretrizes institucionais

As diretrizes seguintes devem ser convertidas em controles proporcionais ao risco, documentadas no inventário de tratamento e demonstradas por evidência atual.

4.1 Papéis, contexto e instruções de tratamento

Antes de iniciar ou alterar uma atividade, a VGF identifica as partes, os papéis de controladora, operadora ou corresponsável, as instruções legítimas e os limites do mandato jurídico.

- Registrar controlador, operadores, suboperadores, categorias de titulares e de dados, finalidade, base legal, sistemas, países, retenção e medidas de segurança.
- Não aceitar instrução manifestamente ilícita; comunicar conflito ao cliente/controlador e documentar a decisão.
- Segregar decisões próprias da VGF das atividades executadas estritamente em nome do cliente.

4.2 Bases legais e teste de necessidade

Cada finalidade deve possuir fundamento jurídico documentado antes da coleta ou do uso. A base legal não é escolhida por conveniência e deve ser reavaliada se o contexto mudar.

- Considerar consentimento, contrato e procedimentos preliminares, obrigação legal/regulatória, exercício regular de direitos, legítimo interesse, proteção da vida, tutela da saúde, crédito ou outra hipótese aplicável.
- Para legítimo interesse, documentar finalidade legítima, necessidade, balanceamento, expectativas, impacto e salvaguardas, com opção de oposição quando aplicável.
- Para dados sensíveis, utilizar apenas hipótese do art. 11 da LGPD e aplicar salvaguardas reforçadas.

4.3 Minimização, qualidade e coleta indireta

Devem ser tratados apenas dados pertinentes, adequados e não excessivos. Dados obtidos de clientes, partes, fontes públicas ou terceiros permanecem sujeitos a avaliação de licitude e transparência.

- Evitar cópias integrais de documentos quando campos específicos forem suficientes.
- Definir controles de atualização, correção, validação e proveniência compatíveis com o impacto.
- Proibir compra ou enriquecimento de bases sem diligência de origem, finalidade, aviso, oposição e contrato.

4.4 Dados sensíveis, crianças, adolescentes e pessoas vulneráveis

Tratamentos de maior impacto exigem acesso restrito, necessidade comprovada, avaliação de risco e linguagem apropriada.

- Aplicar o melhor interesse da criança e do adolescente, verificação proporcional de representação e informação acessível.
- Restringir exposição de saúde, biometria, filiação sindical, origem racial, crença, vida sexual e dados equivalentes.
- Evitar inferências sensíveis e discriminação; revisar decisões com potencial de efeito significativo.

4.5 Transparência e avisos de privacidade

Titulares devem receber informação clara sobre identidade do agente, finalidades, dados, compartilhamentos, direitos, retenção, transferências e canais.

- Usar avisos em camadas e no ponto de coleta, sem textos vagos ou padrões manipulativos.
- Distinguir informação institucional de aconselhamento jurídico e preservar sigilo de clientes e casos.
- Manter versões, data de vigência, registro das mudanças e meios de comunicação proporcionais.

4.6 Direitos dos titulares e atendimento

Pedidos são recebidos por lgpd@vgfadv.com.br | sancle.albuquerque@midnal.com.br, autenticados de modo proporcional e encaminhados ao responsável sem atrasos indevidos.

- Registrar pedido, identidade, escopo, sistemas consultados, decisão, fundamento, resposta e prazo.
- Atender confirmação, acesso, correção, anonimização, bloqueio, eliminação, portabilidade, informação, revogação, oposição e revisão de decisão automatizada, conforme aplicável.
- Conciliar o direito com sigilo profissional, direitos de terceiros, preservação de prova, obrigação legal e exercício regular de direitos, explicando eventual limitação.

4.7 Consentimento e preferências

Quando utilizado, o consentimento deve ser livre, informado, inequívoco, específico, destacado e demonstrável; a recusa ou revogação deve ser simples.

- Registrar titular, versão do aviso, finalidade, ação afirmativa, data/hora, canal e revogação.
- Separar finalidades independentes e não condicionar serviço a dado desnecessário.
- Para crianças, observar representação, melhor interesse e requisitos legais específicos.

4.8 Inventário, ROPA e mapeamento do ciclo de vida

O inventário de dados é a fonte oficial para compreender onde o dado nasce, circula, é armazenado, compartilhado, arquivado e eliminado.

- Revisar ao menos anualmente e a cada novo projeto, fornecedor, sistema, país, categoria de dado ou mudança de finalidade.
- Relacionar bases legais, avisos, contratos, controles, riscos, retenção e evidências.
- Designar proprietário e manter trilha de revisão e aprovação.

4.9 Privacidade desde a concepção, por padrão e RIPD

Projetos, serviços, campanhas, sistemas, integrações e mudanças relevantes devem passar por triagem de privacidade antes da produção.

- Adotar configurações padrão minimizadas, segregação, pseudonimização, criptografia, acesso mínimo e testes.
- Elaborar RIPD quando o tratamento puder gerar alto risco, envolver larga escala, monitoramento, sensíveis, vulneráveis, inovação ou decisões significativas.
- Consultar o DPO e registrar risco residual; não iniciar tratamento de alto risco sem aprovação competente.

4.10 Decisões automatizadas, análise e inteligência artificial

A VGF não delega julgamento jurídico ou decisão com efeito relevante a automação sem supervisão humana adequada, validação e possibilidade de contestação.

- Inventariar modelos, finalidade, dados de entrada, fornecedor, limitações, testes, vieses, segurança e explicabilidade.
- Não inserir dados sigilosos ou pessoais em IA pública sem autorização, contrato, configuração e avaliação aprovados.
- Revisar resultados por profissional qualificado e informar o uso quando legalmente exigido ou material à confiança.

ATENÇÃO Conteúdo gerado por IA é apoio, não autoridade. Deve ser verificado quanto a fatos, citações, vieses, segredo profissional, direitos autorais e estratégia do caso.

4.11 Retenção, arquivamento, anonimização e descarte

Dados são mantidos pelo tempo necessário à finalidade, obrigação legal, contrato, defesa de direitos e tabela de temporalidade aprovada.

- Definir gatilho, prazo, base, responsável, suspensão por litígio e método de disposição para cada classe.
- Excluir ou anonimizar ao fim do prazo; backups seguem ciclo próprio e bloqueio de reutilização até sobrescrita.
- Sanitizar mídias e destruir papel de modo irrecuperável, com certificado quando terceirizado ou relevante.

4.12 Compartilhamento, operadores e suboperadores

O compartilhamento deve ser necessário, compatível, transparente e protegido por diligência e instrumento adequado.

- Contratos devem cobrir finalidade, instruções, confidencialidade, segurança, subcontratação, direitos, incidentes, auditoria, retorno/eliminação e transferências.
- Classificar terceiros por risco e reavaliar periodicamente, exigindo plano de correção quando necessário.
- Manter lista de operadores críticos e contato responsável.

4.13 Transferências internacionais

Transferências são identificadas no inventário e realizadas mediante mecanismo válido, transparência, avaliação do destino e salvaguardas contratuais e técnicas.

- Aplicar a Resolução CD/ANPD nº 19/2024 e suas cláusulas-padrão, quando cabíveis.
- Considerar decisões de adequação vigentes, inclusive o reconhecimento aplicável à União Europeia, sem presumir cobertura de todo fluxo.
- Documentar países, importadores, suboperadores, suporte remoto, backups, leis locais e medidas suplementares.

4.14 Segurança e incidentes com dados pessoais

Medidas técnicas e organizacionais devem refletir natureza, volume, contexto, probabilidade e impacto, preservando confidencialidade, integridade, disponibilidade e resiliência.

- Aplicar controle de acesso, autenticação robusta, criptografia, logs, backup, monitoramento, gestão de vulnerabilidades e continuidade.
- Comunicar suspeitas imediatamente ao fluxo interno; preservar evidências, conter, avaliar risco e registrar decisão.
- Quando houver risco ou dano relevante, o controlador comunica ANPD e titulares nos prazos e conteúdos da Resolução CD/ANPD nº 15/2024; manter registros por ao menos cinco anos.

4.15 Marketing, cookies e relacionamento

Comunicações institucionais devem respeitar privacidade, preferências e as regras éticas da advocacia, com caráter informativo, discreto e não mercantilista.

- Manter base de contatos lícita, identificação do remetente, descadastramento efetivo e lista de supressão.
- Não utilizar listas de origem desconhecida ou abordar pessoa sem fundamento e expectativa compatível.
- Cookies não essenciais e tecnologias equivalentes devem ter transparência e escolha proporcional quando aplicável.

4.16 Sigilo profissional, processos e dever de preservação

O sigilo profissional é requisito reforçado que convive com a LGPD e protege cliente, estratégia, comunicações e informações do caso.

- Aplicar segregação por caso, conflito e equipe; limitar compartilhamento ao necessário.
- Preservar documentos sob ordem judicial, investigação, auditoria ou defesa, suspendendo descarte de modo controlado.
- Avaliar pedidos de autoridades quanto à competência, finalidade, escopo, minimização e registro da entrega.

5. Governança, aplicação, monitoramento e rastreabilidade

5.1 Comunicação, educação e aceite

A VGF disponibiliza conteúdo, trilhas de aprendizagem e assinatura eletrônica de termos na Academy Volk (https://academyvolk.ultramidnal.com.br/), sem prejuízo de orientações presenciais ou em outros canais oficiais.

- Capacitação no ingresso e reciclagem ao menos anual, com módulos proporcionais à função e ao risco.
- Registro de convocação, participação, conclusão, avaliação de aprendizagem e aceite da versão vigente.
- Conteúdo extraordinário quando houver incidente, alteração relevante, nova tecnologia, serviço ou requisito.

5.2 Canal, consulta, relato e não retaliação

Dúvidas e relatos podem ser encaminhados à liderança competente ou à Ouvidoria (ouvidoria@vgfadv.com.br). Questões de dados pessoais devem ser dirigidas aos canais do DPO (lgpd@vgfadv.com.br | sancle.albuquerque@midnal.com.br).

- Relatos de boa-fé devem ser recebidos com respeito, confidencialidade, independência e proibição de retaliação.
- A identidade será restrita ao necessário; anonimato será preservado quando oferecido e juridicamente possível.
- Urgências de segurança, integridade física, fraude ou destruição de evidências exigem escalonamento imediato.

5.3 Monitoramento, desvios e melhoria contínua

A efetividade é monitorada por indicadores, testes amostrais, avaliações de risco, reclamações, incidentes, auditorias, diligências e análise crítica da liderança.

- Não conformidades devem ser registradas, contidas, analisadas quanto à causa e tratadas com responsável e prazo.
- Medidas disciplinares são proporcionais, coerentes, documentadas e aplicadas com contraditório quando cabível.
- Resultados relevantes alimentam revisão de riscos, controles, treinamento e documentação.

5.4 Gestão documental e exceções

Somente documentos aprovados e vigentes podem orientar a operação. Exceções devem ser raras, justificadas, temporárias, avaliadas quanto ao risco e aprovadas por autoridade competente.

- Preservar autoria, aprovação, versão, data, classificação, local oficial e prazo de revisão.
- Retirar ou identificar cópias obsoletas e impedir uso não intencional.
- Registrar aceite de risco, controles compensatórios, responsável e data de expiração da exceção.

5.5 Contato do Encarregado e cooperação regulatória

Sancle Albuquerque — Encarregado (DPO) externo, profissional DPO Practitioner. Canais: lgpd@vgfadv.com.br | sancle.albuquerque@midnal.com.br. O DPO atua como canal, aconselha e monitora, sem substituir a responsabilidade dos agentes de tratamento e donos de processo.

- Garantir acesso do DPO à liderança e aos processos relevantes, com ausência de conflito de interesses.
- Cooperar com ANPD e outras autoridades competentes de forma coordenada, verdadeira e documentada.
- Publicar os canais e manter plano de continuidade para ausências.

5.6 Cobertura executiva da LGPD

Mapa de cobertura temática dos capítulos e artigos da LGPD, com foco na aplicação prática ao contexto de uma sociedade de advogados.

USO DA MATRIZ Os identificadores facilitam rastreabilidade e auditoria. As descrições são sínteses executivas e não substituem a aquisição, leitura e interpretação da norma oficial aplicável.

Referência	Controle / requisito	Aplicação executiva na VGF	Evidências e verificação
Arts. 1–4	Objeto, alcance territorial e exceções	Identificar se a LGPD alcança a operação, o papel da VGF e eventuais exceções sem ampliar sua interpretação.	ROPA, análise de escopo, contrato e parecer quando necessário.

Arts. 5–6	Conceitos e princípios	Usar definições legais e demonstrar finalidade, necessidade, transparência, segurança, prevenção e prestação de contas.	Política, inventário, avisos, riscos e testes.
Arts. 7–10	Bases legais e legítimo interesse	Documentar fundamento antes do tratamento e realizar balanceamento quando usado legítimo interesse.	ROPA, LIA, contrato, obrigação e aprovação.
Arts. 11–13	Dados sensíveis, saúde e pesquisa	Aplicar hipótese específica, minimização e proteção reforçada; limitar usos secundários.	RIPD, acessos, pseudonimização e contratos.
Art. 14	Crianças e adolescentes	Adotar melhor interesse, informação acessível e representação quando cabível.	Triagem, aviso, registro de representação e controles.
Arts. 15–16	Término e conservação	Eliminar, anonimizar ou conservar somente nas hipóteses permitidas, com bloqueio de uso incompatível.	Tabela de temporalidade, legal hold e logs de descarte.
Arts. 17–22	Direitos dos titulares	Operar canal, autenticação, busca, decisão fundamentada e resposta dentro do prazo aplicável.	Procedimento, protocolos, respostas e métricas.
Arts. 23–30	Tratamento pelo poder público	Avaliar requisitos quando a VGF atuar para ente público ou receber dados oriundos do poder público.	Contrato público, finalidade, transparência e compartilhamentos.
Arts. 31–32	Correção e fiscalização no setor público	Cooperar com correções e controles específicos quando integrar fluxo público.	Notificações, planos e registro de correção.
Arts. 33–36	Transferência internacional	Identificar fluxo e mecanismo válido, aplicar cláusulas e medidas suplementares.	Mapa de países, DPA, cláusulas ANPD e avaliação.
Arts. 37–40	Registros, RIPD e operadores	Manter registro das operações, produzir RIPD quando necessário e governar instruções a operadores.	ROPA, RIPD, instruções, DPA e auditoria.
Art. 41	Encarregado	Publicar contato, assegurar independência e acesso à liderança, sem transferir responsabilidade dos agentes.	Nomeação, canal, relatório e plano de substituição.
Arts. 42–45	Responsabilidade e reparação	Prevenir dano, preservar prova de diligência e tratar solidariedade e exceções conforme o papel.	Riscos, controles, incidentes, contratos e defesa.
Arts. 46–49	Segurança e sistemas	Aplicar medidas desde a concepção, responder a incidentes e estruturar sistemas conforme princípios.	SGSI, arquitetura, logs, testes e incidentes.
Art. 50	Governança e boas práticas	Manter programa com regras, reclamações, segurança, supervisão, educação e melhoria.	PIMS, políticas, Academy, auditorias e análise crítica.
Arts. 52–54	Sanções e processo	Conhecer riscos sancionatórios e cooperar com processo regular, sem obstrução.	Matriz legal, resposta regulatória e remediação.
Arts. 55-A–55-L	ANPD	Reconhecer competências da Autoridade e monitorar regulamentações aplicáveis.	Radar regulatório, responsáveis e atualização documental.
Arts. 58-A–65	CNPD e disposições finais	Monitorar diretrizes e vigência que possam alterar obrigações e interpretações.	Registro de mudanças e revisão do PIMS.

5.7 ISO/IEC 27701:2025 — requisitos e domínios do PIMS

A edição 2025 é tratada como sistema de gestão autônomo. A matriz cobre as cláusulas de gestão e os principais domínios de controladoria e operação de PII, sem reproduzir o texto protegido da norma.

USO DA MATRIZ Os identificadores facilitam rastreabilidade e auditoria. As descrições são sínteses executivas e não substituem a aquisição, leitura e interpretação da norma oficial aplicável.

Referência	Controle / requisito	Aplicação executiva na VGF	Evidências e verificação
Cl. 4	Contexto da organização	Definir escopo do PIMS, partes interessadas, requisitos e interfaces relevantes para privacidade e tratamento de PII.	Escopo aprovado, mapa de partes interessadas, requisitos e processos.

Cl. 5	Liderança	Demonstrar compromisso, aprovar política, atribuir papéis e integrar privacidade e tratamento de PII às decisões da VGF.	Política, organograma, atas, comunicações e provisão de recursos.
Cl. 6	Planejamento	Avaliar riscos e oportunidades, definir objetivos mensuráveis e planejar mudanças relacionadas a privacidade e tratamento de PII.	Matriz de riscos, objetivos, indicadores, planos e aceites de risco.
Cl. 7	Apoio	Assegurar recursos, competência, conscientização, comunicação e informação documentada controlada.	Orçamento, competências, Academy, comunicações e controle documental.
Cl. 8	Operação	Planejar, executar e controlar processos e terceiros que materializam privacidade e tratamento de PII, inclusive mudanças e exceções.	Procedimentos, contratos, tickets, aprovações, testes e registros operacionais.
Cl. 9	Avaliação de desempenho	Monitorar indicadores, realizar auditoria interna proporcional e promover análise crítica da liderança.	Dashboards, testes, auditorias, atas e planos de correção.
Cl. 10	Melhoria	Tratar não conformidades e incidentes, eliminar causas, verificar eficácia e melhorar continuamente.	Registro de desvios, causa raiz, ações, verificação e lições aprendidas.
PIMS-01	Determinação de papéis de PII	Definir quando a VGF é controladora, operadora ou atua em arranjo conjunto e documentar interfaces.	ROPA, contrato, DPA e decisão de papel.
PIMS-02	Finalidade e fundamento	Vincular cada tratamento a propósito legítimo, base aplicável e limites de reutilização.	ROPA, LIA, avisos e aprovações.
PIMS-03	Consentimento e preferências	Quando utilizado, registrar obtenção, versão, escopo e revogação.	Logs de consentimento e lista de supressão.
PIMS-04	Direitos e comunicação com titulares	Operar processo rastreável, acessível e compatível com sigilo e direitos de terceiros.	Protocolos, SLA, respostas e métricas.
PIMS-05	Privacy by design/default	Integrar requisitos no projeto, padrão mínimo, testes e aprovação antes da produção.	Checklist, threat/privacy model e gate.
PIMS-06	Risco e impacto de privacidade	Realizar triagem e avaliação detalhada quando o risco for elevado.	RIPD, plano, aceite e revisão.
PIMS-07	Minimização, qualidade e exatidão	Limitar campos e cópias, controlar proveniência e corrigir inexatidão material.	Dicionário, validações e amostras.
PIMS-08	Retenção e disposição	Definir gatilho, prazo, hold, exclusão, anonimização e evidência.	Tabela, logs e certificados.
PIMS-09	Compartilhamento e operadores	Aplicar diligência, instrução, contrato, suboperadores e supervisão.	Cadastro, DPA, avaliações e relatórios.
PIMS-10	Transferências transfronteiriças	Identificar países, mecanismo e medidas suplementares.	Mapa, cláusulas, regiões e aprovação.
PIMS-11	Segurança de PII	Aplicar controle proporcional, segregação, criptografia, logs e continuidade.	SoA, configuração, testes e incidentes.
PIMS-12	Incidentes e violações	Avaliar risco, conter, registrar, comunicar e aprender.	Dossiê, comunicação, causa raiz e plano.
PIMS-13	Transparência e avisos	Informar de modo claro finalidade, dados, partes, direitos, retenção e canais.	Avisos versionados e prova de disponibilização.
PIMS-14	Terceiros, auditoria e conformidade	Monitorar eficácia e exigir correção proporcional.	Due diligence, auditoria, indicadores e CAPA.

5.8 GDPR — alinhamento por capítulos

O GDPR é referência internacional e obrigação quando seu alcance territorial se verificar. A VGF deve confirmar aplicabilidade em cada fluxo europeu.

USO DA MATRIZ Os identificadores facilitam rastreabilidade e auditoria. As descrições são sínteses executivas e não substituem a aquisição, leitura e interpretação da norma oficial aplicável.

Referência	Controle / requisito	Aplicação executiva na VGF	Evidências e verificação
Cap. I	Disposições gerais	Confirmar escopo material, territorial, papéis e estabelecimento.	Análise de aplicabilidade e ROPA.
Cap. II	Princípios e licitude	Documentar princípios, bases, condições de consentimento e categorias especiais.	ROPA, LIA, consentimento e RIPD.
Cap. III	Direitos do titular	Atender transparência, acesso, retificação, apagamento, restrição, portabilidade, oposição e automação.	Procedimento, protocolos e respostas.
Cap. IV	Controlador e operador	Aplicar accountability, design/default, contratos, registros, segurança, incidentes e DPO.	DPA, ROPA, SGSI, incidentes e nomeação.
Cap. V	Transferências internacionais	Usar decisão de adequação, salvaguarda apropriada ou derrogação estrita conforme caso.	SCC, TIA, países e medidas.
Cap. VI–VII	Autoridades e cooperação	Identificar autoridade líder e cooperar em arranjos transfronteiriços quando aplicável.	Mapa regulatório e comunicações.
Cap. VIII	Recursos, responsabilidade e sanções	Preservar direitos, documentação de diligência e resposta regulatória.	Riscos, auditorias e dossiês.
Cap. IX–XI	Situações específicas e disposições finais	Avaliar regras nacionais, segredo profissional, emprego, arquivo e atualizações.	Parecer local, contratos e radar regulatório.

5.9 Referências normativas e informacionais

As referências abaixo orientam a interpretação e a atualização deste documento. Normas técnicas são aplicadas de forma proporcional ao contexto da VGF e não representam declaração de certificação.

- Portal institucional da VGF Advogados — https://www.vgfadv.com.br
- Código de Ética e Disciplina da OAB — https://www.oab.org.br/leisnormas/legislacao/resolucoes/02-2015
- Provimento CFOAB nº 205/2021 — publicidade e informação da advocacia — https://www.oab.org.br/leisnormas/legislacao/provimentos/205-2021
- Lei nº 13.709/2018 — LGPD, texto compilado — https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709compilado.htm
- Regulamentações da ANPD — https://www.gov.br/anpd/pt-br/acesso-a-informacao/institucional/atos-normativos/regulamentacoes_anpd
- Transferência Internacional de Dados — ANPD — https://www.gov.br/anpd/pt-br/assuntos/assuntos-internacionais/transferencia-internacional-de-dados
- Regulamento (UE) 2016/679 — GDPR — https://eur-lex.europa.eu/eli/reg/2016/679/oj
- ISO/IEC 27701:2025 — PIMS — https://www.iso.org/standard/27701
- ISO/IEC 27001:2022 — SGSI — https://www.iso.org/standard/27001

5.10 Matriz de rastreabilidade para avaliações de terceiros

A matriz indica onde o compromisso está definido e qual evidência operacional deve corroborar eventual resposta a questionários. A política, isoladamente, demonstra desenho de controle; a efetividade depende de registros atuais, amostras, configurações, contratos, relatórios ou entrevistas.

Formulário / item	Tema avaliado	Referência neste documento	Evidência recomendada
Privacidade 1–10	Natureza do serviço, acesso, ciclo de vida, dados, sistemas e fase.	2; 4.1–4.4; 4.8	Contrato/escopo, ROPA, diagrama de fluxo, inventário de sistemas e acessos.
Privacidade 11–13	DPO e decisões automatizadas.	3.2; 4.6; 4.10; 5.5	Nomeação do DPO, canal publicado, registro de IA/automação e revisão humana.
Privacidade 14–19	Subcontratação, compartilhamento e transferência	4.12–4.13	Due diligence, DPA, lista de

Formulário / item	Tema avaliado	Referência neste documento	Evidência recomendada
	internacional.		suboperadores, países, cláusulas ANPD e arquitetura.
Privacidade 20	Direitos dos titulares.	4.6	Procedimento, protocolo, amostras de resposta, SLA e métricas.
Privacidade 21–24	Descarte, sanitização e retenção.	4.11; seção 6	Tabela de temporalidade, logs de exclusão e certificados de destruição.
Privacidade 25–32	Políticas, consentimento, treinamento, data mapping, PbD, RIPD e confidencialidade.	1; 4.7–4.9; 5.1; seção 6	Versão aprovada, termos Academy, ROPA, LIA/RIPD, NDA e registros de revisão.
Privacidade 33–34	Marketing e origem de leads.	4.15	Aviso/campanha, prova de base, opt-out, lista de supressão e diligência da fonte.
Privacidade 35–36	Gestão e histórico de incidentes.	4.14; 5.3	Registro de incidentes, análise de risco, comunicações e lições aprendidas; responder fatos separadamente.

5.C01 Caderno de controle — governança do PIMS e contexto organizacional

LEITURA EXECUTIVA Este caderno converte o compromisso sobre governança do pims e contexto organizacional em uma rotina verificável. Aplica-se a toda operação com dados pessoais, inclusive projetos, contratos, sistemas, processos físicos e serviços prestados em nome de clientes e deve ser usado antes da decisão, durante a execução e na revisão de eficácia. O objetivo é permitir que qualquer leitor compreenda o que deve ser feito, quem decide, qual evidência comprova a prática e quando o tema precisa ser escalado.

Objetivo, resultado e critério de aceitação

O resultado esperado para governança do pims e contexto organizacional é uma decisão coerente com LGPD, sigilo profissional, ISO/IEC 27701:2025 e, quando aplicável, GDPR, baseada em risco, documentada no nível proporcional ao impacto e passível de reconstrução por terceiro independente. O controle é considerado implementado somente quando há responsável designado, critério prévio, execução demonstrável, tratamento de exceções e verificação periódica.

Aplicação operacional mínima

- Planejar: o dono do processo, com orientação do Encarregado (DPO) define finalidade, entradas, critérios, alçada, prazo e evidência necessária para governança do pims e contexto organizacional.
- Executar: utilizar fluxo oficial, segregação de funções e validações proporcionais; decisões sensíveis dependem de Encarregado (DPO), Comitê multidisciplinar ou Diretoria, conforme risco residual.
- Registrar: preservar solicitação, análise, aprovação, resultado, comunicação e eventual exceção em repositório oficial do PIMS ou sistema corporativo associado ao processo.
- Verificar: realizar ao menos anual e após mudança relevante, incidente ou reclamação teste de desenho e amostra de eficácia, registrando população, seleção, resultado e conclusão.
- Corrigir: desvios devem ser contidos, avaliados quanto à causa, tratados por plano com responsável e submetidos a reteste.

Elemento	Padrão verificável
Responsabilidade	Dono: dono do processo, com orientação do Encarregado (DPO). Consultados: Jurídico, Segurança da Informação, Tecnologia, Pessoas, Compliance e gestor do contrato. Aprovação/escalonamento: Encarregado (DPO), Comitê multidisciplinar ou Diretoria, conforme risco residual.
Evidência mínima	Registro de entrada, análise, decisão, execução e verificação; conservação em repositório oficial do PIMS ou sistema corporativo associado ao processo com acesso por necessidade.
Indicadores	Percentual de casos conformes; exceções vencidas; tempo de decisão; reincidência; cobertura de treinamento; ações corretivas no prazo.
Teste e alerta	Amostra baseada em risco e revisão após mudança. Escalar imediatamente quando houver tratamento de alto risco, dado sensível em escala, decisão automatizada relevante, transferência sem mecanismo confirmado ou incidente material.

Perguntas executivas para aprovação

- A finalidade e a necessidade de governança do pims e contexto organizacional estão claras e permanecem válidas?
- Os riscos, pessoas afetadas, dependências, obrigações e possíveis conflitos foram avaliados?
- A evidência produzida permite demonstrar não apenas a existência, mas a efetividade do controle?
- Há condição de parada, prazo de reavaliação e responsável por corrigir eventual resultado adverso?

GATILHO DE PROJETO OU CONTRATO Em novo projeto, produto, fornecedor ou contrato, o tema governança do pims e contexto organizacional deve integrar a avaliação de entrada. Se a resposta depender de premissa não confirmada, a aprovação será condicionada; se houver tratamento de alto risco, dado sensível em escala, decisão

automatizada relevante, transferência sem mecanismo confirmado ou incidente material, o caso seguirá para Encarregado (DPO), Comitê multidisciplinar ou Diretoria, conforme risco residual.

5.C02 Caderno de controle — inventário e registro das operações de tratamento (ROPA)

LEITURA EXECUTIVA Este caderno converte o compromisso sobre inventário e registro das operações de tratamento (ropa) em uma rotina verificável. Aplica-se a toda operação com dados pessoais, inclusive projetos, contratos, sistemas, processos físicos e serviços prestados em nome de clientes e deve ser usado antes da decisão, durante a execução e na revisão de eficácia. O objetivo é permitir que qualquer leitor compreenda o que deve ser feito, quem decide, qual evidência comprova a prática e quando o tema precisa ser escalado.

Objetivo, resultado e critério de aceitação

O resultado esperado para inventário e registro das operações de tratamento (ropa) é uma decisão coerente com LGPD, sigilo profissional, ISO/IEC 27701:2025 e, quando aplicável, GDPR, baseada em risco, documentada no nível proporcional ao impacto e passível de reconstrução por terceiro independente. O controle é considerado implementado somente quando há responsável designado, critério prévio, execução demonstrável, tratamento de exceções e verificação periódica.

Aplicação operacional mínima

- Planejar: o dono do processo, com orientação do Encarregado (DPO) define finalidade, entradas, critérios, alçada, prazo e evidência necessária para inventário e registro das operações de tratamento (ropa).
- Executar: utilizar fluxo oficial, segregação de funções e validações proporcionais; decisões sensíveis dependem de Encarregado (DPO), Comitê multidisciplinar ou Diretoria, conforme risco residual.
- Registrar: preservar solicitação, análise, aprovação, resultado, comunicação e eventual exceção em repositório oficial do PIMS ou sistema corporativo associado ao processo.
- Verificar: realizar ao menos anual e após mudança relevante, incidente ou reclamação teste de desenho e amostra de eficácia, registrando população, seleção, resultado e conclusão.
- Corrigir: desvios devem ser contidos, avaliados quanto à causa, tratados por plano com responsável e submetidos a reteste.

Elemento	Padrão verificável
Responsabilidade	Dono: dono do processo, com orientação do Encarregado (DPO). Consultados: Jurídico, Segurança da Informação, Tecnologia, Pessoas, Compliance e gestor do contrato. Aprovação/escalonamento: Encarregado (DPO), Comitê multidisciplinar ou Diretoria, conforme risco residual.
Evidência mínima	Registro de entrada, análise, decisão, execução e verificação; conservação em repositório oficial do PIMS ou sistema corporativo associado ao processo com acesso por necessidade.
Indicadores	Percentual de casos conformes; exceções vencidas; tempo de decisão; reincidência; cobertura de treinamento; ações corretivas no prazo.
Teste e alerta	Amostra baseada em risco e revisão após mudança. Escalar imediatamente quando houver tratamento de alto risco, dado sensível em escala, decisão automatizada relevante, transferência sem mecanismo confirmado ou incidente material.

Perguntas executivas para aprovação

- A finalidade e a necessidade de inventário e registro das operações de tratamento (ropa) estão claras e permanecem válidas?
- Os riscos, pessoas afetadas, dependências, obrigações e possíveis conflitos foram avaliados?
- A evidência produzida permite demonstrar não apenas a existência, mas a efetividade do controle?
- Há condição de parada, prazo de reavaliação e responsável por corrigir eventual resultado adverso?

GATILHO DE PROJETO OU CONTRATO Em novo projeto, produto, fornecedor ou contrato, o tema inventário e registro das operações de tratamento (ropa) deve integrar a avaliação de entrada. Se a resposta depender de premissa não confirmada, a aprovação será condicionada; se houver tratamento de alto risco, dado sensível em

escala, decisão automatizada relevante, transferência sem mecanismo confirmado ou incidente material, o caso seguirá para Encarregado (DPO), Comitê multidisciplinar ou Diretoria, conforme risco residual.

5.C03 Caderno de controle — mapa de dados, integrações e fluxos transfronteiriços

LEITURA EXECUTIVA Este caderno converte o compromisso sobre mapa de dados, integrações e fluxos transfronteiriços em uma rotina verificável. Aplica-se a toda operação com dados pessoais, inclusive projetos, contratos, sistemas, processos físicos e serviços prestados em nome de clientes e deve ser usado antes da decisão, durante a execução e na revisão de eficácia. O objetivo é permitir que qualquer leitor compreenda o que deve ser feito, quem decide, qual evidência comprova a prática e quando o tema precisa ser escalado.

Objetivo, resultado e critério de aceitação

O resultado esperado para mapa de dados, integrações e fluxos transfronteiriços é uma decisão coerente com LGPD, sigilo profissional, ISO/IEC 27701:2025 e, quando aplicável, GDPR, baseada em risco, documentada no nível proporcional ao impacto e passível de reconstrução por terceiro independente. O controle é considerado implementado somente quando há responsável designado, critério prévio, execução demonstrável, tratamento de exceções e verificação periódica.

Aplicação operacional mínima

- Planejar: o dono do processo, com orientação do Encarregado (DPO) define finalidade, entradas, critérios, alçada, prazo e evidência necessária para mapa de dados, integrações e fluxos transfronteiriços.
- Executar: utilizar fluxo oficial, segregação de funções e validações proporcionais; decisões sensíveis dependem de Encarregado (DPO), Comitê multidisciplinar ou Diretoria, conforme risco residual.
- Registrar: preservar solicitação, análise, aprovação, resultado, comunicação e eventual exceção em repositório oficial do PIMS ou sistema corporativo associado ao processo.
- Verificar: realizar ao menos anual e após mudança relevante, incidente ou reclamação teste de desenho e amostra de eficácia, registrando população, seleção, resultado e conclusão.
- Corrigir: desvios devem ser contidos, avaliados quanto à causa, tratados por plano com responsável e submetidos a reteste.

Elemento	Padrão verificável
Responsabilidade	Dono: dono do processo, com orientação do Encarregado (DPO). Consultados: Jurídico, Segurança da Informação, Tecnologia, Pessoas, Compliance e gestor do contrato. Aprovação/escalonamento: Encarregado (DPO), Comitê multidisciplinar ou Diretoria, conforme risco residual.
Evidência mínima	Registro de entrada, análise, decisão, execução e verificação; conservação em repositório oficial do PIMS ou sistema corporativo associado ao processo com acesso por necessidade.
Indicadores	Percentual de casos conformes; exceções vencidas; tempo de decisão; reincidência; cobertura de treinamento; ações corretivas no prazo.
Teste e alerta	Amostra baseada em risco e revisão após mudança. Escalar imediatamente quando houver tratamento de alto risco, dado sensível em escala, decisão automatizada relevante, transferência sem mecanismo confirmado ou incidente material.

Perguntas executivas para aprovação

- A finalidade e a necessidade de mapa de dados, integrações e fluxos transfronteiriços estão claras e permanecem válidas?
- Os riscos, pessoas afetadas, dependências, obrigações e possíveis conflitos foram avaliados?
- A evidência produzida permite demonstrar não apenas a existência, mas a efetividade do controle?
- Há condição de parada, prazo de reavaliação e responsável por corrigir eventual resultado adverso?

GATILHO DE PROJETO OU CONTRATO Em novo projeto, produto, fornecedor ou contrato, o tema mapa de dados, integrações e fluxos transfronteiriços deve integrar a avaliação de entrada. Se a resposta depender de premissa não confirmada, a aprovação será condicionada; se houver tratamento de alto risco, dado sensível em

escala, decisão automatizada relevante, transferência sem mecanismo confirmado ou incidente material, o caso seguirá para Encarregado (DPO), Comitê multidisciplinar ou Diretoria, conforme risco residual.

5.C04 Caderno de controle — definição de papéis entre controlador, operador e suboperador

LEITURA EXECUTIVA Este caderno converte o compromisso sobre definição de papéis entre controlador, operador e suboperador em uma rotina verificável. Aplica-se a toda operação com dados pessoais, inclusive projetos, contratos, sistemas, processos físicos e serviços prestados em nome de clientes e deve ser usado antes da decisão, durante a execução e na revisão de eficácia. O objetivo é permitir que qualquer leitor compreenda o que deve ser feito, quem decide, qual evidência comprova a prática e quando o tema precisa ser escalado.

Objetivo, resultado e critério de aceitação

O resultado esperado para definição de papéis entre controlador, operador e suboperador é uma decisão coerente com LGPD, sigilo profissional, ISO/IEC 27701:2025 e, quando aplicável, GDPR, baseada em risco, documentada no nível proporcional ao impacto e passível de reconstrução por terceiro independente. O controle é considerado implementado somente quando há responsável designado, critério prévio, execução demonstrável, tratamento de exceções e verificação periódica.

Aplicação operacional mínima

- Planejar: o dono do processo, com orientação do Encarregado (DPO) define finalidade, entradas, critérios, alçada, prazo e evidência necessária para definição de papéis entre controlador, operador e suboperador.
- Executar: utilizar fluxo oficial, segregação de funções e validações proporcionais; decisões sensíveis dependem de Encarregado (DPO), Comitê multidisciplinar ou Diretoria, conforme risco residual.
- Registrar: preservar solicitação, análise, aprovação, resultado, comunicação e eventual exceção em repositório oficial do PIMS ou sistema corporativo associado ao processo.
- Verificar: realizar ao menos anual e após mudança relevante, incidente ou reclamação teste de desenho e amostra de eficácia, registrando população, seleção, resultado e conclusão.
- Corrigir: desvios devem ser contidos, avaliados quanto à causa, tratados por plano com responsável e submetidos a reteste.

Elemento	Padrão verificável
Responsabilidade	Dono: dono do processo, com orientação do Encarregado (DPO). Consultados: Jurídico, Segurança da Informação, Tecnologia, Pessoas, Compliance e gestor do contrato. Aprovação/escalonamento: Encarregado (DPO), Comitê multidisciplinar ou Diretoria, conforme risco residual.
Evidência mínima	Registro de entrada, análise, decisão, execução e verificação; conservação em repositório oficial do PIMS ou sistema corporativo associado ao processo com acesso por necessidade.
Indicadores	Percentual de casos conformes; exceções vencidas; tempo de decisão; reincidência; cobertura de treinamento; ações corretivas no prazo.
Teste e alerta	Amostra baseada em risco e revisão após mudança. Escalar imediatamente quando houver tratamento de alto risco, dado sensível em escala, decisão automatizada relevante, transferência sem mecanismo confirmado ou incidente material.

Perguntas executivas para aprovação

- A finalidade e a necessidade de definição de papéis entre controlador, operador e suboperador estão claras e permanecem válidas?
- Os riscos, pessoas afetadas, dependências, obrigações e possíveis conflitos foram avaliados?
- A evidência produzida permite demonstrar não apenas a existência, mas a efetividade do controle?
- Há condição de parada, prazo de reavaliação e responsável por corrigir eventual resultado adverso?

GATILHO DE PROJETO OU CONTRATO Em novo projeto, produto, fornecedor ou contrato, o tema definição de

papéis entre controlador, operador e suboperador deve integrar a avaliação de entrada. Se a resposta depender de premissa não confirmada, a aprovação será condicionada; se houver tratamento de alto risco, dado sensível em escala, decisão automatizada relevante, transferência sem mecanismo confirmado ou incidente material, o caso seguirá para Encarregado (DPO), Comitê multidisciplinar ou Diretoria, conforme risco residual.

5.C05 Caderno de controle — finalidade, compatibilidade de uso e limitação de propósito

LEITURA EXECUTIVA Este caderno converte o compromisso sobre finalidade, compatibilidade de uso e limitação de propósito em uma rotina verificável. Aplica-se a toda operação com dados pessoais, inclusive projetos, contratos, sistemas, processos físicos e serviços prestados em nome de clientes e deve ser usado antes da decisão, durante a execução e na revisão de eficácia. O objetivo é permitir que qualquer leitor compreenda o que deve ser feito, quem decide, qual evidência comprova a prática e quando o tema precisa ser escalado.

Objetivo, resultado e critério de aceitação

O resultado esperado para finalidade, compatibilidade de uso e limitação de propósito é uma decisão coerente com LGPD, sigilo profissional, ISO/IEC 27701:2025 e, quando aplicável, GDPR, baseada em risco, documentada no nível proporcional ao impacto e passível de reconstrução por terceiro independente. O controle é considerado implementado somente quando há responsável designado, critério prévio, execução demonstrável, tratamento de exceções e verificação periódica.

Aplicação operacional mínima

- Planejar: o dono do processo, com orientação do Encarregado (DPO) define finalidade, entradas, critérios, alçada, prazo e evidência necessária para finalidade, compatibilidade de uso e limitação de propósito.
- Executar: utilizar fluxo oficial, segregação de funções e validações proporcionais; decisões sensíveis dependem de Encarregado (DPO), Comitê multidisciplinar ou Diretoria, conforme risco residual.
- Registrar: preservar solicitação, análise, aprovação, resultado, comunicação e eventual exceção em repositório oficial do PIMS ou sistema corporativo associado ao processo.
- Verificar: realizar ao menos anual e após mudança relevante, incidente ou reclamação teste de desenho e amostra de eficácia, registrando população, seleção, resultado e conclusão.
- Corrigir: desvios devem ser contidos, avaliados quanto à causa, tratados por plano com responsável e submetidos a reteste.

Elemento	Padrão verificável
Responsabilidade	Dono: dono do processo, com orientação do Encarregado (DPO). Consultados: Jurídico, Segurança da Informação, Tecnologia, Pessoas, Compliance e gestor do contrato. Aprovação/escalonamento: Encarregado (DPO), Comitê multidisciplinar ou Diretoria, conforme risco residual.
Evidência mínima	Registro de entrada, análise, decisão, execução e verificação; conservação em repositório oficial do PIMS ou sistema corporativo associado ao processo com acesso por necessidade.
Indicadores	Percentual de casos conformes; exceções vencidas; tempo de decisão; reincidência; cobertura de treinamento; ações corretivas no prazo.
Teste e alerta	Amostra baseada em risco e revisão após mudança. Escalar imediatamente quando houver tratamento de alto risco, dado sensível em escala, decisão automatizada relevante, transferência sem mecanismo confirmado ou incidente material.

Perguntas executivas para aprovação

- A finalidade e a necessidade de finalidade, compatibilidade de uso e limitação de propósito estão claras e permanecem válidas?
- Os riscos, pessoas afetadas, dependências, obrigações e possíveis conflitos foram avaliados?
- A evidência produzida permite demonstrar não apenas a existência, mas a efetividade do controle?
- Há condição de parada, prazo de reavaliação e responsável por corrigir eventual resultado adverso?

GATILHO DE PROJETO OU CONTRATO Em novo projeto, produto, fornecedor ou contrato, o tema finalidade, compatibilidade de uso e limitação de propósito deve integrar a avaliação de entrada. Se a resposta depender de premissa não confirmada, a aprovação será condicionada; se houver tratamento de alto risco, dado sensível em

escala, decisão automatizada relevante, transferência sem mecanismo confirmado ou incidente material, o caso seguirá para Encarregado (DPO), Comitê multidisciplinar ou Diretoria, conforme risco residual.

5.C06 Caderno de controle — seleção e documentação de bases legais

LEITURA EXECUTIVA Este caderno converte o compromisso sobre seleção e documentação de bases legais em uma rotina verificável. Aplica-se a toda operação com dados pessoais, inclusive projetos, contratos, sistemas, processos físicos e serviços prestados em nome de clientes e deve ser usado antes da decisão, durante a execução e na revisão de eficácia. O objetivo é permitir que qualquer leitor compreenda o que deve ser feito, quem decide, qual evidência comprova a prática e quando o tema precisa ser escalado.

Objetivo, resultado e critério de aceitação

O resultado esperado para seleção e documentação de bases legais é uma decisão coerente com LGPD, sigilo profissional, ISO/IEC 27701:2025 e, quando aplicável, GDPR, baseada em risco, documentada no nível proporcional ao impacto e passível de reconstrução por terceiro independente. O controle é considerado implementado somente quando há responsável designado, critério prévio, execução demonstrável, tratamento de exceções e verificação periódica.

Aplicação operacional mínima

- Planejar: o dono do processo, com orientação do Encarregado (DPO) define finalidade, entradas, critérios, alçada, prazo e evidência necessária para seleção e documentação de bases legais.
- Executar: utilizar fluxo oficial, segregação de funções e validações proporcionais; decisões sensíveis dependem de Encarregado (DPO), Comitê multidisciplinar ou Diretoria, conforme risco residual.
- Registrar: preservar solicitação, análise, aprovação, resultado, comunicação e eventual exceção em repositório oficial do PIMS ou sistema corporativo associado ao processo.
- Verificar: realizar ao menos anual e após mudança relevante, incidente ou reclamação teste de desenho e amostra de eficácia, registrando população, seleção, resultado e conclusão.
- Corrigir: desvios devem ser contidos, avaliados quanto à causa, tratados por plano com responsável e submetidos a reteste.

Elemento	Padrão verificável
Responsabilidade	Dono: dono do processo, com orientação do Encarregado (DPO). Consultados: Jurídico, Segurança da Informação, Tecnologia, Pessoas, Compliance e gestor do contrato. Aprovação/escalonamento: Encarregado (DPO), Comitê multidisciplinar ou Diretoria, conforme risco residual.
Evidência mínima	Registro de entrada, análise, decisão, execução e verificação; conservação em repositório oficial do PIMS ou sistema corporativo associado ao processo com acesso por necessidade.
Indicadores	Percentual de casos conformes; exceções vencidas; tempo de decisão; reincidência; cobertura de treinamento; ações corretivas no prazo.
Teste e alerta	Amostra baseada em risco e revisão após mudança. Escalar imediatamente quando houver tratamento de alto risco, dado sensível em escala, decisão automatizada relevante, transferência sem mecanismo confirmado ou incidente material.

Perguntas executivas para aprovação

- A finalidade e a necessidade de seleção e documentação de bases legais estão claras e permanecem válidas?
- Os riscos, pessoas afetadas, dependências, obrigações e possíveis conflitos foram avaliados?
- A evidência produzida permite demonstrar não apenas a existência, mas a efetividade do controle?
- Há condição de parada, prazo de reavaliação e responsável por corrigir eventual resultado adverso?

GATILHO DE PROJETO OU CONTRATO Em novo projeto, produto, fornecedor ou contrato, o tema seleção e documentação de bases legais deve integrar a avaliação de entrada. Se a resposta depender de premissa não confirmada, a aprovação será condicionada; se houver tratamento de alto risco, dado sensível em escala, decisão

automatizada relevante, transferência sem mecanismo confirmado ou incidente material, o caso seguirá para Encarregado (DPO), Comitê multidisciplinar ou Diretoria, conforme risco residual.

5.C07 Caderno de controle — teste de legítimo interesse (LIA)

LEITURA EXECUTIVA Este caderno converte o compromisso sobre teste de legítimo interesse (lia) em uma rotina verificável. Aplica-se a toda operação com dados pessoais, inclusive projetos, contratos, sistemas, processos físicos e serviços prestados em nome de clientes e deve ser usado antes da decisão, durante a execução e na revisão de eficácia. O objetivo é permitir que qualquer leitor compreenda o que deve ser feito, quem decide, qual evidência comprova a prática e quando o tema precisa ser escalado.

Objetivo, resultado e critério de aceitação

O resultado esperado para teste de legítimo interesse (lia) é uma decisão coerente com LGPD, sigilo profissional, ISO/IEC 27701:2025 e, quando aplicável, GDPR, baseada em risco, documentada no nível proporcional ao impacto e passível de reconstrução por terceiro independente. O controle é considerado implementado somente quando há responsável designado, critério prévio, execução demonstrável, tratamento de exceções e verificação periódica.

Aplicação operacional mínima

- Planejar: o dono do processo, com orientação do Encarregado (DPO) define finalidade, entradas, critérios, alçada, prazo e evidência necessária para teste de legítimo interesse (lia).
- Executar: utilizar fluxo oficial, segregação de funções e validações proporcionais; decisões sensíveis dependem de Encarregado (DPO), Comitê multidisciplinar ou Diretoria, conforme risco residual.
- Registrar: preservar solicitação, análise, aprovação, resultado, comunicação e eventual exceção em repositório oficial do PIMS ou sistema corporativo associado ao processo.
- Verificar: realizar ao menos anual e após mudança relevante, incidente ou reclamação teste de desenho e amostra de eficácia, registrando população, seleção, resultado e conclusão.
- Corrigir: desvios devem ser contidos, avaliados quanto à causa, tratados por plano com responsável e submetidos a reteste.

Elemento	Padrão verificável
Responsabilidade	Dono: dono do processo, com orientação do Encarregado (DPO). Consultados: Jurídico, Segurança da Informação, Tecnologia, Pessoas, Compliance e gestor do contrato. Aprovação/escalonamento: Encarregado (DPO), Comitê multidisciplinar ou Diretoria, conforme risco residual.
Evidência mínima	Registro de entrada, análise, decisão, execução e verificação; conservação em repositório oficial do PIMS ou sistema corporativo associado ao processo com acesso por necessidade.
Indicadores	Percentual de casos conformes; exceções vencidas; tempo de decisão; reincidência; cobertura de treinamento; ações corretivas no prazo.
Teste e alerta	Amostra baseada em risco e revisão após mudança. Escalar imediatamente quando houver tratamento de alto risco, dado sensível em escala, decisão automatizada relevante, transferência sem mecanismo confirmado ou incidente material.

Perguntas executivas para aprovação

- A finalidade e a necessidade de teste de legítimo interesse (lia) estão claras e permanecem válidas?
- Os riscos, pessoas afetadas, dependências, obrigações e possíveis conflitos foram avaliados?
- A evidência produzida permite demonstrar não apenas a existência, mas a efetividade do controle?
- Há condição de parada, prazo de reavaliação e responsável por corrigir eventual resultado adverso?

GATILHO DE PROJETO OU CONTRATO Em novo projeto, produto, fornecedor ou contrato, o tema teste de legítimo interesse (lia) deve integrar a avaliação de entrada. Se a resposta depender de premissa não confirmada, a aprovação será condicionada; se houver tratamento de alto risco, dado sensível em escala, decisão automatizada relevante, transferência sem mecanismo confirmado ou incidente material, o caso seguirá para

Encarregado (DPO), Comitê multidisciplinar ou Diretoria, conforme risco residual.

5.C08 Caderno de controle — consentimento, preferências e prova de manifestação

LEITURA EXECUTIVA Este caderno converte o compromisso sobre consentimento, preferências e prova de manifestação em uma rotina verificável. Aplica-se a toda operação com dados pessoais, inclusive projetos, contratos, sistemas, processos físicos e serviços prestados em nome de clientes e deve ser usado antes da decisão, durante a execução e na revisão de eficácia. O objetivo é permitir que qualquer leitor compreenda o que deve ser feito, quem decide, qual evidência comprova a prática e quando o tema precisa ser escalado.

Objetivo, resultado e critério de aceitação

O resultado esperado para consentimento, preferências e prova de manifestação é uma decisão coerente com LGPD, sigilo profissional, ISO/IEC 27701:2025 e, quando aplicável, GDPR, baseada em risco, documentada no nível proporcional ao impacto e passível de reconstrução por terceiro independente. O controle é considerado implementado somente quando há responsável designado, critério prévio, execução demonstrável, tratamento de exceções e verificação periódica.

Aplicação operacional mínima

- Planejar: o dono do processo, com orientação do Encarregado (DPO) define finalidade, entradas, critérios, alçada, prazo e evidência necessária para consentimento, preferências e prova de manifestação.
- Executar: utilizar fluxo oficial, segregação de funções e validações proporcionais; decisões sensíveis dependem de Encarregado (DPO), Comitê multidisciplinar ou Diretoria, conforme risco residual.
- Registrar: preservar solicitação, análise, aprovação, resultado, comunicação e eventual exceção em repositório oficial do PIMS ou sistema corporativo associado ao processo.
- Verificar: realizar ao menos anual e após mudança relevante, incidente ou reclamação teste de desenho e amostra de eficácia, registrando população, seleção, resultado e conclusão.
- Corrigir: desvios devem ser contidos, avaliados quanto à causa, tratados por plano com responsável e submetidos a reteste.

Elemento	Padrão verificável
Responsabilidade	Dono: dono do processo, com orientação do Encarregado (DPO). Consultados: Jurídico, Segurança da Informação, Tecnologia, Pessoas, Compliance e gestor do contrato. Aprovação/escalonamento: Encarregado (DPO), Comitê multidisciplinar ou Diretoria, conforme risco residual.
Evidência mínima	Registro de entrada, análise, decisão, execução e verificação; conservação em repositório oficial do PIMS ou sistema corporativo associado ao processo com acesso por necessidade.
Indicadores	Percentual de casos conformes; exceções vencidas; tempo de decisão; reincidência; cobertura de treinamento; ações corretivas no prazo.
Teste e alerta	Amostra baseada em risco e revisão após mudança. Escalar imediatamente quando houver tratamento de alto risco, dado sensível em escala, decisão automatizada relevante, transferência sem mecanismo confirmado ou incidente material.

Perguntas executivas para aprovação

- A finalidade e a necessidade de consentimento, preferências e prova de manifestação estão claras e permanecem válidas?
- Os riscos, pessoas afetadas, dependências, obrigações e possíveis conflitos foram avaliados?
- A evidência produzida permite demonstrar não apenas a existência, mas a efetividade do controle?
- Há condição de parada, prazo de reavaliação e responsável por corrigir eventual resultado adverso?

GATILHO DE PROJETO OU CONTRATO Em novo projeto, produto, fornecedor ou contrato, o tema consentimento, preferências e prova de manifestação deve integrar a avaliação de entrada. Se a resposta depender de premissa não confirmada, a aprovação será condicionada; se houver tratamento de alto risco, dado

sensível em escala, decisão automatizada relevante, transferência sem mecanismo confirmado ou incidente material, o caso seguirá para Encarregado (DPO), Comitê multidisciplinar ou Diretoria, conforme risco residual.

5.C09 Caderno de controle — dados pessoais sensíveis e proteção reforçada

LEITURA EXECUTIVA Este caderno converte o compromisso sobre dados pessoais sensíveis e proteção reforçada em uma rotina verificável. Aplica-se a toda operação com dados pessoais, inclusive projetos, contratos, sistemas, processos físicos e serviços prestados em nome de clientes e deve ser usado antes da decisão, durante a execução e na revisão de eficácia. O objetivo é permitir que qualquer leitor compreenda o que deve ser feito, quem decide, qual evidência comprova a prática e quando o tema precisa ser escalado.

Objetivo, resultado e critério de aceitação

O resultado esperado para dados pessoais sensíveis e proteção reforçada é uma decisão coerente com LGPD, sigilo profissional, ISO/IEC 27701:2025 e, quando aplicável, GDPR, baseada em risco, documentada no nível proporcional ao impacto e passível de reconstrução por terceiro independente. O controle é considerado implementado somente quando há responsável designado, critério prévio, execução demonstrável, tratamento de exceções e verificação periódica.

Aplicação operacional mínima

- Planejar: o dono do processo, com orientação do Encarregado (DPO) define finalidade, entradas, critérios, alçada, prazo e evidência necessária para dados pessoais sensíveis e proteção reforçada.
- Executar: utilizar fluxo oficial, segregação de funções e validações proporcionais; decisões sensíveis dependem de Encarregado (DPO), Comitê multidisciplinar ou Diretoria, conforme risco residual.
- Registrar: preservar solicitação, análise, aprovação, resultado, comunicação e eventual exceção em repositório oficial do PIMS ou sistema corporativo associado ao processo.
- Verificar: realizar ao menos anual e após mudança relevante, incidente ou reclamação teste de desenho e amostra de eficácia, registrando população, seleção, resultado e conclusão.
- Corrigir: desvios devem ser contidos, avaliados quanto à causa, tratados por plano com responsável e submetidos a reteste.

Elemento	Padrão verificável
Responsabilidade	Dono: dono do processo, com orientação do Encarregado (DPO). Consultados: Jurídico, Segurança da Informação, Tecnologia, Pessoas, Compliance e gestor do contrato. Aprovação/escalonamento: Encarregado (DPO), Comitê multidisciplinar ou Diretoria, conforme risco residual.
Evidência mínima	Registro de entrada, análise, decisão, execução e verificação; conservação em repositório oficial do PIMS ou sistema corporativo associado ao processo com acesso por necessidade.
Indicadores	Percentual de casos conformes; exceções vencidas; tempo de decisão; reincidência; cobertura de treinamento; ações corretivas no prazo.
Teste e alerta	Amostra baseada em risco e revisão após mudança. Escalar imediatamente quando houver tratamento de alto risco, dado sensível em escala, decisão automatizada relevante, transferência sem mecanismo confirmado ou incidente material.

Perguntas executivas para aprovação

- A finalidade e a necessidade de dados pessoais sensíveis e proteção reforçada estão claras e permanecem válidas?
- Os riscos, pessoas afetadas, dependências, obrigações e possíveis conflitos foram avaliados?
- A evidência produzida permite demonstrar não apenas a existência, mas a efetividade do controle?
- Há condição de parada, prazo de reavaliação e responsável por corrigir eventual resultado adverso?

GATILHO DE PROJETO OU CONTRATO Em novo projeto, produto, fornecedor ou contrato, o tema dados pessoais sensíveis e proteção reforçada deve integrar a avaliação de entrada. Se a resposta depender de premissa não confirmada, a aprovação será condicionada; se houver tratamento de alto risco, dado sensível em

escala, decisão automatizada relevante, transferência sem mecanismo confirmado ou incidente material, o caso seguirá para Encarregado (DPO), Comitê multidisciplinar ou Diretoria, conforme risco residual.

5.C10 Caderno de controle — dados de crianças e adolescentes e melhor interesse

LEITURA EXECUTIVA Este caderno converte o compromisso sobre dados de crianças e adolescentes e melhor interesse em uma rotina verificável. Aplica-se a toda operação com dados pessoais, inclusive projetos, contratos, sistemas, processos físicos e serviços prestados em nome de clientes e deve ser usado antes da decisão, durante a execução e na revisão de eficácia. O objetivo é permitir que qualquer leitor compreenda o que deve ser feito, quem decide, qual evidência comprova a prática e quando o tema precisa ser escalado.

Objetivo, resultado e critério de aceitação

O resultado esperado para dados de crianças e adolescentes e melhor interesse é uma decisão coerente com LGPD, sigilo profissional, ISO/IEC 27701:2025 e, quando aplicável, GDPR, baseada em risco, documentada no nível proporcional ao impacto e passível de reconstrução por terceiro independente. O controle é considerado implementado somente quando há responsável designado, critério prévio, execução demonstrável, tratamento de exceções e verificação periódica.

Aplicação operacional mínima

- Planejar: o dono do processo, com orientação do Encarregado (DPO) define finalidade, entradas, critérios, alçada, prazo e evidência necessária para dados de crianças e adolescentes e melhor interesse.
- Executar: utilizar fluxo oficial, segregação de funções e validações proporcionais; decisões sensíveis dependem de Encarregado (DPO), Comitê multidisciplinar ou Diretoria, conforme risco residual.
- Registrar: preservar solicitação, análise, aprovação, resultado, comunicação e eventual exceção em repositório oficial do PIMS ou sistema corporativo associado ao processo.
- Verificar: realizar ao menos anual e após mudança relevante, incidente ou reclamação teste de desenho e amostra de eficácia, registrando população, seleção, resultado e conclusão.
- Corrigir: desvios devem ser contidos, avaliados quanto à causa, tratados por plano com responsável e submetidos a reteste.

Elemento	Padrão verificável
Responsabilidade	Dono: dono do processo, com orientação do Encarregado (DPO). Consultados: Jurídico, Segurança da Informação, Tecnologia, Pessoas, Compliance e gestor do contrato. Aprovação/escalonamento: Encarregado (DPO), Comitê multidisciplinar ou Diretoria, conforme risco residual.
Evidência mínima	Registro de entrada, análise, decisão, execução e verificação; conservação em repositório oficial do PIMS ou sistema corporativo associado ao processo com acesso por necessidade.
Indicadores	Percentual de casos conformes; exceções vencidas; tempo de decisão; reincidência; cobertura de treinamento; ações corretivas no prazo.
Teste e alerta	Amostra baseada em risco e revisão após mudança. Escalar imediatamente quando houver tratamento de alto risco, dado sensível em escala, decisão automatizada relevante, transferência sem mecanismo confirmado ou incidente material.

Perguntas executivas para aprovação

- A finalidade e a necessidade de dados de crianças e adolescentes e melhor interesse estão claras e permanecem válidas?
- Os riscos, pessoas afetadas, dependências, obrigações e possíveis conflitos foram avaliados?
- A evidência produzida permite demonstrar não apenas a existência, mas a efetividade do controle?
- Há condição de parada, prazo de reavaliação e responsável por corrigir eventual resultado adverso?

GATILHO DE PROJETO OU CONTRATO Em novo projeto, produto, fornecedor ou contrato, o tema dados de crianças e adolescentes e melhor interesse deve integrar a avaliação de entrada. Se a resposta depender de premissa não confirmada, a aprovação será condicionada; se houver tratamento de alto risco, dado sensível em

escala, decisão automatizada relevante, transferência sem mecanismo confirmado ou incidente material, o caso seguirá para Encarregado (DPO), Comitê multidisciplinar ou Diretoria, conforme risco residual.

5.C11 Caderno de controle — transparência, avisos e comunicação em camadas

LEITURA EXECUTIVA Este caderno converte o compromisso sobre transparência, avisos e comunicação em camadas em uma rotina verificável. Aplica-se a toda operação com dados pessoais, inclusive projetos, contratos, sistemas, processos físicos e serviços prestados em nome de clientes e deve ser usado antes da decisão, durante a execução e na revisão de eficácia. O objetivo é permitir que qualquer leitor compreenda o que deve ser feito, quem decide, qual evidência comprova a prática e quando o tema precisa ser escalado.

Objetivo, resultado e critério de aceitação

O resultado esperado para transparência, avisos e comunicação em camadas é uma decisão coerente com LGPD, sigilo profissional, ISO/IEC 27701:2025 e, quando aplicável, GDPR, baseada em risco, documentada no nível proporcional ao impacto e passível de reconstrução por terceiro independente. O controle é considerado implementado somente quando há responsável designado, critério prévio, execução demonstrável, tratamento de exceções e verificação periódica.

Aplicação operacional mínima

- Planejar: o dono do processo, com orientação do Encarregado (DPO) define finalidade, entradas, critérios, alçada, prazo e evidência necessária para transparência, avisos e comunicação em camadas.
- Executar: utilizar fluxo oficial, segregação de funções e validações proporcionais; decisões sensíveis dependem de Encarregado (DPO), Comitê multidisciplinar ou Diretoria, conforme risco residual.
- Registrar: preservar solicitação, análise, aprovação, resultado, comunicação e eventual exceção em repositório oficial do PIMS ou sistema corporativo associado ao processo.
- Verificar: realizar ao menos anual e após mudança relevante, incidente ou reclamação teste de desenho e amostra de eficácia, registrando população, seleção, resultado e conclusão.
- Corrigir: desvios devem ser contidos, avaliados quanto à causa, tratados por plano com responsável e submetidos a reteste.

Elemento	Padrão verificável
Responsabilidade	Dono: dono do processo, com orientação do Encarregado (DPO). Consultados: Jurídico, Segurança da Informação, Tecnologia, Pessoas, Compliance e gestor do contrato. Aprovação/escalonamento: Encarregado (DPO), Comitê multidisciplinar ou Diretoria, conforme risco residual.
Evidência mínima	Registro de entrada, análise, decisão, execução e verificação; conservação em repositório oficial do PIMS ou sistema corporativo associado ao processo com acesso por necessidade.
Indicadores	Percentual de casos conformes; exceções vencidas; tempo de decisão; reincidência; cobertura de treinamento; ações corretivas no prazo.
Teste e alerta	Amostra baseada em risco e revisão após mudança. Escalar imediatamente quando houver tratamento de alto risco, dado sensível em escala, decisão automatizada relevante, transferência sem mecanismo confirmado ou incidente material.

Perguntas executivas para aprovação

- A finalidade e a necessidade de transparência, avisos e comunicação em camadas estão claras e permanecem válidas?
- Os riscos, pessoas afetadas, dependências, obrigações e possíveis conflitos foram avaliados?
- A evidência produzida permite demonstrar não apenas a existência, mas a efetividade do controle?
- Há condição de parada, prazo de reavaliação e responsável por corrigir eventual resultado adverso?

GATILHO DE PROJETO OU CONTRATO Em novo projeto, produto, fornecedor ou contrato, o tema transparência, avisos e comunicação em camadas deve integrar a avaliação de entrada. Se a resposta depender de premissa não confirmada, a aprovação será condicionada; se houver tratamento de alto risco, dado sensível em escala,

decisão automatizada relevante, transferência sem mecanismo confirmado ou incidente material, o caso seguirá para Encarregado (DPO), Comitê multidisciplinar ou Diretoria, conforme risco residual.

5.C12 Caderno de controle — minimização, qualidade, exatidão e proveniência

LEITURA EXECUTIVA Este caderno converte o compromisso sobre minimização, qualidade, exatidão e proveniência em uma rotina verificável. Aplica-se a toda operação com dados pessoais, inclusive projetos, contratos, sistemas, processos físicos e serviços prestados em nome de clientes e deve ser usado antes da decisão, durante a execução e na revisão de eficácia. O objetivo é permitir que qualquer leitor compreenda o que deve ser feito, quem decide, qual evidência comprova a prática e quando o tema precisa ser escalado.

Objetivo, resultado e critério de aceitação

O resultado esperado para minimização, qualidade, exatidão e proveniência é uma decisão coerente com LGPD, sigilo profissional, ISO/IEC 27701:2025 e, quando aplicável, GDPR, baseada em risco, documentada no nível proporcional ao impacto e passível de reconstrução por terceiro independente. O controle é considerado implementado somente quando há responsável designado, critério prévio, execução demonstrável, tratamento de exceções e verificação periódica.

Aplicação operacional mínima

- Planejar: o dono do processo, com orientação do Encarregado (DPO) define finalidade, entradas, critérios, alçada, prazo e evidência necessária para minimização, qualidade, exatidão e proveniência.
- Executar: utilizar fluxo oficial, segregação de funções e validações proporcionais; decisões sensíveis dependem de Encarregado (DPO), Comitê multidisciplinar ou Diretoria, conforme risco residual.
- Registrar: preservar solicitação, análise, aprovação, resultado, comunicação e eventual exceção em repositório oficial do PIMS ou sistema corporativo associado ao processo.
- Verificar: realizar ao menos anual e após mudança relevante, incidente ou reclamação teste de desenho e amostra de eficácia, registrando população, seleção, resultado e conclusão.
- Corrigir: desvios devem ser contidos, avaliados quanto à causa, tratados por plano com responsável e submetidos a reteste.

Elemento	Padrão verificável
Responsabilidade	Dono: dono do processo, com orientação do Encarregado (DPO). Consultados: Jurídico, Segurança da Informação, Tecnologia, Pessoas, Compliance e gestor do contrato. Aprovação/escalonamento: Encarregado (DPO), Comitê multidisciplinar ou Diretoria, conforme risco residual.
Evidência mínima	Registro de entrada, análise, decisão, execução e verificação; conservação em repositório oficial do PIMS ou sistema corporativo associado ao processo com acesso por necessidade.
Indicadores	Percentual de casos conformes; exceções vencidas; tempo de decisão; reincidência; cobertura de treinamento; ações corretivas no prazo.
Teste e alerta	Amostra baseada em risco e revisão após mudança. Escalar imediatamente quando houver tratamento de alto risco, dado sensível em escala, decisão automatizada relevante, transferência sem mecanismo confirmado ou incidente material.

Perguntas executivas para aprovação

- A finalidade e a necessidade de minimização, qualidade, exatidão e proveniência estão claras e permanecem válidas?
- Os riscos, pessoas afetadas, dependências, obrigações e possíveis conflitos foram avaliados?
- A evidência produzida permite demonstrar não apenas a existência, mas a efetividade do controle?
- Há condição de parada, prazo de reavaliação e responsável por corrigir eventual resultado adverso?

GATILHO DE PROJETO OU CONTRATO Em novo projeto, produto, fornecedor ou contrato, o tema minimização, qualidade, exatidão e proveniência deve integrar a avaliação de entrada. Se a resposta depender de premissa não confirmada, a aprovação será condicionada; se houver tratamento de alto risco, dado sensível em escala,

decisão automatizada relevante, transferência sem mecanismo confirmado ou incidente material, o caso seguirá para Encarregado (DPO), Comitê multidisciplinar ou Diretoria, conforme risco residual.

5.C13 Caderno de controle — privacy by design e privacy by default

LEITURA EXECUTIVA Este caderno converte o compromisso sobre privacy by design e privacy by default em uma rotina verificável. Aplica-se a toda operação com dados pessoais, inclusive projetos, contratos, sistemas, processos físicos e serviços prestados em nome de clientes e deve ser usado antes da decisão, durante a execução e na revisão de eficácia. O objetivo é permitir que qualquer leitor compreenda o que deve ser feito, quem decide, qual evidência comprova a prática e quando o tema precisa ser escalado.

Objetivo, resultado e critério de aceitação

O resultado esperado para privacy by design e privacy by default é uma decisão coerente com LGPD, sigilo profissional, ISO/IEC 27701:2025 e, quando aplicável, GDPR, baseada em risco, documentada no nível proporcional ao impacto e passível de reconstrução por terceiro independente. O controle é considerado implementado somente quando há responsável designado, critério prévio, execução demonstrável, tratamento de exceções e verificação periódica.

Aplicação operacional mínima

- Planejar: o dono do processo, com orientação do Encarregado (DPO) define finalidade, entradas, critérios, alçada, prazo e evidência necessária para privacy by design e privacy by default.
- Executar: utilizar fluxo oficial, segregação de funções e validações proporcionais; decisões sensíveis dependem de Encarregado (DPO), Comitê multidisciplinar ou Diretoria, conforme risco residual.
- Registrar: preservar solicitação, análise, aprovação, resultado, comunicação e eventual exceção em repositório oficial do PIMS ou sistema corporativo associado ao processo.
- Verificar: realizar ao menos anual e após mudança relevante, incidente ou reclamação teste de desenho e amostra de eficácia, registrando população, seleção, resultado e conclusão.
- Corrigir: desvios devem ser contidos, avaliados quanto à causa, tratados por plano com responsável e submetidos a reteste.

Elemento	Padrão verificável
Responsabilidade	Dono: dono do processo, com orientação do Encarregado (DPO). Consultados: Jurídico, Segurança da Informação, Tecnologia, Pessoas, Compliance e gestor do contrato. Aprovação/escalonamento: Encarregado (DPO), Comitê multidisciplinar ou Diretoria, conforme risco residual.
Evidência mínima	Registro de entrada, análise, decisão, execução e verificação; conservação em repositório oficial do PIMS ou sistema corporativo associado ao processo com acesso por necessidade.
Indicadores	Percentual de casos conformes; exceções vencidas; tempo de decisão; reincidência; cobertura de treinamento; ações corretivas no prazo.
Teste e alerta	Amostra baseada em risco e revisão após mudança. Escalar imediatamente quando houver tratamento de alto risco, dado sensível em escala, decisão automatizada relevante, transferência sem mecanismo confirmado ou incidente material.

Perguntas executivas para aprovação

- A finalidade e a necessidade de privacy by design e privacy by default estão claras e permanecem válidas?
- Os riscos, pessoas afetadas, dependências, obrigações e possíveis conflitos foram avaliados?
- A evidência produzida permite demonstrar não apenas a existência, mas a efetividade do controle?
- Há condição de parada, prazo de reavaliação e responsável por corrigir eventual resultado adverso?

GATILHO DE PROJETO OU CONTRATO Em novo projeto, produto, fornecedor ou contrato, o tema privacy by design e privacy by default deve integrar a avaliação de entrada. Se a resposta depender de premissa não confirmada, a aprovação será condicionada; se houver tratamento de alto risco, dado sensível em escala, decisão

automatizada relevante, transferência sem mecanismo confirmado ou incidente material, o caso seguirá para Encarregado (DPO), Comitê multidisciplinar ou Diretoria, conforme risco residual.

5.C14 Caderno de controle — triagem de risco e avaliação de impacto (AIPD/RIPD)

LEITURA EXECUTIVA Este caderno converte o compromisso sobre triagem de risco e avaliação de impacto (aipd/ripd) em uma rotina verificável. Aplica-se a toda operação com dados pessoais, inclusive projetos, contratos, sistemas, processos físicos e serviços prestados em nome de clientes e deve ser usado antes da decisão, durante a execução e na revisão de eficácia. O objetivo é permitir que qualquer leitor compreenda o que deve ser feito, quem decide, qual evidência comprova a prática e quando o tema precisa ser escalado.

Objetivo, resultado e critério de aceitação

O resultado esperado para triagem de risco e avaliação de impacto (aipd/ripd) é uma decisão coerente com LGPD, sigilo profissional, ISO/IEC 27701:2025 e, quando aplicável, GDPR, baseada em risco, documentada no nível proporcional ao impacto e passível de reconstrução por terceiro independente. O controle é considerado implementado somente quando há responsável designado, critério prévio, execução demonstrável, tratamento de exceções e verificação periódica.

Aplicação operacional mínima

- Planejar: o dono do processo, com orientação do Encarregado (DPO) define finalidade, entradas, critérios, alçada, prazo e evidência necessária para triagem de risco e avaliação de impacto (aipd/ripd).
- Executar: utilizar fluxo oficial, segregação de funções e validações proporcionais; decisões sensíveis dependem de Encarregado (DPO), Comitê multidisciplinar ou Diretoria, conforme risco residual.
- Registrar: preservar solicitação, análise, aprovação, resultado, comunicação e eventual exceção em repositório oficial do PIMS ou sistema corporativo associado ao processo.
- Verificar: realizar ao menos anual e após mudança relevante, incidente ou reclamação teste de desenho e amostra de eficácia, registrando população, seleção, resultado e conclusão.
- Corrigir: desvios devem ser contidos, avaliados quanto à causa, tratados por plano com responsável e submetidos a reteste.

Elemento	Padrão verificável
Responsabilidade	Dono: dono do processo, com orientação do Encarregado (DPO). Consultados: Jurídico, Segurança da Informação, Tecnologia, Pessoas, Compliance e gestor do contrato. Aprovação/escalonamento: Encarregado (DPO), Comitê multidisciplinar ou Diretoria, conforme risco residual.
Evidência mínima	Registro de entrada, análise, decisão, execução e verificação; conservação em repositório oficial do PIMS ou sistema corporativo associado ao processo com acesso por necessidade.
Indicadores	Percentual de casos conformes; exceções vencidas; tempo de decisão; reincidência; cobertura de treinamento; ações corretivas no prazo.
Teste e alerta	Amostra baseada em risco e revisão após mudança. Escalar imediatamente quando houver tratamento de alto risco, dado sensível em escala, decisão automatizada relevante, transferência sem mecanismo confirmado ou incidente material.

Perguntas executivas para aprovação

- A finalidade e a necessidade de triagem de risco e avaliação de impacto (aipd/ripd) estão claras e permanecem válidas?
- Os riscos, pessoas afetadas, dependências, obrigações e possíveis conflitos foram avaliados?
- A evidência produzida permite demonstrar não apenas a existência, mas a efetividade do controle?
- Há condição de parada, prazo de reavaliação e responsável por corrigir eventual resultado adverso?

GATILHO DE PROJETO OU CONTRATO Em novo projeto, produto, fornecedor ou contrato, o tema triagem de risco e avaliação de impacto (aipd/ripd) deve integrar a avaliação de entrada. Se a resposta depender de premissa não confirmada, a aprovação será condicionada; se houver tratamento de alto risco, dado sensível em

escala, decisão automatizada relevante, transferência sem mecanismo confirmado ou incidente material, o caso seguirá para Encarregado (DPO), Comitê multidisciplinar ou Diretoria, conforme risco residual.

5.C15 Caderno de controle — direitos dos titulares e autenticação proporcional

LEITURA EXECUTIVA Este caderno converte o compromisso sobre direitos dos titulares e autenticação proporcional em uma rotina verificável. Aplica-se a toda operação com dados pessoais, inclusive projetos, contratos, sistemas, processos físicos e serviços prestados em nome de clientes e deve ser usado antes da decisão, durante a execução e na revisão de eficácia. O objetivo é permitir que qualquer leitor compreenda o que deve ser feito, quem decide, qual evidência comprova a prática e quando o tema precisa ser escalado.

Objetivo, resultado e critério de aceitação

O resultado esperado para direitos dos titulares e autenticação proporcional é uma decisão coerente com LGPD, sigilo profissional, ISO/IEC 27701:2025 e, quando aplicável, GDPR, baseada em risco, documentada no nível proporcional ao impacto e passível de reconstrução por terceiro independente. O controle é considerado implementado somente quando há responsável designado, critério prévio, execução demonstrável, tratamento de exceções e verificação periódica.

Aplicação operacional mínima

- Planejar: o dono do processo, com orientação do Encarregado (DPO) define finalidade, entradas, critérios, alçada, prazo e evidência necessária para direitos dos titulares e autenticação proporcional.
- Executar: utilizar fluxo oficial, segregação de funções e validações proporcionais; decisões sensíveis dependem de Encarregado (DPO), Comitê multidisciplinar ou Diretoria, conforme risco residual.
- Registrar: preservar solicitação, análise, aprovação, resultado, comunicação e eventual exceção em repositório oficial do PIMS ou sistema corporativo associado ao processo.
- Verificar: realizar ao menos anual e após mudança relevante, incidente ou reclamação teste de desenho e amostra de eficácia, registrando população, seleção, resultado e conclusão.
- Corrigir: desvios devem ser contidos, avaliados quanto à causa, tratados por plano com responsável e submetidos a reteste.

Elemento	Padrão verificável
Responsabilidade	Dono: dono do processo, com orientação do Encarregado (DPO). Consultados: Jurídico, Segurança da Informação, Tecnologia, Pessoas, Compliance e gestor do contrato. Aprovação/escalonamento: Encarregado (DPO), Comitê multidisciplinar ou Diretoria, conforme risco residual.
Evidência mínima	Registro de entrada, análise, decisão, execução e verificação; conservação em repositório oficial do PIMS ou sistema corporativo associado ao processo com acesso por necessidade.
Indicadores	Percentual de casos conformes; exceções vencidas; tempo de decisão; reincidência; cobertura de treinamento; ações corretivas no prazo.
Teste e alerta	Amostra baseada em risco e revisão após mudança. Escalar imediatamente quando houver tratamento de alto risco, dado sensível em escala, decisão automatizada relevante, transferência sem mecanismo confirmado ou incidente material.

Perguntas executivas para aprovação

- A finalidade e a necessidade de direitos dos titulares e autenticação proporcional estão claras e permanecem válidas?
- Os riscos, pessoas afetadas, dependências, obrigações e possíveis conflitos foram avaliados?
- A evidência produzida permite demonstrar não apenas a existência, mas a efetividade do controle?
- Há condição de parada, prazo de reavaliação e responsável por corrigir eventual resultado adverso?

GATILHO DE PROJETO OU CONTRATO Em novo projeto, produto, fornecedor ou contrato, o tema direitos dos titulares e autenticação proporcional deve integrar a avaliação de entrada. Se a resposta depender de premissa não confirmada, a aprovação será condicionada; se houver tratamento de alto risco, dado sensível em escala,

decisão automatizada relevante, transferência sem mecanismo confirmado ou incidente material, o caso seguirá para Encarregado (DPO), Comitê multidisciplinar ou Diretoria, conforme risco residual.

5.C16 Caderno de controle — decisões automatizadas, perfilamento e revisão humana

LEITURA EXECUTIVA Este caderno converte o compromisso sobre decisões automatizadas, perfilamento e revisão humana em uma rotina verificável. Aplica-se a toda operação com dados pessoais, inclusive projetos, contratos, sistemas, processos físicos e serviços prestados em nome de clientes e deve ser usado antes da decisão, durante a execução e na revisão de eficácia. O objetivo é permitir que qualquer leitor compreenda o que deve ser feito, quem decide, qual evidência comprova a prática e quando o tema precisa ser escalado.

Objetivo, resultado e critério de aceitação

O resultado esperado para decisões automatizadas, perfilamento e revisão humana é uma decisão coerente com LGPD, sigilo profissional, ISO/IEC 27701:2025 e, quando aplicável, GDPR, baseada em risco, documentada no nível proporcional ao impacto e passível de reconstrução por terceiro independente. O controle é considerado implementado somente quando há responsável designado, critério prévio, execução demonstrável, tratamento de exceções e verificação periódica.

Aplicação operacional mínima

- Planejar: o dono do processo, com orientação do Encarregado (DPO) define finalidade, entradas, critérios, alçada, prazo e evidência necessária para decisões automatizadas, perfilamento e revisão humana.
- Executar: utilizar fluxo oficial, segregação de funções e validações proporcionais; decisões sensíveis dependem de Encarregado (DPO), Comitê multidisciplinar ou Diretoria, conforme risco residual.
- Registrar: preservar solicitação, análise, aprovação, resultado, comunicação e eventual exceção em repositório oficial do PIMS ou sistema corporativo associado ao processo.
- Verificar: realizar ao menos anual e após mudança relevante, incidente ou reclamação teste de desenho e amostra de eficácia, registrando população, seleção, resultado e conclusão.
- Corrigir: desvios devem ser contidos, avaliados quanto à causa, tratados por plano com responsável e submetidos a reteste.

Elemento	Padrão verificável
Responsabilidade	Dono: dono do processo, com orientação do Encarregado (DPO). Consultados: Jurídico, Segurança da Informação, Tecnologia, Pessoas, Compliance e gestor do contrato. Aprovação/escalonamento: Encarregado (DPO), Comitê multidisciplinar ou Diretoria, conforme risco residual.
Evidência mínima	Registro de entrada, análise, decisão, execução e verificação; conservação em repositório oficial do PIMS ou sistema corporativo associado ao processo com acesso por necessidade.
Indicadores	Percentual de casos conformes; exceções vencidas; tempo de decisão; reincidência; cobertura de treinamento; ações corretivas no prazo.
Teste e alerta	Amostra baseada em risco e revisão após mudança. Escalar imediatamente quando houver tratamento de alto risco, dado sensível em escala, decisão automatizada relevante, transferência sem mecanismo confirmado ou incidente material.

Perguntas executivas para aprovação

- A finalidade e a necessidade de decisões automatizadas, perfilamento e revisão humana estão claras e permanecem válidas?
- Os riscos, pessoas afetadas, dependências, obrigações e possíveis conflitos foram avaliados?
- A evidência produzida permite demonstrar não apenas a existência, mas a efetividade do controle?
- Há condição de parada, prazo de reavaliação e responsável por corrigir eventual resultado adverso?

GATILHO DE PROJETO OU CONTRATO Em novo projeto, produto, fornecedor ou contrato, o tema decisões automatizadas, perfilamento e revisão humana deve integrar a avaliação de entrada. Se a resposta depender de premissa não confirmada, a aprovação será condicionada; se houver tratamento de alto risco, dado sensível em

escala, decisão automatizada relevante, transferência sem mecanismo confirmado ou incidente material, o caso seguirá para Encarregado (DPO), Comitê multidisciplinar ou Diretoria, conforme risco residual.

5.C17 Caderno de controle — compartilhamento com clientes, autoridades e terceiros

LEITURA EXECUTIVA Este caderno converte o compromisso sobre compartilhamento com clientes, autoridades e terceiros em uma rotina verificável. Aplica-se a toda operação com dados pessoais, inclusive projetos, contratos, sistemas, processos físicos e serviços prestados em nome de clientes e deve ser usado antes da decisão, durante a execução e na revisão de eficácia. O objetivo é permitir que qualquer leitor compreenda o que deve ser feito, quem decide, qual evidência comprova a prática e quando o tema precisa ser escalado.

Objetivo, resultado e critério de aceitação

O resultado esperado para compartilhamento com clientes, autoridades e terceiros é uma decisão coerente com LGPD, sigilo profissional, ISO/IEC 27701:2025 e, quando aplicável, GDPR, baseada em risco, documentada no nível proporcional ao impacto e passível de reconstrução por terceiro independente. O controle é considerado implementado somente quando há responsável designado, critério prévio, execução demonstrável, tratamento de exceções e verificação periódica.

Aplicação operacional mínima

- Planejar: o dono do processo, com orientação do Encarregado (DPO) define finalidade, entradas, critérios, alçada, prazo e evidência necessária para compartilhamento com clientes, autoridades e terceiros.
- Executar: utilizar fluxo oficial, segregação de funções e validações proporcionais; decisões sensíveis dependem de Encarregado (DPO), Comitê multidisciplinar ou Diretoria, conforme risco residual.
- Registrar: preservar solicitação, análise, aprovação, resultado, comunicação e eventual exceção em repositório oficial do PIMS ou sistema corporativo associado ao processo.
- Verificar: realizar ao menos anual e após mudança relevante, incidente ou reclamação teste de desenho e amostra de eficácia, registrando população, seleção, resultado e conclusão.
- Corrigir: desvios devem ser contidos, avaliados quanto à causa, tratados por plano com responsável e submetidos a reteste.

Elemento	Padrão verificável
Responsabilidade	Dono: dono do processo, com orientação do Encarregado (DPO). Consultados: Jurídico, Segurança da Informação, Tecnologia, Pessoas, Compliance e gestor do contrato. Aprovação/escalonamento: Encarregado (DPO), Comitê multidisciplinar ou Diretoria, conforme risco residual.
Evidência mínima	Registro de entrada, análise, decisão, execução e verificação; conservação em repositório oficial do PIMS ou sistema corporativo associado ao processo com acesso por necessidade.
Indicadores	Percentual de casos conformes; exceções vencidas; tempo de decisão; reincidência; cobertura de treinamento; ações corretivas no prazo.
Teste e alerta	Amostra baseada em risco e revisão após mudança. Escalar imediatamente quando houver tratamento de alto risco, dado sensível em escala, decisão automatizada relevante, transferência sem mecanismo confirmado ou incidente material.

Perguntas executivas para aprovação

- A finalidade e a necessidade de compartilhamento com clientes, autoridades e terceiros estão claras e permanecem válidas?
- Os riscos, pessoas afetadas, dependências, obrigações e possíveis conflitos foram avaliados?
- A evidência produzida permite demonstrar não apenas a existência, mas a efetividade do controle?
- Há condição de parada, prazo de reavaliação e responsável por corrigir eventual resultado adverso?

GATILHO DE PROJETO OU CONTRATO Em novo projeto, produto, fornecedor ou contrato, o tema compartilhamento com clientes, autoridades e terceiros deve integrar a avaliação de entrada. Se a resposta depender de premissa não confirmada, a aprovação será condicionada; se houver tratamento de alto risco, dado

sensível em escala, decisão automatizada relevante, transferência sem mecanismo confirmado ou incidente material, o caso seguirá para Encarregado (DPO), Comitê multidisciplinar ou Diretoria, conforme risco residual.

5.C18 Caderno de controle — due diligence e contratação de operadores

LEITURA EXECUTIVA Este caderno converte o compromisso sobre due diligence e contratação de operadores em uma rotina verificável. Aplica-se a toda operação com dados pessoais, inclusive projetos, contratos, sistemas, processos físicos e serviços prestados em nome de clientes e deve ser usado antes da decisão, durante a execução e na revisão de eficácia. O objetivo é permitir que qualquer leitor compreenda o que deve ser feito, quem decide, qual evidência comprova a prática e quando o tema precisa ser escalado.

Objetivo, resultado e critério de aceitação

O resultado esperado para due diligence e contratação de operadores é uma decisão coerente com LGPD, sigilo profissional, ISO/IEC 27701:2025 e, quando aplicável, GDPR, baseada em risco, documentada no nível proporcional ao impacto e passível de reconstrução por terceiro independente. O controle é considerado implementado somente quando há responsável designado, critério prévio, execução demonstrável, tratamento de exceções e verificação periódica.

Aplicação operacional mínima

- Planejar: o dono do processo, com orientação do Encarregado (DPO) define finalidade, entradas, critérios, alçada, prazo e evidência necessária para due diligence e contratação de operadores.
- Executar: utilizar fluxo oficial, segregação de funções e validações proporcionais; decisões sensíveis dependem de Encarregado (DPO), Comitê multidisciplinar ou Diretoria, conforme risco residual.
- Registrar: preservar solicitação, análise, aprovação, resultado, comunicação e eventual exceção em repositório oficial do PIMS ou sistema corporativo associado ao processo.
- Verificar: realizar ao menos anual e após mudança relevante, incidente ou reclamação teste de desenho e amostra de eficácia, registrando população, seleção, resultado e conclusão.
- Corrigir: desvios devem ser contidos, avaliados quanto à causa, tratados por plano com responsável e submetidos a reteste.

Elemento	Padrão verificável
Responsabilidade	Dono: dono do processo, com orientação do Encarregado (DPO). Consultados: Jurídico, Segurança da Informação, Tecnologia, Pessoas, Compliance e gestor do contrato. Aprovação/escalonamento: Encarregado (DPO), Comitê multidisciplinar ou Diretoria, conforme risco residual.
Evidência mínima	Registro de entrada, análise, decisão, execução e verificação; conservação em repositório oficial do PIMS ou sistema corporativo associado ao processo com acesso por necessidade.
Indicadores	Percentual de casos conformes; exceções vencidas; tempo de decisão; reincidência; cobertura de treinamento; ações corretivas no prazo.
Teste e alerta	Amostra baseada em risco e revisão após mudança. Escalar imediatamente quando houver tratamento de alto risco, dado sensível em escala, decisão automatizada relevante, transferência sem mecanismo confirmado ou incidente material.

Perguntas executivas para aprovação

- A finalidade e a necessidade de due diligence e contratação de operadores estão claras e permanecem válidas?
- Os riscos, pessoas afetadas, dependências, obrigações e possíveis conflitos foram avaliados?
- A evidência produzida permite demonstrar não apenas a existência, mas a efetividade do controle?
- Há condição de parada, prazo de reavaliação e responsável por corrigir eventual resultado adverso?

GATILHO DE PROJETO OU CONTRATO Em novo projeto, produto, fornecedor ou contrato, o tema due diligence e contratação de operadores deve integrar a avaliação de entrada. Se a resposta depender de premissa não confirmada, a aprovação será condicionada; se houver tratamento de alto risco, dado sensível em escala, decisão

automatizada relevante, transferência sem mecanismo confirmado ou incidente material, o caso seguirá para Encarregado (DPO), Comitê multidisciplinar ou Diretoria, conforme risco residual.

5.C19 Caderno de controle — transferências internacionais e medidas suplementares

LEITURA EXECUTIVA Este caderno converte o compromisso sobre transferências internacionais e medidas suplementares em uma rotina verificável. Aplica-se a toda operação com dados pessoais, inclusive projetos, contratos, sistemas, processos físicos e serviços prestados em nome de clientes e deve ser usado antes da decisão, durante a execução e na revisão de eficácia. O objetivo é permitir que qualquer leitor compreenda o que deve ser feito, quem decide, qual evidência comprova a prática e quando o tema precisa ser escalado.

Objetivo, resultado e critério de aceitação

O resultado esperado para transferências internacionais e medidas suplementares é uma decisão coerente com LGPD, sigilo profissional, ISO/IEC 27701:2025 e, quando aplicável, GDPR, baseada em risco, documentada no nível proporcional ao impacto e passível de reconstrução por terceiro independente. O controle é considerado implementado somente quando há responsável designado, critério prévio, execução demonstrável, tratamento de exceções e verificação periódica.

Aplicação operacional mínima

- Planejar: o dono do processo, com orientação do Encarregado (DPO) define finalidade, entradas, critérios, alçada, prazo e evidência necessária para transferências internacionais e medidas suplementares.
- Executar: utilizar fluxo oficial, segregação de funções e validações proporcionais; decisões sensíveis dependem de Encarregado (DPO), Comitê multidisciplinar ou Diretoria, conforme risco residual.
- Registrar: preservar solicitação, análise, aprovação, resultado, comunicação e eventual exceção em repositório oficial do PIMS ou sistema corporativo associado ao processo.
- Verificar: realizar ao menos anual e após mudança relevante, incidente ou reclamação teste de desenho e amostra de eficácia, registrando população, seleção, resultado e conclusão.
- Corrigir: desvios devem ser contidos, avaliados quanto à causa, tratados por plano com responsável e submetidos a reteste.

Elemento	Padrão verificável
Responsabilidade	Dono: dono do processo, com orientação do Encarregado (DPO). Consultados: Jurídico, Segurança da Informação, Tecnologia, Pessoas, Compliance e gestor do contrato. Aprovação/escalonamento: Encarregado (DPO), Comitê multidisciplinar ou Diretoria, conforme risco residual.
Evidência mínima	Registro de entrada, análise, decisão, execução e verificação; conservação em repositório oficial do PIMS ou sistema corporativo associado ao processo com acesso por necessidade.
Indicadores	Percentual de casos conformes; exceções vencidas; tempo de decisão; reincidência; cobertura de treinamento; ações corretivas no prazo.
Teste e alerta	Amostra baseada em risco e revisão após mudança. Escalar imediatamente quando houver tratamento de alto risco, dado sensível em escala, decisão automatizada relevante, transferência sem mecanismo confirmado ou incidente material.

Perguntas executivas para aprovação

- A finalidade e a necessidade de transferências internacionais e medidas suplementares estão claras e permanecem válidas?
- Os riscos, pessoas afetadas, dependências, obrigações e possíveis conflitos foram avaliados?
- A evidência produzida permite demonstrar não apenas a existência, mas a efetividade do controle?
- Há condição de parada, prazo de reavaliação e responsável por corrigir eventual resultado adverso?

GATILHO DE PROJETO OU CONTRATO Em novo projeto, produto, fornecedor ou contrato, o tema transferências internacionais e medidas suplementares deve integrar a avaliação de entrada. Se a resposta depender de premissa não confirmada, a aprovação será condicionada; se houver tratamento de alto risco, dado sensível em

escala, decisão automatizada relevante, transferência sem mecanismo confirmado ou incidente material, o caso seguirá para Encarregado (DPO), Comitê multidisciplinar ou Diretoria, conforme risco residual.

5.C20 Caderno de controle — retenção, legal hold, anonimização e descarte

LEITURA EXECUTIVA Este caderno converte o compromisso sobre retenção, legal hold, anonimização e descarte em uma rotina verificável. Aplica-se a toda operação com dados pessoais, inclusive projetos, contratos, sistemas, processos físicos e serviços prestados em nome de clientes e deve ser usado antes da decisão, durante a execução e na revisão de eficácia. O objetivo é permitir que qualquer leitor compreenda o que deve ser feito, quem decide, qual evidência comprova a prática e quando o tema precisa ser escalado.

Objetivo, resultado e critério de aceitação

O resultado esperado para retenção, legal hold, anonimização e descarte é uma decisão coerente com LGPD, sigilo profissional, ISO/IEC 27701:2025 e, quando aplicável, GDPR, baseada em risco, documentada no nível proporcional ao impacto e passível de reconstrução por terceiro independente. O controle é considerado implementado somente quando há responsável designado, critério prévio, execução demonstrável, tratamento de exceções e verificação periódica.

Aplicação operacional mínima

- Planejar: o dono do processo, com orientação do Encarregado (DPO) define finalidade, entradas, critérios, alçada, prazo e evidência necessária para retenção, legal hold, anonimização e descarte.
- Executar: utilizar fluxo oficial, segregação de funções e validações proporcionais; decisões sensíveis dependem de Encarregado (DPO), Comitê multidisciplinar ou Diretoria, conforme risco residual.
- Registrar: preservar solicitação, análise, aprovação, resultado, comunicação e eventual exceção em repositório oficial do PIMS ou sistema corporativo associado ao processo.
- Verificar: realizar ao menos anual e após mudança relevante, incidente ou reclamação teste de desenho e amostra de eficácia, registrando população, seleção, resultado e conclusão.
- Corrigir: desvios devem ser contidos, avaliados quanto à causa, tratados por plano com responsável e submetidos a reteste.

Elemento	Padrão verificável
Responsabilidade	Dono: dono do processo, com orientação do Encarregado (DPO). Consultados: Jurídico, Segurança da Informação, Tecnologia, Pessoas, Compliance e gestor do contrato. Aprovação/escalonamento: Encarregado (DPO), Comitê multidisciplinar ou Diretoria, conforme risco residual.
Evidência mínima	Registro de entrada, análise, decisão, execução e verificação; conservação em repositório oficial do PIMS ou sistema corporativo associado ao processo com acesso por necessidade.
Indicadores	Percentual de casos conformes; exceções vencidas; tempo de decisão; reincidência; cobertura de treinamento; ações corretivas no prazo.
Teste e alerta	Amostra baseada em risco e revisão após mudança. Escalar imediatamente quando houver tratamento de alto risco, dado sensível em escala, decisão automatizada relevante, transferência sem mecanismo confirmado ou incidente material.

Perguntas executivas para aprovação

- A finalidade e a necessidade de retenção, legal hold, anonimização e descarte estão claras e permanecem válidas?
- Os riscos, pessoas afetadas, dependências, obrigações e possíveis conflitos foram avaliados?
- A evidência produzida permite demonstrar não apenas a existência, mas a efetividade do controle?
- Há condição de parada, prazo de reavaliação e responsável por corrigir eventual resultado adverso?

GATILHO DE PROJETO OU CONTRATO Em novo projeto, produto, fornecedor ou contrato, o tema retenção, legal hold, anonimização e descarte deve integrar a avaliação de entrada. Se a resposta depender de premissa não confirmada, a aprovação será condicionada; se houver tratamento de alto risco, dado sensível em escala, decisão

automatizada relevante, transferência sem mecanismo confirmado ou incidente material, o caso seguirá para Encarregado (DPO), Comitê multidisciplinar ou Diretoria, conforme risco residual.

5.C21 Caderno de controle — segurança de dados pessoais e segregação de acesso

LEITURA EXECUTIVA Este caderno converte o compromisso sobre segurança de dados pessoais e segregação de acesso em uma rotina verificável. Aplica-se a toda operação com dados pessoais, inclusive projetos, contratos, sistemas, processos físicos e serviços prestados em nome de clientes e deve ser usado antes da decisão, durante a execução e na revisão de eficácia. O objetivo é permitir que qualquer leitor compreenda o que deve ser feito, quem decide, qual evidência comprova a prática e quando o tema precisa ser escalado.

Objetivo, resultado e critério de aceitação

O resultado esperado para segurança de dados pessoais e segregação de acesso é uma decisão coerente com LGPD, sigilo profissional, ISO/IEC 27701:2025 e, quando aplicável, GDPR, baseada em risco, documentada no nível proporcional ao impacto e passível de reconstrução por terceiro independente. O controle é considerado implementado somente quando há responsável designado, critério prévio, execução demonstrável, tratamento de exceções e verificação periódica.

Aplicação operacional mínima

- Planejar: o dono do processo, com orientação do Encarregado (DPO) define finalidade, entradas, critérios, alçada, prazo e evidência necessária para segurança de dados pessoais e segregação de acesso.
- Executar: utilizar fluxo oficial, segregação de funções e validações proporcionais; decisões sensíveis dependem de Encarregado (DPO), Comitê multidisciplinar ou Diretoria, conforme risco residual.
- Registrar: preservar solicitação, análise, aprovação, resultado, comunicação e eventual exceção em repositório oficial do PIMS ou sistema corporativo associado ao processo.
- Verificar: realizar ao menos anual e após mudança relevante, incidente ou reclamação teste de desenho e amostra de eficácia, registrando população, seleção, resultado e conclusão.
- Corrigir: desvios devem ser contidos, avaliados quanto à causa, tratados por plano com responsável e submetidos a reteste.

Elemento	Padrão verificável
Responsabilidade	Dono: dono do processo, com orientação do Encarregado (DPO). Consultados: Jurídico, Segurança da Informação, Tecnologia, Pessoas, Compliance e gestor do contrato. Aprovação/escalonamento: Encarregado (DPO), Comitê multidisciplinar ou Diretoria, conforme risco residual.
Evidência mínima	Registro de entrada, análise, decisão, execução e verificação; conservação em repositório oficial do PIMS ou sistema corporativo associado ao processo com acesso por necessidade.
Indicadores	Percentual de casos conformes; exceções vencidas; tempo de decisão; reincidência; cobertura de treinamento; ações corretivas no prazo.
Teste e alerta	Amostra baseada em risco e revisão após mudança. Escalar imediatamente quando houver tratamento de alto risco, dado sensível em escala, decisão automatizada relevante, transferência sem mecanismo confirmado ou incidente material.

Perguntas executivas para aprovação

- A finalidade e a necessidade de segurança de dados pessoais e segregação de acesso estão claras e permanecem válidas?
- Os riscos, pessoas afetadas, dependências, obrigações e possíveis conflitos foram avaliados?
- A evidência produzida permite demonstrar não apenas a existência, mas a efetividade do controle?
- Há condição de parada, prazo de reavaliação e responsável por corrigir eventual resultado adverso?

GATILHO DE PROJETO OU CONTRATO Em novo projeto, produto, fornecedor ou contrato, o tema segurança de dados pessoais e segregação de acesso deve integrar a avaliação de entrada. Se a resposta depender de premissa não confirmada, a aprovação será condicionada; se houver tratamento de alto risco, dado sensível em

escala, decisão automatizada relevante, transferência sem mecanismo confirmado ou incidente material, o caso seguirá para Encarregado (DPO), Comitê multidisciplinar ou Diretoria, conforme risco residual.

5.C22 Caderno de controle — gestão de incidentes e avaliação de risco ao titular

LEITURA EXECUTIVA Este caderno converte o compromisso sobre gestão de incidentes e avaliação de risco ao titular em uma rotina verificável. Aplica-se a toda operação com dados pessoais, inclusive projetos, contratos, sistemas, processos físicos e serviços prestados em nome de clientes e deve ser usado antes da decisão, durante a execução e na revisão de eficácia. O objetivo é permitir que qualquer leitor compreenda o que deve ser feito, quem decide, qual evidência comprova a prática e quando o tema precisa ser escalado.

Objetivo, resultado e critério de aceitação

O resultado esperado para gestão de incidentes e avaliação de risco ao titular é uma decisão coerente com LGPD, sigilo profissional, ISO/IEC 27701:2025 e, quando aplicável, GDPR, baseada em risco, documentada no nível proporcional ao impacto e passível de reconstrução por terceiro independente. O controle é considerado implementado somente quando há responsável designado, critério prévio, execução demonstrável, tratamento de exceções e verificação periódica.

Aplicação operacional mínima

- Planejar: o dono do processo, com orientação do Encarregado (DPO) define finalidade, entradas, critérios, alçada, prazo e evidência necessária para gestão de incidentes e avaliação de risco ao titular.
- Executar: utilizar fluxo oficial, segregação de funções e validações proporcionais; decisões sensíveis dependem de Encarregado (DPO), Comitê multidisciplinar ou Diretoria, conforme risco residual.
- Registrar: preservar solicitação, análise, aprovação, resultado, comunicação e eventual exceção em repositório oficial do PIMS ou sistema corporativo associado ao processo.
- Verificar: realizar ao menos anual e após mudança relevante, incidente ou reclamação teste de desenho e amostra de eficácia, registrando população, seleção, resultado e conclusão.
- Corrigir: desvios devem ser contidos, avaliados quanto à causa, tratados por plano com responsável e submetidos a reteste.

Elemento	Padrão verificável
Responsabilidade	Dono: dono do processo, com orientação do Encarregado (DPO). Consultados: Jurídico, Segurança da Informação, Tecnologia, Pessoas, Compliance e gestor do contrato. Aprovação/escalonamento: Encarregado (DPO), Comitê multidisciplinar ou Diretoria, conforme risco residual.
Evidência mínima	Registro de entrada, análise, decisão, execução e verificação; conservação em repositório oficial do PIMS ou sistema corporativo associado ao processo com acesso por necessidade.
Indicadores	Percentual de casos conformes; exceções vencidas; tempo de decisão; reincidência; cobertura de treinamento; ações corretivas no prazo.
Teste e alerta	Amostra baseada em risco e revisão após mudança. Escalar imediatamente quando houver tratamento de alto risco, dado sensível em escala, decisão automatizada relevante, transferência sem mecanismo confirmado ou incidente material.

Perguntas executivas para aprovação

- A finalidade e a necessidade de gestão de incidentes e avaliação de risco ao titular estão claras e permanecem válidas?
- Os riscos, pessoas afetadas, dependências, obrigações e possíveis conflitos foram avaliados?
- A evidência produzida permite demonstrar não apenas a existência, mas a efetividade do controle?
- Há condição de parada, prazo de reavaliação e responsável por corrigir eventual resultado adverso?

GATILHO DE PROJETO OU CONTRATO Em novo projeto, produto, fornecedor ou contrato, o tema gestão de incidentes e avaliação de risco ao titular deve integrar a avaliação de entrada. Se a resposta depender de premissa não confirmada, a aprovação será condicionada; se houver tratamento de alto risco, dado sensível em

escala, decisão automatizada relevante, transferência sem mecanismo confirmado ou incidente material, o caso seguirá para Encarregado (DPO), Comitê multidisciplinar ou Diretoria, conforme risco residual.

5.C23 Caderno de controle — comunicação à ANPD, titulares e partes contratuais

LEITURA EXECUTIVA Este caderno converte o compromisso sobre comunicação à anpd, titulares e partes contratuais em uma rotina verificável. Aplica-se a toda operação com dados pessoais, inclusive projetos, contratos, sistemas, processos físicos e serviços prestados em nome de clientes e deve ser usado antes da decisão, durante a execução e na revisão de eficácia. O objetivo é permitir que qualquer leitor compreenda o que deve ser feito, quem decide, qual evidência comprova a prática e quando o tema precisa ser escalado.

Objetivo, resultado e critério de aceitação

O resultado esperado para comunicação à anpd, titulares e partes contratuais é uma decisão coerente com LGPD, sigilo profissional, ISO/IEC 27701:2025 e, quando aplicável, GDPR, baseada em risco, documentada no nível proporcional ao impacto e passível de reconstrução por terceiro independente. O controle é considerado implementado somente quando há responsável designado, critério prévio, execução demonstrável, tratamento de exceções e verificação periódica.

Aplicação operacional mínima

- Planejar: o dono do processo, com orientação do Encarregado (DPO) define finalidade, entradas, critérios, alçada, prazo e evidência necessária para comunicação à anpd, titulares e partes contratuais.
- Executar: utilizar fluxo oficial, segregação de funções e validações proporcionais; decisões sensíveis dependem de Encarregado (DPO), Comitê multidisciplinar ou Diretoria, conforme risco residual.
- Registrar: preservar solicitação, análise, aprovação, resultado, comunicação e eventual exceção em repositório oficial do PIMS ou sistema corporativo associado ao processo.
- Verificar: realizar ao menos anual e após mudança relevante, incidente ou reclamação teste de desenho e amostra de eficácia, registrando população, seleção, resultado e conclusão.
- Corrigir: desvios devem ser contidos, avaliados quanto à causa, tratados por plano com responsável e submetidos a reteste.

Elemento	Padrão verificável
Responsabilidade	Dono: dono do processo, com orientação do Encarregado (DPO). Consultados: Jurídico, Segurança da Informação, Tecnologia, Pessoas, Compliance e gestor do contrato. Aprovação/escalonamento: Encarregado (DPO), Comitê multidisciplinar ou Diretoria, conforme risco residual.
Evidência mínima	Registro de entrada, análise, decisão, execução e verificação; conservação em repositório oficial do PIMS ou sistema corporativo associado ao processo com acesso por necessidade.
Indicadores	Percentual de casos conformes; exceções vencidas; tempo de decisão; reincidência; cobertura de treinamento; ações corretivas no prazo.
Teste e alerta	Amostra baseada em risco e revisão após mudança. Escalar imediatamente quando houver tratamento de alto risco, dado sensível em escala, decisão automatizada relevante, transferência sem mecanismo confirmado ou incidente material.

Perguntas executivas para aprovação

- A finalidade e a necessidade de comunicação à anpd, titulares e partes contratuais estão claras e permanecem válidas?
- Os riscos, pessoas afetadas, dependências, obrigações e possíveis conflitos foram avaliados?
- A evidência produzida permite demonstrar não apenas a existência, mas a efetividade do controle?
- Há condição de parada, prazo de reavaliação e responsável por corrigir eventual resultado adverso?

GATILHO DE PROJETO OU CONTRATO Em novo projeto, produto, fornecedor ou contrato, o tema comunicação à anpd, titulares e partes contratuais deve integrar a avaliação de entrada. Se a resposta depender de premissa não confirmada, a aprovação será condicionada; se houver tratamento de alto risco, dado sensível em escala,

decisão automatizada relevante, transferência sem mecanismo confirmado ou incidente material, o caso seguirá para Encarregado (DPO), Comitê multidisciplinar ou Diretoria, conforme risco residual.

5.C24 Caderno de controle — monitoramento, auditoria e indicadores de privacidade

LEITURA EXECUTIVA Este caderno converte o compromisso sobre monitoramento, auditoria e indicadores de privacidade em uma rotina verificável. Aplica-se a toda operação com dados pessoais, inclusive projetos, contratos, sistemas, processos físicos e serviços prestados em nome de clientes e deve ser usado antes da decisão, durante a execução e na revisão de eficácia. O objetivo é permitir que qualquer leitor compreenda o que deve ser feito, quem decide, qual evidência comprova a prática e quando o tema precisa ser escalado.

Objetivo, resultado e critério de aceitação

O resultado esperado para monitoramento, auditoria e indicadores de privacidade é uma decisão coerente com LGPD, sigilo profissional, ISO/IEC 27701:2025 e, quando aplicável, GDPR, baseada em risco, documentada no nível proporcional ao impacto e passível de reconstrução por terceiro independente. O controle é considerado implementado somente quando há responsável designado, critério prévio, execução demonstrável, tratamento de exceções e verificação periódica.

Aplicação operacional mínima

- Planejar: o dono do processo, com orientação do Encarregado (DPO) define finalidade, entradas, critérios, alçada, prazo e evidência necessária para monitoramento, auditoria e indicadores de privacidade.
- Executar: utilizar fluxo oficial, segregação de funções e validações proporcionais; decisões sensíveis dependem de Encarregado (DPO), Comitê multidisciplinar ou Diretoria, conforme risco residual.
- Registrar: preservar solicitação, análise, aprovação, resultado, comunicação e eventual exceção em repositório oficial do PIMS ou sistema corporativo associado ao processo.
- Verificar: realizar ao menos anual e após mudança relevante, incidente ou reclamação teste de desenho e amostra de eficácia, registrando população, seleção, resultado e conclusão.
- Corrigir: desvios devem ser contidos, avaliados quanto à causa, tratados por plano com responsável e submetidos a reteste.

Elemento	Padrão verificável
Responsabilidade	Dono: dono do processo, com orientação do Encarregado (DPO). Consultados: Jurídico, Segurança da Informação, Tecnologia, Pessoas, Compliance e gestor do contrato. Aprovação/escalonamento: Encarregado (DPO), Comitê multidisciplinar ou Diretoria, conforme risco residual.
Evidência mínima	Registro de entrada, análise, decisão, execução e verificação; conservação em repositório oficial do PIMS ou sistema corporativo associado ao processo com acesso por necessidade.
Indicadores	Percentual de casos conformes; exceções vencidas; tempo de decisão; reincidência; cobertura de treinamento; ações corretivas no prazo.
Teste e alerta	Amostra baseada em risco e revisão após mudança. Escalar imediatamente quando houver tratamento de alto risco, dado sensível em escala, decisão automatizada relevante, transferência sem mecanismo confirmado ou incidente material.

Perguntas executivas para aprovação

- A finalidade e a necessidade de monitoramento, auditoria e indicadores de privacidade estão claras e permanecem válidas?
- Os riscos, pessoas afetadas, dependências, obrigações e possíveis conflitos foram avaliados?
- A evidência produzida permite demonstrar não apenas a existência, mas a efetividade do controle?
- Há condição de parada, prazo de reavaliação e responsável por corrigir eventual resultado adverso?

GATILHO DE PROJETO OU CONTRATO Em novo projeto, produto, fornecedor ou contrato, o tema monitoramento, auditoria e indicadores de privacidade deve integrar a avaliação de entrada. Se a resposta depender de premissa não confirmada, a aprovação será condicionada; se houver tratamento de alto risco, dado

sensível em escala, decisão automatizada relevante, transferência sem mecanismo confirmado ou incidente material, o caso seguirá para Encarregado (DPO), Comitê multidisciplinar ou Diretoria, conforme risco residual.

5.C25 Caderno de controle — capacitação por função e comprovação de ciência

LEITURA EXECUTIVA Este caderno converte o compromisso sobre capacitação por função e comprovação de ciência em uma rotina verificável. Aplica-se a toda operação com dados pessoais, inclusive projetos, contratos, sistemas, processos físicos e serviços prestados em nome de clientes e deve ser usado antes da decisão, durante a execução e na revisão de eficácia. O objetivo é permitir que qualquer leitor compreenda o que deve ser feito, quem decide, qual evidência comprova a prática e quando o tema precisa ser escalado.

Objetivo, resultado e critério de aceitação

O resultado esperado para capacitação por função e comprovação de ciência é uma decisão coerente com LGPD, sigilo profissional, ISO/IEC 27701:2025 e, quando aplicável, GDPR, baseada em risco, documentada no nível proporcional ao impacto e passível de reconstrução por terceiro independente. O controle é considerado implementado somente quando há responsável designado, critério prévio, execução demonstrável, tratamento de exceções e verificação periódica.

Aplicação operacional mínima

- Planejar: o dono do processo, com orientação do Encarregado (DPO) define finalidade, entradas, critérios, alçada, prazo e evidência necessária para capacitação por função e comprovação de ciência.
- Executar: utilizar fluxo oficial, segregação de funções e validações proporcionais; decisões sensíveis dependem de Encarregado (DPO), Comitê multidisciplinar ou Diretoria, conforme risco residual.
- Registrar: preservar solicitação, análise, aprovação, resultado, comunicação e eventual exceção em repositório oficial do PIMS ou sistema corporativo associado ao processo.
- Verificar: realizar ao menos anual e após mudança relevante, incidente ou reclamação teste de desenho e amostra de eficácia, registrando população, seleção, resultado e conclusão.
- Corrigir: desvios devem ser contidos, avaliados quanto à causa, tratados por plano com responsável e submetidos a reteste.

Elemento	Padrão verificável
Responsabilidade	Dono: dono do processo, com orientação do Encarregado (DPO). Consultados: Jurídico, Segurança da Informação, Tecnologia, Pessoas, Compliance e gestor do contrato. Aprovação/escalonamento: Encarregado (DPO), Comitê multidisciplinar ou Diretoria, conforme risco residual.
Evidência mínima	Registro de entrada, análise, decisão, execução e verificação; conservação em repositório oficial do PIMS ou sistema corporativo associado ao processo com acesso por necessidade.
Indicadores	Percentual de casos conformes; exceções vencidas; tempo de decisão; reincidência; cobertura de treinamento; ações corretivas no prazo.
Teste e alerta	Amostra baseada em risco e revisão após mudança. Escalar imediatamente quando houver tratamento de alto risco, dado sensível em escala, decisão automatizada relevante, transferência sem mecanismo confirmado ou incidente material.

Perguntas executivas para aprovação

- A finalidade e a necessidade de capacitação por função e comprovação de ciência estão claras e permanecem válidas?
- Os riscos, pessoas afetadas, dependências, obrigações e possíveis conflitos foram avaliados?
- A evidência produzida permite demonstrar não apenas a existência, mas a efetividade do controle?
- Há condição de parada, prazo de reavaliação e responsável por corrigir eventual resultado adverso?

GATILHO DE PROJETO OU CONTRATO Em novo projeto, produto, fornecedor ou contrato, o tema capacitação por função e comprovação de ciência deve integrar a avaliação de entrada. Se a resposta depender de premissa não confirmada, a aprovação será condicionada; se houver tratamento de alto risco, dado sensível em escala,

decisão automatizada relevante, transferência sem mecanismo confirmado ou incidente material, o caso seguirá para Encarregado (DPO), Comitê multidisciplinar ou Diretoria, conforme risco residual.

5.C26 Caderno de controle — gestão de exceções, riscos residuais e planos de ação

LEITURA EXECUTIVA Este caderno converte o compromisso sobre gestão de exceções, riscos residuais e planos de ação em uma rotina verificável. Aplica-se a toda operação com dados pessoais, inclusive projetos, contratos, sistemas, processos físicos e serviços prestados em nome de clientes e deve ser usado antes da decisão, durante a execução e na revisão de eficácia. O objetivo é permitir que qualquer leitor compreenda o que deve ser feito, quem decide, qual evidência comprova a prática e quando o tema precisa ser escalado.

Objetivo, resultado e critério de aceitação

O resultado esperado para gestão de exceções, riscos residuais e planos de ação é uma decisão coerente com LGPD, sigilo profissional, ISO/IEC 27701:2025 e, quando aplicável, GDPR, baseada em risco, documentada no nível proporcional ao impacto e passível de reconstrução por terceiro independente. O controle é considerado implementado somente quando há responsável designado, critério prévio, execução demonstrável, tratamento de exceções e verificação periódica.

Aplicação operacional mínima

- Planejar: o dono do processo, com orientação do Encarregado (DPO) define finalidade, entradas, critérios, alçada, prazo e evidência necessária para gestão de exceções, riscos residuais e planos de ação.
- Executar: utilizar fluxo oficial, segregação de funções e validações proporcionais; decisões sensíveis dependem de Encarregado (DPO), Comitê multidisciplinar ou Diretoria, conforme risco residual.
- Registrar: preservar solicitação, análise, aprovação, resultado, comunicação e eventual exceção em repositório oficial do PIMS ou sistema corporativo associado ao processo.
- Verificar: realizar ao menos anual e após mudança relevante, incidente ou reclamação teste de desenho e amostra de eficácia, registrando população, seleção, resultado e conclusão.
- Corrigir: desvios devem ser contidos, avaliados quanto à causa, tratados por plano com responsável e submetidos a reteste.

Elemento	Padrão verificável
Responsabilidade	Dono: dono do processo, com orientação do Encarregado (DPO). Consultados: Jurídico, Segurança da Informação, Tecnologia, Pessoas, Compliance e gestor do contrato. Aprovação/escalonamento: Encarregado (DPO), Comitê multidisciplinar ou Diretoria, conforme risco residual.
Evidência mínima	Registro de entrada, análise, decisão, execução e verificação; conservação em repositório oficial do PIMS ou sistema corporativo associado ao processo com acesso por necessidade.
Indicadores	Percentual de casos conformes; exceções vencidas; tempo de decisão; reincidência; cobertura de treinamento; ações corretivas no prazo.
Teste e alerta	Amostra baseada em risco e revisão após mudança. Escalar imediatamente quando houver tratamento de alto risco, dado sensível em escala, decisão automatizada relevante, transferência sem mecanismo confirmado ou incidente material.

Perguntas executivas para aprovação

- A finalidade e a necessidade de gestão de exceções, riscos residuais e planos de ação estão claras e permanecem válidas?
- Os riscos, pessoas afetadas, dependências, obrigações e possíveis conflitos foram avaliados?
- A evidência produzida permite demonstrar não apenas a existência, mas a efetividade do controle?
- Há condição de parada, prazo de reavaliação e responsável por corrigir eventual resultado adverso?

GATILHO DE PROJETO OU CONTRATO Em novo projeto, produto, fornecedor ou contrato, o tema gestão de exceções, riscos residuais e planos de ação deve integrar a avaliação de entrada. Se a resposta depender de premissa não confirmada, a aprovação será condicionada; se houver tratamento de alto risco, dado sensível em

escala, decisão automatizada relevante, transferência sem mecanismo confirmado ou incidente material, o caso seguirá para Encarregado (DPO), Comitê multidisciplinar ou Diretoria, conforme risco residual.

5.C27 Caderno de controle — privacidade em inteligência artificial e novas tecnologias

LEITURA EXECUTIVA Este caderno converte o compromisso sobre privacidade em inteligência artificial e novas tecnologias em uma rotina verificável. Aplica-se a toda operação com dados pessoais, inclusive projetos, contratos, sistemas, processos físicos e serviços prestados em nome de clientes e deve ser usado antes da decisão, durante a execução e na revisão de eficácia. O objetivo é permitir que qualquer leitor compreenda o que deve ser feito, quem decide, qual evidência comprova a prática e quando o tema precisa ser escalado.

Objetivo, resultado e critério de aceitação

O resultado esperado para privacidade em inteligência artificial e novas tecnologias é uma decisão coerente com LGPD, sigilo profissional, ISO/IEC 27701:2025 e, quando aplicável, GDPR, baseada em risco, documentada no nível proporcional ao impacto e passível de reconstrução por terceiro independente. O controle é considerado implementado somente quando há responsável designado, critério prévio, execução demonstrável, tratamento de exceções e verificação periódica.

Aplicação operacional mínima

- Planejar: o dono do processo, com orientação do Encarregado (DPO) define finalidade, entradas, critérios, alçada, prazo e evidência necessária para privacidade em inteligência artificial e novas tecnologias.
- Executar: utilizar fluxo oficial, segregação de funções e validações proporcionais; decisões sensíveis dependem de Encarregado (DPO), Comitê multidisciplinar ou Diretoria, conforme risco residual.
- Registrar: preservar solicitação, análise, aprovação, resultado, comunicação e eventual exceção em repositório oficial do PIMS ou sistema corporativo associado ao processo.
- Verificar: realizar ao menos anual e após mudança relevante, incidente ou reclamação teste de desenho e amostra de eficácia, registrando população, seleção, resultado e conclusão.
- Corrigir: desvios devem ser contidos, avaliados quanto à causa, tratados por plano com responsável e submetidos a reteste.

Elemento	Padrão verificável
Responsabilidade	Dono: dono do processo, com orientação do Encarregado (DPO). Consultados: Jurídico, Segurança da Informação, Tecnologia, Pessoas, Compliance e gestor do contrato. Aprovação/escalonamento: Encarregado (DPO), Comitê multidisciplinar ou Diretoria, conforme risco residual.
Evidência mínima	Registro de entrada, análise, decisão, execução e verificação; conservação em repositório oficial do PIMS ou sistema corporativo associado ao processo com acesso por necessidade.
Indicadores	Percentual de casos conformes; exceções vencidas; tempo de decisão; reincidência; cobertura de treinamento; ações corretivas no prazo.
Teste e alerta	Amostra baseada em risco e revisão após mudança. Escalar imediatamente quando houver tratamento de alto risco, dado sensível em escala, decisão automatizada relevante, transferência sem mecanismo confirmado ou incidente material.

Perguntas executivas para aprovação

- A finalidade e a necessidade de privacidade em inteligência artificial e novas tecnologias estão claras e permanecem válidas?
- Os riscos, pessoas afetadas, dependências, obrigações e possíveis conflitos foram avaliados?
- A evidência produzida permite demonstrar não apenas a existência, mas a efetividade do controle?
- Há condição de parada, prazo de reavaliação e responsável por corrigir eventual resultado adverso?

GATILHO DE PROJETO OU CONTRATO Em novo projeto, produto, fornecedor ou contrato, o tema privacidade em inteligência artificial e novas tecnologias deve integrar a avaliação de entrada. Se a resposta depender de premissa não confirmada, a aprovação será condicionada; se houver tratamento de alto risco, dado sensível em

escala, decisão automatizada relevante, transferência sem mecanismo confirmado ou incidente material, o caso seguirá para Encarregado (DPO), Comitê multidisciplinar ou Diretoria, conforme risco residual.

5.C28 Caderno de controle — análise crítica, melhoria contínua e prestação de contas

LEITURA EXECUTIVA Este caderno converte o compromisso sobre análise crítica, melhoria contínua e prestação de contas em uma rotina verificável. Aplica-se a toda operação com dados pessoais, inclusive projetos, contratos, sistemas, processos físicos e serviços prestados em nome de clientes e deve ser usado antes da decisão, durante a execução e na revisão de eficácia. O objetivo é permitir que qualquer leitor compreenda o que deve ser feito, quem decide, qual evidência comprova a prática e quando o tema precisa ser escalado.

Objetivo, resultado e critério de aceitação

O resultado esperado para análise crítica, melhoria contínua e prestação de contas é uma decisão coerente com LGPD, sigilo profissional, ISO/IEC 27701:2025 e, quando aplicável, GDPR, baseada em risco, documentada no nível proporcional ao impacto e passível de reconstrução por terceiro independente. O controle é considerado implementado somente quando há responsável designado, critério prévio, execução demonstrável, tratamento de exceções e verificação periódica.

Aplicação operacional mínima

- Planejar: o dono do processo, com orientação do Encarregado (DPO) define finalidade, entradas, critérios, alçada, prazo e evidência necessária para análise crítica, melhoria contínua e prestação de contas.
- Executar: utilizar fluxo oficial, segregação de funções e validações proporcionais; decisões sensíveis dependem de Encarregado (DPO), Comitê multidisciplinar ou Diretoria, conforme risco residual.
- Registrar: preservar solicitação, análise, aprovação, resultado, comunicação e eventual exceção em repositório oficial do PIMS ou sistema corporativo associado ao processo.
- Verificar: realizar ao menos anual e após mudança relevante, incidente ou reclamação teste de desenho e amostra de eficácia, registrando população, seleção, resultado e conclusão.
- Corrigir: desvios devem ser contidos, avaliados quanto à causa, tratados por plano com responsável e submetidos a reteste.

Elemento	Padrão verificável
Responsabilidade	Dono: dono do processo, com orientação do Encarregado (DPO). Consultados: Jurídico, Segurança da Informação, Tecnologia, Pessoas, Compliance e gestor do contrato. Aprovação/escalonamento: Encarregado (DPO), Comitê multidisciplinar ou Diretoria, conforme risco residual.
Evidência mínima	Registro de entrada, análise, decisão, execução e verificação; conservação em repositório oficial do PIMS ou sistema corporativo associado ao processo com acesso por necessidade.
Indicadores	Percentual de casos conformes; exceções vencidas; tempo de decisão; reincidência; cobertura de treinamento; ações corretivas no prazo.
Teste e alerta	Amostra baseada em risco e revisão após mudança. Escalar imediatamente quando houver tratamento de alto risco, dado sensível em escala, decisão automatizada relevante, transferência sem mecanismo confirmado ou incidente material.

Perguntas executivas para aprovação

- A finalidade e a necessidade de análise crítica, melhoria contínua e prestação de contas estão claras e permanecem válidas?
- Os riscos, pessoas afetadas, dependências, obrigações e possíveis conflitos foram avaliados?
- A evidência produzida permite demonstrar não apenas a existência, mas a efetividade do controle?
- Há condição de parada, prazo de reavaliação e responsável por corrigir eventual resultado adverso?

GATILHO DE PROJETO OU CONTRATO Em novo projeto, produto, fornecedor ou contrato, o tema análise crítica, melhoria contínua e prestação de contas deve integrar a avaliação de entrada. Se a resposta depender de premissa não confirmada, a aprovação será condicionada; se houver tratamento de alto risco, dado sensível em

escala, decisão automatizada relevante, transferência sem mecanismo confirmado ou incidente material, o caso seguirá para Encarregado (DPO), Comitê multidisciplinar ou Diretoria, conforme risco residual.

6. Potenciais Registros que podem Ser Gerados

Os registros abaixo são potenciais evidências de execução. A retenção indicada é recomendação mínima e deve ser ajustada pelo inventário de dados, tabela de temporalidade, obrigação legal, ordem de preservação, contrato e necessidade de defesa de direitos. Registros sujeitos a sigilo profissional ou legal exigem segregação e acesso por necessidade de conhecer.

Registro / Evidência	Tipo	Responsável (Área dona)	Local oficial	Proteção (mínimo)	Contém dados pessoais?	Retenção mínima (recom.)	Disposição final	Classificação	Descarte seguro	Observações de conformidade
Inventário/ROPA de tratamentos	Matriz	DPO + donos de processo	Repositório SGI/PIMS	MFA, perfis, histórico, backup	Sim	Vigência + 5 anos	Eliminar/anonimizar após prazo	Confidencial	Exclusão verificada	Revisão anual e por mudança; vincular finalidade, base, retenção e operadores.
Solicitações de titulares e respostas	Processo/registro	DPO	Sistema de chamados restrito	Acesso mínimo, criptografia e trilha	Sim	5 anos após encerramento	Eliminar com log	Confidencial	Exclusão segura	Preservar identidade, fundamento, prazos e resposta; restringir documentos comprobatórios.
RIPD, LIA e triagens	Relatório	DPO + projeto	Repositório PIMS	Controle de versão e aprovação	Possivelmente	Vida do tratamento + 5 anos	Eliminar após prescrição aplicável	Restrito	Exclusão segura	Atualizar quando mudar risco, tecnologia, dado, finalidade ou fornecedor.
Consentimentos e preferências	Log	Processo responsável	Plataforma/sistema oficial	Integridade, data/hora e versão	Sim	Vigência + 5 anos	Eliminar; manter supressão mínima	Confidencial	Exclusão segura	Registrar concessão e revogação sem reutilizar o contato.
DPA, cláusulas e diligência de operadores	Contrato/dossiê	Jurídico + Compras + DPO	ECM contratual	Perfis, assinatura e versionamento	Possivelmente	Contrato + 10 anos	Eliminar após prazo e hold	Restrito	Trituração/exclusão certificada	Incluir suboperadores, incidentes, retorno, descarte e transferências.
Registro de incidentes de dados	Dossiê	Segurança + DPO	Repositório de incidentes	Segregação, imutabilidade e logs	Sim	Mínimo 5 anos	Eliminar após prazo/hold	Altamente restrito	Exclusão criptográfica	Atender Res. CD/ANPD 15/2024; preservar cronologia, risco e decisões.
Comprovação de treinamento e aceite	Certificado/log	Pessoas + Compliance + DPO	Academy Volk	Conta individual, MFA/admin e backup	Sim	Vínculo + 5 anos	Eliminar/anonimizar	Interno	Exclusão segura	Vincular versão, conteúdo, avaliação e conclusão.
Logs de descarte e certificados	Log/certificado	TI + Gestão documental	Repositório SGI	Integridade e dupla verificação	Possivelmente	5 anos	Eliminar após prazo	Confidencial	Exclusão segura	Não reter conteúdo descartado; registrar classe, método, responsável e data.

FECHAMENTO O proprietário do documento deve verificar, na revisão anual, se os registros estão sendo produzidos, protegidos, retidos e descartados conforme definido. Lacunas devem gerar plano de ação com responsável e prazo.