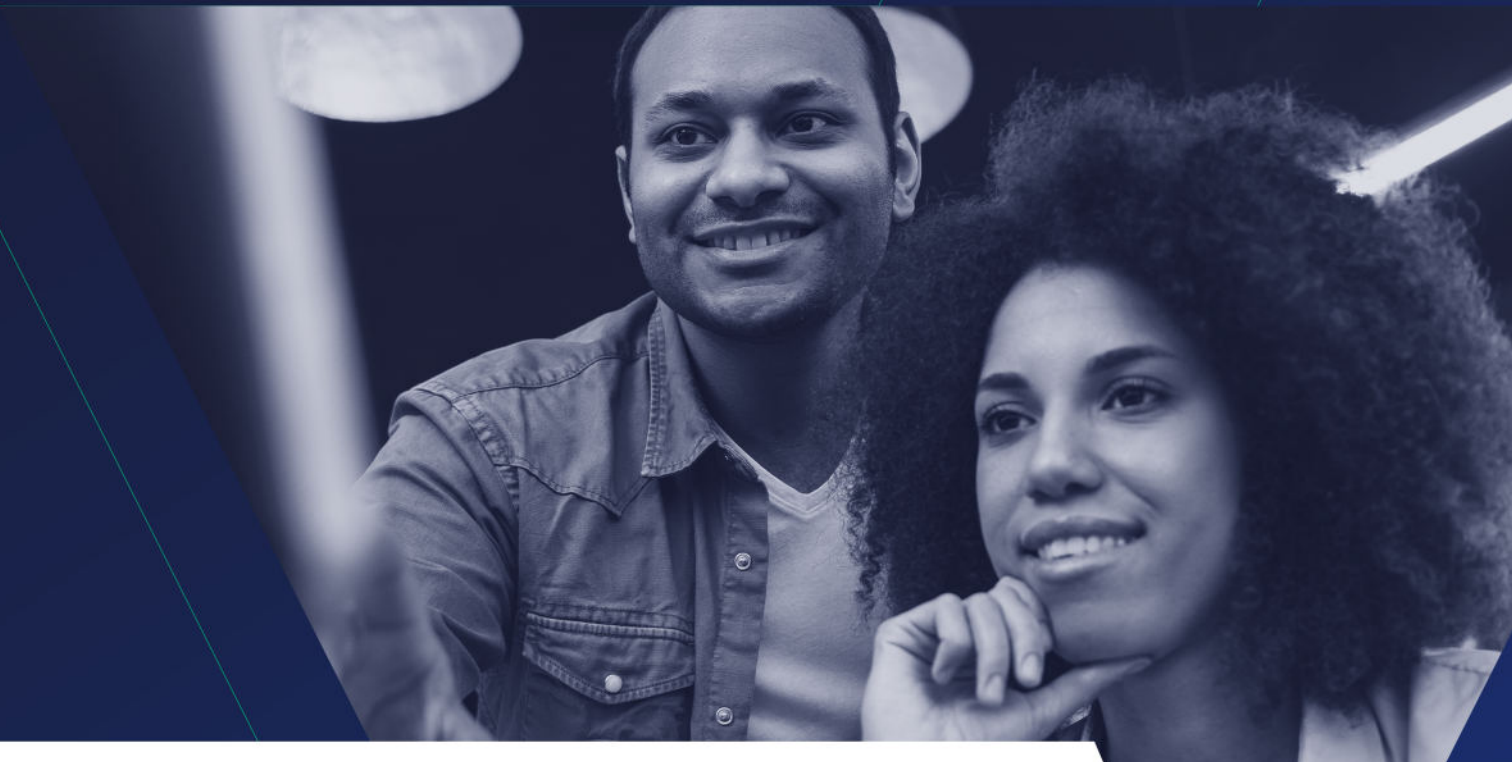
VERT ANALYTICS



POLÍTICA DE **PRIVACIDADE E PROTEÇÃO DE DADOS**

DIRETRIZES ALINHADAS À LGPD, À ISO/IEC 27001:2025, À SEGURANÇA DA INFORMAÇÃO E À PROTEÇÃO INTEGRAL.

EDIÇÃO PÚBLICA E EXECUTIVA.

ÍNDICE

POLÍTICA DE PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS 10

1. Mensagem institucional 11

2. Objetivo 11

3. Escopo e a quem está política se aplica 12

4. Identificação da Vert Analytics 13

5. Princípios de privacidade 13

6. Governança e Sistema de Gestão de Privacidade 14

7. Encarregado pelo tratamento de dados pessoais - DPO 15

8. Como os dados pessoais podem ser obtidos 16

9. Categorias de dados pessoais 17

10. Finalidades e bases legais 18

11. Dados pessoais sensíveis e biometria 19

12. Dados de crianças e adolescentes 19

13. Cookies, pixels e tecnologias similares 20

14. Inteligência artificial, perfilamento e decisões automatizadas 21

ÍNDICE

15. Compartilhamento e destinatários 22

16. Transferência internacional de dados pessoais 22

17. Armazenamento, retenção e eliminação 23

18. Segurança, privacidade desde a concepção e incidentes 24

19. Direitos dos titulares 26

20. Como exercer direitos e apresentar solicitações 27

21. Recrutamento, colaboradorese prestadores 28

22. Fornecedores, suboperadores e diligência 28

23. Redes sociais, links e sites de terceiros 29

24. Atualização, validade e interpretação 29

25. Compromissos do SGPI alinhados à ISO/IEC 27701:2025 30

26. Documentação relacionada 31

27. Referências externas 32

28. Glossário essencial 33

29. Controle de versões, aprovação e vigência 38

POLÍTICA DE PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS

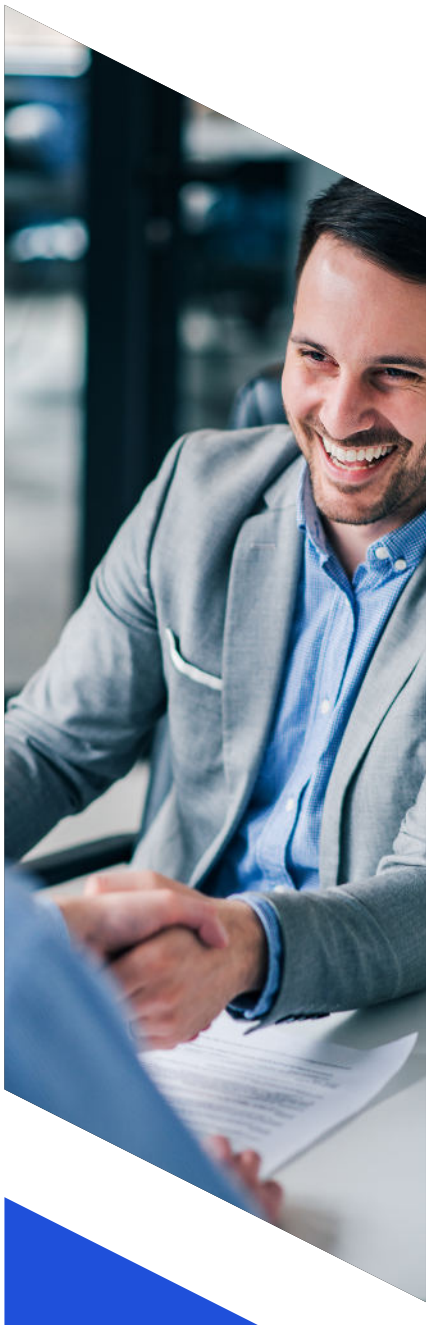
Código	POL-002	**Classificação**	Pública
Versão	1.0	**Data de emissão**	13/07/2026
Elaboração	Comitê Multidisciplinar do SGSI/SGPI e DPO	**Aprovação**	Alta Direção
Abrangência	Vert Analytics, titulares, pessoas, serviços e terceiros	**Revisão**	Anual ou por mudança relevante
Referencial	LGPD, ISO/IEC 27701:2025 e normas da ANPD	**Integração**	ISO/IEC 27001:2022 e ECA Digital
Repositório oficial	ECM institucional / Wiki.vert	**Impressão**	Cópia não controlada

Natureza desta edição

Esta Política substitui e consolida a política anteriormente divulgada no site da Vert Analytics. Ela apresenta, em linguagem acessível, como os dados pessoais são tratados em canais institucionais e como a Vert atua como controladora ou operadora. Procedimentos, inventários, avaliações de impacto, riscos, contratos e configurações técnicas permanecem em documentos internos de acesso controlado.

ENCARREGADO PELO TRATAMENTO DE DADOS PESSOAIS (DPO)

DPO titular: Cristiane Barbosa
DPO substituto: Sara de Albuquerque
Designados para atuar como ponto focal entre a Vert Analytics, os titulares e a ANPD
E-mail do DPO: dpo@vertanalytics.com.br



1. MENSAGEM INSTITUCIONAL

Na Vert Analytics, privacidade é parte da confiança entregue. Nossas atividades de inteligência artificial, análise de dados, automação, prevenção a fraudes, onboarding digital, reconhecimento facial, verificação documental e autenticação biométrica exigem responsabilidade, transparência e segurança durante todo o ciclo de vida das informações.

Esta Política demonstra o compromisso da Alta Direção com a proteção dos direitos fundamentais de liberdade, privacidade e livre desenvolvimento da personalidade. O tratamento de dados pessoais é realizado de forma proporcional aos riscos, limitado a finalidades legítimas e acompanhado por governança, controles, registros, monitoramento e melhoria contínua.

Compromisso central

Tratar dados pessoais com propósito legítimo, necessidade, transparência, segurança, prevenção, não discriminação e responsabilização, preservando os direitos dos titulares e a inovação responsável.

2. OBJETIVO

- Informar de forma clara quais dados pessoais podem ser tratados, por quais motivos, com quem podem ser compartilhados e por quanto tempo são conservados.
- Explicar os direitos dos titulares e os canais para exercício desses direitos.
- Estabelecer compromissos públicos alinhados à Lei nº 13.709/2018 (LGPD), à ISO/IEC 27701:2025 e às normas vigentes da ANPD.

- Definir a atuação da Vert Analytics como controladora, operadora ou, excepcionalmente, em situações de controladoria conjunta.
- Orientar o tratamento de dados pessoais sensíveis, biométricos, de crianças e adolescentes, bem como transferências internacionais e uso de inteligência artificial.

3. ESCOPO E A QUEM ESTÁ POLÍTICA SE APLICA

Esta Política aplica-se aos dados pessoais tratados pela Vert Analytics em seus sites, formulários, redes sociais, eventos, campanhas, comunicações, processos comerciais, atendimento, suporte, recrutamento, relacionamento com fornecedores e demais canais institucionais. Também descreve princípios aplicáveis aos serviços prestados a clientes.

Quando um cliente determina a finalidade e os meios essenciais do tratamento em uma solução operada pela Vert, o cliente normalmente será o controlador e a Vert atuará como operadora, conforme contrato e instruções documentadas. Nessas situações, o aviso de privacidade do controlador deve ser consultado pelo titular.

Atenção ao papel da Vert

O papel jurídico não é definido apenas pelo contrato ou pelo nome utilizado. Ele depende de quem efetivamente decide as finalidades e os meios essenciais de cada tratamento. Uma mesma organização pode ser controladora em uma atividade e operadora em outra.

4. IDENTIFICAÇÃO DA VERT ANALYTICS

Identificação	Informação
Razão social	Vert Analytics Ltda.
CNPJ	53.307.871/0001-19
Atuação	Soluções de inteligência artificial, análise de dados, automação, prevenção a fraudes, onboarding digital e tecnologias relacionadas.
Sede e presença	Sede em Brasília/DF, com atuação e presença institucional em outras localidades, conforme informações atualizadas no site.
Site	www.vertanalytics.com.br
Canal de privacidade	privacidade@vertanalytics.com.br
Canal do DPO	dpo@vertanalytics.com.br

5. PRINCÍPIOS DE PRIVACIDADE

- **Finalidade:** Tratamento para propósitos legítimos, específicos, explícitos e informados.
- **Adequação:** Compatibilidade entre o tratamento, a finalidade informada e o contexto.
- **Necessidade:** Limitação ao mínimo de dados e operações indispensáveis.
- **Livre acesso:** Consulta facilitada e gratuita sobre forma e duração do tratamento.
- **Qualidade dos dados:** Exatidão, clareza, relevância e atualização de acordo com a necessidade.
- **Transparência:** Informações claras, precisas e acessíveis, preservados segredos comercial e industrial.
- **Segurança:** Medidas técnicas e administrativas adequadas aos riscos.
- **Prevenção:** Adoção de medidas para evitar danos antes que ocorram.

- **Não discriminação:** Proibição de tratamento para fins discriminatórios ilícitos ou abusivos.
- **Responsabilização:** Demonstração de medidas eficazes e capacidade de prestar contas.
- **Proteção integral:** Melhor interesse e prioridade absoluta quando houver crianças e adolescentes.
- **Privacidade desde a concepção:** Requisitos incorporados a projetos, produtos, mudanças e decisões.

6. GOVERNANÇA E SISTEMA DE GESTÃO DE PRIVACIDADE

A Vert mantém um Sistema de Gestão de Privacidade da Informação (SGPI/PIMS) integrado ao Sistema de Gestão de Segurança da Informação. O modelo considera contexto, partes interessadas, riscos, obrigações, objetivos, recursos, controles, auditorias, indicadores, incidentes, análise crítica e melhoria contínua.

Papel	Responsabilidade executiva
Alta Direção	Aprovar políticas, fornecer recursos, definir prioridades, acompanhar resultados e assumir responsabilidade institucional.
Comitê Multidisciplinar SGSI/SGPI	Coordenar riscos, inventários, planos, auditorias, incidentes, documentos e ações de melhoria.
DPO titular e DPO substituto	Orientar, receber comunicações, apoiar titulares e interlocução com a ANPD, monitorar conformidade e reportar temas relevantes.
Proprietários de processos e sistemas	Definir finalidade, necessidade, acesso, retenção, compartilhamento e medidas de proteção.
Tecnologia e Segurança	Operar controles, logs, acessos, vulnerabilidades, continuidade e resposta a incidentes.
Jurídico, Contratos e Compras	Avaliar bases legais, cláusulas, responsabilidades, terceiros e transferências internacionais.
Gestão de Pessoas	Proteger dados de candidatos, colaboradores e terceiros durante todo o ciclo de relacionamento.
Todos os usuários	Usar dados somente para finalidade autorizada, proteger acessos e reportar eventos.

7. ENCARREGADO PELO TRATAMENTO DE DADOS PESSOAIS - DPO

ENCARREGADO PELO TRATAMENTO DE DADOS PESSOAIS (DPO)

DPO titular: Cristiane Barbosa
DPO substituto: Sandra Albuquerque

Designados para atuar com autonomia técnica e como canal entre a Vert Analytics, os titulares e a ANPD.

E-mail direto: dpo@vertanalytics.com.br

O DPO atua como canal de comunicação entre a Vert Analytics, os titulares e a Agência Nacional de Proteção de Dados (ANPD).

A DPO titular e o DPO substituto atuam com autonomia técnica, objetividade e tratamento adequado de eventuais conflitos de interesse. A designação do DPO não transfere nem reduz a responsabilidade dos agentes de tratamento da Alta Direção.

- Receber comunicações dos titulares, orientar seu atendimento e acompanhar os prazos.
- Receber comunicações da ANPD e adotar providências junto às áreas competentes.
- Orientar colaboradores, fornecedores e gestores sobre práticas de proteção de dados.
- Apoiar avaliações de impacto, contratos, riscos, incidentes e análise de conformidade.
- Reportar à governança riscos relevantes, lacunas, conflitos e necessidades de melhoria.

8. COMO OS DADOS PESSOAIS PODEM SER OBTIDOS

Origem	Exemplos e limites
Fornecidos diretamente	Formulários, contatos comerciais, newsletter, eventos, suporte, candidaturas, contratos, cadastros e comunicações.
Gerados pelo uso	Logs, páginas acessadas, data e hora, eventos de segurança, interações, preferências e informações técnicas.
Cookies e tecnologias similares	Identificadores, sessão, desempenho, analytics e publicidade, conforme escolhas e configuração do navegador.
Clientes controladores	Dados disponibilizados para execução de serviços contratados, conforme instruções e responsabilidades definidas.
Parceiros e fornecedores	Dados necessários ao relacionamento, execução contratual, autenticação, suporte, segurança e compliance.
Fontes públicas ou legitimamente acessíveis	Informações públicas, profissionais ou empresariais, respeitados contexto, finalidade e direitos.
Integrações e APIs	Dados recebidos de sistemas autorizados, plataformas de cliente, provedores de identidade e serviços tecnológicos.

9. CATEGORIAS DE DADOS PESSOAIS

Categoria	Exemplos
Identificação e contato	Nome, e-mail, telefone, endereço, documento, cidade, cargo, empresa e perfis profissionais.
Dados profissionais e acadêmicos	Currículo, experiência, formação, competências, referências e histórico de candidaturas.
Dados comerciais e contratuais	Empresa, função, interesse, proposta, contrato, representantes, faturamento e relacionamento.
Dados de navegação e dispositivo	IP, data e hora, navegador, sistema operacional, páginas, identificadores, sessão e eventos.
Comunicações e conteúdo	Mensagens, solicitações, gravações autorizadas, anexos, comentários, respostas e registros de suporte.
Dados de autenticação e segurança	Identificadores, logs, tentativas, permissões, tokens e evidências de segurança, sem divulgação de segredos.
Dados pessoais sensíveis	Biometria, saúde ou outros dados sensíveis apenas quando necessários, legais e adequadamente protegidos.
Dados de crianças e adolescentes	Somente quando a atividade permitir, exigir ou receber esse público, com salvaguardas reforçadas.
Dados processados por conta de clientes	Documentos, imagens, transações, cadastros, biometria, dados antifraude e outros definidos pelo controlador.

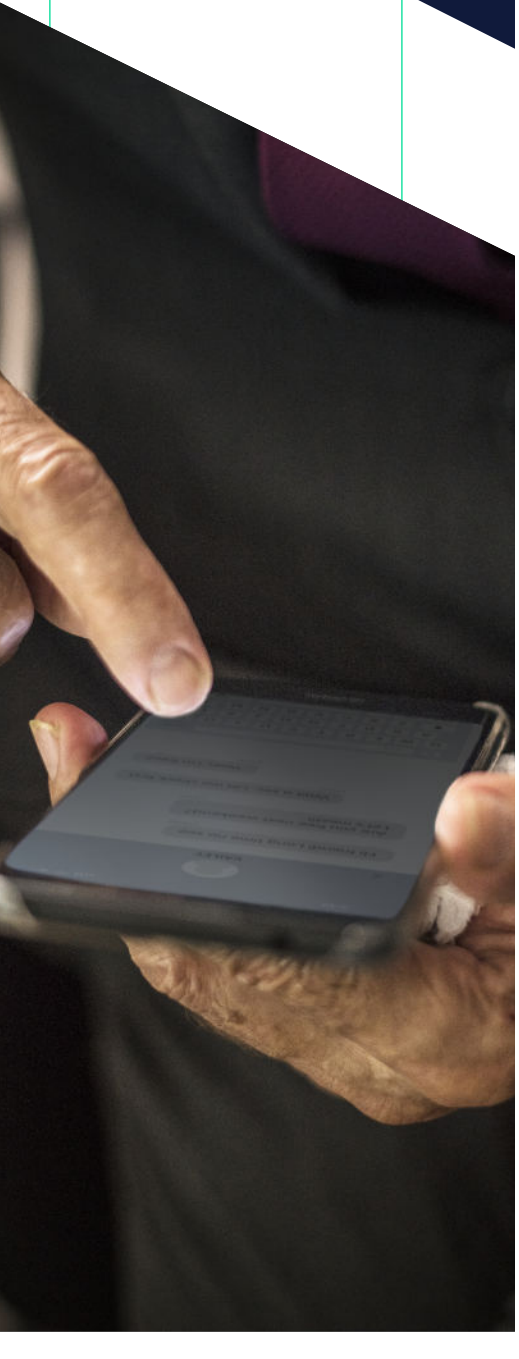
10. FINALIDADES E BASES LEGAIS

Atividade	Finalidade	Base legal típica
Contato e relacionamento comercial	Responder solicitações, elaborar propostas, organizar reuniões e acompanhar oportunidades.	Procedimentos preliminares; legítimo interesse; consentimento quando necessário.
Comunicações e marketing	Enviar conteúdos, convites, novidades e comunicações compatíveis com o relacionamento.	Consentimento ou legítimo interesse após avaliação; descadastramento disponível.
Eventos e materiais	Gerenciar inscrições, participação, certificação, entrega de conteúdo e comunicação relacionada.	Contrato/procedimentos preliminares; consentimento; legítimo interesse.
Recrutamento e seleção	Avaliar candidaturas, comunicar etapas, formar banco de talentos quando autorizado e cumprir obrigações.	Procedimentos preliminares; legítimo interesse; consentimento para retenção adicional; obrigação legal.
Execução de contratos	Entregar produtos e serviços, administrar fornecedores, faturamento, suporte, segurança e níveis de serviço.	Contrato; obrigação legal/regulatória; exercício regular de direitos.
Segurança e prevenção a fraudes	Proteger identidades, sistemas, transações, ativos, pessoas e informações.	Legítimo interesse; obrigação legal; exercício de direitos; proteção ao crédito; bases do art. 11 quando envolver sensíveis.
Cumprimento legal e regulatório	Atender leis, autoridades, auditorias, fiscalização, obrigações fiscais e decisões.	Obrigação legal ou regulatória; exercício regular de direitos.
Gestão, auditoria e melhoria	Avaliar desempenho, qualidade, segurança, riscos, incidentes e melhoria de processos.	Legítimo interesse; obrigação contratual; exercício regular de direitos.
Serviços para clientes	Processar dados conforme finalidade e instruções do controlador.	Base legal definida pelo controlador; contrato de operador e instruções documentadas.

A base legal depende do contexto

A lista apresenta bases normalmente aplicáveis, mas a base definitiva é registrada no inventário de tratamento e pode variar conforme o titular, o dado, a finalidade, o contrato e o papel exercido pela Vert. O consentimento não é utilizado quando outra base legal mais adequada sustenta o tratamento.

11. DADOS PESSOAIS SENSÍVEIS E BIOMETRIA



Dados pessoais sensíveis recebem proteção reforçada. A Vert pode tratar biometria, imagens faciais, informações de saúde ou outras categorias sensíveis quando a solução contratada ou a atividade legítima exigir, observadas finalidade, necessidade, controle de acesso, segurança, registro e base legal do art. 11 da LGPD.

Biometria e autenticação: podem ser utilizadas em processos de identificação, autenticação, onboarding e prevenção a fraudes, observados os direitos e liberdades fundamentais.

Minimização: templates, vetores ou características derivadas devem ser preferidos quando tecnicamente adequados, evitando cópias desnecessárias da imagem original.

Teste e desenvolvimento: dados reais sensíveis devem ser evitados, mascarados, anonimizados ou formalmente autorizados.

Acesso e retenção: são limitados a pessoas e sistemas autorizados, pelo tempo necessário e conforme contrato e matriz de temporalidade.

Decisão e revisão: resultados biométricos ou de risco não devem ser tratados como infalíveis e exigem controles contra falsos positivos, vieses e uso indevido.

12. DADOS DE CRIANÇAS E ADOLESCENTES

A Vert Analytics não direciona, em regra, seus canais institucionais e comunicações comerciais a crianças. Contudo, determinadas soluções tecnológicas, projetos de clientes ou interações podem envolver crianças e adolescentes. Nesses casos, o tratamento deve observar seu melhor interesse, proteção integral, prioridade absoluta, desenvolvimento progressivo e linguagem apropriada.

- A finalidade deve ser clara, legítima e compatível com o melhor interesse da criança ou do adolescente.
- Podem ser utilizadas as hipóteses legais previstas nos arts. 7º ou 11 da LGPD, conforme interpretação vigente da ANPD, sempre com avaliação do melhor interesse.
- Quando o consentimento for a base aplicável para dados de criança, ele será específico, destacado e obtido de pelo menos um responsável legal, com esforços razoáveis de verificação.
- Serão evitados coleta excessiva, exposição pública, incentivo à entrega de dados e mecanismos de design manipulativo.
- Não serão realizados perfilamento comportamental ou publicidade comercial direcionada a crianças e adolescentes quando vedados pela legislação aplicável.
- Mecanismos de aferição de idade, quando exigidos, deverão ser proporcionais, confiáveis, minimamente invasivos e não utilizados para finalidades incompatíveis.
- Projetos ou plataformas de acesso provável por esse público serão avaliados também à luz do ECA Digital e da regulamentação vigente.
- Solicitações de responsáveis serão avaliadas respeitando direitos, segurança e autonomia progressiva do titular.

Proteção reforçada

Dados de crianças e adolescentes são considerados de maior vulnerabilidade na análise de riscos, incidentes, avaliações de impacto, desenho de interfaces, transparência, retenção e escolha de fornecedores.

13. COOKIES, PIXELS E TECNOLOGIAS SIMILARES

Categoria	Finalidade	Tratamento
Estritamente necessários	Permitem segurança, navegação, sessão, formulários e funcionalidades essenciais.	Ativos quando indispensáveis ao funcionamento.
Preferências	Memorizam escolhas de idioma, região, interface ou outras opções.	Conforme escolha ou configuração do usuário.
Medição e desempenho	Ajudam a compreender utilização, erros, desempenho e melhoria.	Ativados conforme mecanismo de consentimento ou base aplicável.
Publicidade e conversão	Medem campanhas, limitam repetição e apoiam comunicações relevantes.	Dependem de escolha e controles aplicáveis; podem ser desativados.

O usuário pode gerenciar preferências por meio do banner ou centro de cookies, quando disponível, e das configurações do navegador. A desativação de cookies essenciais pode impedir funcionalidades. A lista de provedores, duração e finalidades pode ser atualizada no painel específico do site.

14. INTELIGÊNCIA ARTIFICIAL, PERFILAMENTO E DECISÕES AUTOMATIZADAS

A Vert desenvolve e utiliza soluções analíticas e de inteligência artificial. Dados pessoais podem ser processados para classificação, extração de informações, detecção de anomalias, prevenção a fraudes, apoio à decisão, automação e melhoria de serviços, conforme o papel exercido e a finalidade legítima.

- O uso de dados pessoais em modelos, prompts, bases de treinamento, teste ou validação deve ser autorizado, necessário e protegido.
- Dados de clientes não são utilizados para treinar modelos para finalidade própria incompatível sem previsão jurídica e contratual adequada.
- Resultados automatizados são submetidos a controles de qualidade, segurança, explicabilidade proporcional e revisão humana quando necessária.
- O titular pode solicitar revisão de decisão tomada unicamente com base em tratamento automatizado que afete seus interesses, nos termos aplicáveis da LGPD.
- Serão adotadas medidas para reduzir discriminação, vieses indevidos, alucinações, exposição de dados e inferências abusivas.
- Informações sobre critérios e procedimentos podem ser fornecidas na medida legalmente aplicável, preservados segredos comercial e industrial.

15. COMPARTILHAMENTO E DESTINATÁRIOS

Destinatário	Condição e finalidade
Empresas do grupo ou afiliadas	Quando necessário para atividades legítimas, gestão, suporte ou integração, com controles e responsabilidades.
Provedores de tecnologia e nuvem	Hospedagem, comunicação, segurança, analytics, suporte, armazenamento e infraestrutura.
Parceiros e fornecedores	Execução de contrato, evento, marketing autorizado, recrutamento, consultoria, auditoria e operações.
Clientes controladores	Disponibilização de dados e resultados tratados em seu nome e conforme suas instruções.
Autoridades e órgãos públicos	Cumprimento de obrigação, requisição válida, ordem ou defesa de direitos.
Operações societárias	Auditoria e reorganização, investimento, aquisição, incorporação ou transação, com salvaguardas.
Entidades de certificação e auditoria	Demonstração de conformidade, preservando minimização, confidencialidade e necessidade.

A Vert não comercializa dados pessoais como atividade de venda de listas. Compartilhamentos são limitados à finalidade, regidos por contratos, confidencialidade, segurança, instruções e avaliação de risco quando aplicável.

16. TRANSFERÊNCIA INTERNACIONAL DE DADOS PESSOAIS

Alguns fornecedores, serviços de nuvem, suporte, comunicação, segurança, modelos de inteligência artificial ou empresas relacionadas podem operar fora do Brasil ou permitir acesso internacional. Essas operações são avaliadas e formalizadas conforme a LGPD e o Regulamento de Transferência Internacional de Dados da ANPD.

Mecanismos: decisão de adequação, cláusulas-padrão contratuais da ANPD, cláusulas específicas aprovadas, normas corporativas globais ou outras hipóteses legais aplicáveis.

Avaliação: natureza e volume dos dados, país de destino, destinatário, suboperadores, legislação local, acesso governamental, segurança e possibilidade de transferência posterior.

Contratos: obrigações de finalidade, segurança, incidentes, direitos, subcontratação, retorno, eliminação e cooperação são estabelecidas nos instrumentos aplicáveis.

Transparência: informações adicionais sobre países, destinatários e mecanismos podem ser solicitadas ao canal de privacidade, respeitados contratos e segredos legítimos.

Transferência posterior: o importador não deve repassar dados a outro destinatário sem garantia de proteção equivalente e autorização exigida.

Regra prática

O simples uso de nuvem ou de serviço global não dispensa análise. A Vert registra os fluxos internacionais e seleciona o mecanismo adequado antes de transferir ou permitir acesso a dados pessoais fora do Brasil.

17. ARMAZENAMENTO, RETENÇÃO E ELIMINAÇÃO

Os dados podem ser armazenados em ambientes próprios ou de fornecedores contratados, no Brasil ou no exterior, conforme requisitos de segurança, contrato, continuidade e transferência internacional. Não é adotado um único prazo para todos os dados: a retenção depende da finalidade, base legal, contrato, risco e obrigação aplicável.

Categoria	Critério de retenção
Dados de contato e marketing	Durante o relacionamento, até oposição, descadastramento ou fim da finalidade, preservados registros mínimos de preferência.
Propostas e relacionamento comercial	Pelo período necessário à negociação, histórico e defesa de direitos.
Contratos, fiscais e financeiros	Conforme prazos legais, regulatórios e de exercício de direitos.
Currículos e candidaturas	Durante o processo e, se autorizado ou sustentado por base adequada, por período definido para futuras vagas.
Logs e segurança	Pelo período necessário à segurança, auditoria, investigação, obrigação legal e matriz de temporalidade.
Dados processados para clientes	Conforme contrato e instruções do controlador, inclusive devolução ou eliminação ao término.
Incidentes e direitos	Pelo período necessário à apuração, prestação de contas, comunicação e defesa de direitos.

Encerrada a finalidade e ausente obrigação ou fundamento de conservação, os dados são eliminados, anonimizados ou mantidos de forma restrita. Backups seguem ciclos de retenção e descarte, sem reintrodução para uso ordinário.

18. SEGURANÇA, PRIVACIDADE DESDE A CONCEPÇÃO E INCIDENTES

A Vert aplica medidas administrativas, físicas e técnicas proporcionais aos riscos, integradas à POL-001 - Política de Segurança da Informação. Nenhum ambiente é absolutamente imune, mas a organização mantém prevenção, detecção, resposta, recuperação, registros, testes e melhoria contínua.

- Gestão de identidades, menor privilégio, segregação de funções e autenticação reforçada.
- Criptografia e proteção de comunicações, endpoints, nuvem, bancos, backups e segredos.

- Logs, monitoramento, gestão de vulnerabilidades, configuração, mudanças e desenvolvimento seguro.
- Classificação, mascaramento, prevenção de vazamento e minimização de dados.
- Avaliações de impacto, riscos, fornecedores, continuidade e testes de recuperação.
- Treinamento, termos de confidencialidade, trabalho remoto e resposta a incidentes.

Quando um incidente com dados pessoais puder acarretar risco ou dano relevante, a Vert, na condição de controladora, avaliará e realizará as comunicações à ANPD e aos titulares no prazo regulatório aplicável, atualmente de três dias úteis a partir do conhecimento, ressalvada legislação específica. Como operadora, informará o controlador sem demora injustificada e prestará as informações necessárias.

19. DIREITOS DOS TITULARES

Direito	O que significa
Confirmação e acesso	Saber se existe tratamento e obter acesso aos dados e informações pertinentes.
Correção	Solicitar atualização de dados incompletos, inexatos ou desatualizados.
Anonimização, bloqueio ou eliminação	Requerer tratamento de dados desnecessários, excessivos ou em desconformidade.
Portabilidade	Solicitar portabilidade, quando regulamentada e tecnicamente aplicável, preservados segredos.
Informação sobre compartilhamento	Conhecer entidades públicas e privadas com as quais houve uso compartilhado.
Informação sobre consentimento	Conhecer a possibilidade de negar consentimento e suas consequências.
Revogação do consentimento	Retirar consentimento com procedimento facilitado, sem afetar tratamentos anteriores válidos.
Oposição	Opor-se a tratamento baseado em hipótese distinta de consentimento em caso de descumprimento da LGPD.
Revisão de decisão automatizada	Solicitar revisão e informações sobre critérios, quando aplicável.
Petição e reclamação	Peticionar perante a ANPD e exercer direitos perante órgãos de defesa competentes.
Eliminação de dados tratados com consentimento	Solicitar a eliminação dos dados tratados com base no consentimento, ressalvadas as hipóteses legais de conservação.

20. COMO EXERCER DIREITOS E APRESENTAR SOLICITAÇÕES

ENCARREGADO PELO TRATAMENTO DE DADOS PESSOAIS (DPO)

DPO titular: Cristiane Barbosa
DPO substituto: Sara de Albuquerque
Designados para atuar com autonomia técnica e como canal entre a Vert Analytics, titulares e a ANPD.

E-mail direto: dpo@vertanalytics.com.br

- Envie a solicitação ao canal do DPO ou ao e-mail privacidade@vertanalytics.com.br.
- Informe nome, meio de contato, direito pretendido e contexto suficiente para localizar o tratamento.
- A Vert poderá solicitar confirmação de identidade proporcional ao risco, evitando coleta excessiva.
- Quando a Vert atuar como operadora, a solicitação será encaminhada ou orientada ao controlador responsável, sem impedir assistência contratual.
- A resposta será fornecida de forma clara, segura e dentro dos prazos legais ou regulatórios aplicáveis.
- Pedidos manifestamente infundados, abusivos ou que afetem direitos de terceiros serão avaliados e fundamentados.

Sem custo e sem retaliação

O exercício regular de direitos é gratuito e não deve resultar em tratamento discriminatório. Custos excepcionais só serão considerados quando permitidos pela legislação.

21. RECRUTAMENTO, COLABORADORES E PRESTADORES

Dados de candidatos, colaboradores, administradores, estagiários, prestadores e dependentes são tratados para recrutamento, admissão, gestão contratual, benefícios, segurança, acesso, desempenho, capacitação, obrigações legais, saúde e segurança ocupacional, defesa de direitos e encerramento do vínculo.

- Acesso restrito às áreas e fornecedores que necessitem dos dados.
- Verificações prévias proporcionais à função, à legislação e ao risco.
- Dados sensíveis tratados apenas quando necessários e com salvaguardas reforçadas.
- Monitoramento corporativo realizado com finalidade legítima, transparência e proporcionalidade.
- Currículos não selecionados eliminados ou mantidos por período definido quando houver autorização ou base legal.
- Obrigações de confidencialidade e proteção permanecem após o término, quando aplicável.

22. FORNECEDORES, SUBOPERADORES E DILIGÊNCIA

Terceiros que tratem dados pessoais são avaliados conforme criticidade, acesso, localização, subcontratação, segurança, continuidade e capacidade de atender direitos e incidentes. Contratos definem papel, finalidade, instruções, confidencialidade, medidas de segurança, transferências, auditoria, retorno e eliminação.

Suboperadores: a contratação deve observar autorização e condições previstas no contrato com o controlador.

Mudanças relevantes: alterações de serviço, localização, escopo ou subcontratação podem exigir reavaliação.

Evidências: certificações, auditorias, relatórios, testes ou questionários podem ser solicitados de forma proporcional.

Encerramento: acessos são revogados e dados são devolvidos, eliminados ou mantidos apenas quando houver obrigação.

23. REDES SOCIAIS, LINKS E SITES DE TERCEIROS

Os canais da Vert podem conter links, widgets ou integrações de terceiros. O acesso a esses ambientes está sujeito às políticas e práticas do respectivo responsável. A Vert seleciona fornecedores e parceiros de forma diligente, mas não controla tratamentos independentes realizados por terceiros fora de suas instruções.

Interações públicas em redes sociais podem ficar visíveis a outros usuários. Evite publicar dados pessoais sensíveis, credenciais, documentos ou informações confidenciais nesses canais.

24. ATUALIZAÇÃO, VALIDADE E INTERPRETAÇÃO

Esta Política poderá ser atualizada para refletir mudanças legais, regulatórias, tecnológicas, contratuais, de serviços ou de governança. A versão vigente, data e alterações relevantes serão disponibilizadas

no canal institucional. Mudanças que exijam nova manifestação do titular serão tratadas por mecanismo adequado.

A Política é interpretada segundo a legislação brasileira, sem limitar direitos do titular, competências da ANPD, órgãos de defesa do consumidor ou jurisdições legalmente competentes. Caso uma disposição seja inválida, as demais permanecerão vigentes na medida permitida.

25. COMPROMISSOS DO SGPI ALINHADOS À ISO/IEC 27701:2025

A ISO/IEC 27701:2025 estabelece requisitos e orientações para criar, implementar, manter e melhorar continuamente um Sistema de Gestão de Privacidade da Informação, aplicável a controladores e operadores. A Vert utiliza a norma como referência de governança, sem reproduzir seu conteúdo protegido.

Tema do SGPI	Aplicação executiva
Contexto e escopo	Identificar atividades, partes interessadas, requisitos, fronteiras, papéis e dependências.
Liderança e política	Demonstrar compromisso, aprovar diretrizes, atribuir autoridade e integrar privacidade ao negócio.
Riscos e oportunidades	Avaliar impactos sobre titulares e riscos organizacionais, definindo tratamento e aceitação.
Objetivos e planejamento	Estabelecer metas mensuráveis, responsáveis, prazos, recursos e indicadores.
Competência e conscientização	Treinar pessoas conforme função, risco e mudanças, registrando eficácia.
Informação documentada	Controlar políticas, procedimentos, registros, inventários, contratos e evidências.
Inventário e registros de tratamento	Manter ROPA, mapa de dados, finalidades, bases, categorias, destinatários e retenção.
Privacidade desde a concepção	Integrar requisitos a projetos, aquisições, mudanças, IA, nuvem e desenvolvimento.
Controlador e operador	Definir responsabilidades, instruções, transparência, assistência, suboperadores e encerramento.

Direitos e transparência	Oferecer informações acessíveis e processos eficazes para solicitações.
Terceiros e transferências	Avaliar fornecedores, contratos, localização, mecanismos internacionais e cadeia de tratamento.
Segurança e incidentes	Prevenir, detectar, responder, comunicar, aprender e demonstrar medidas proporcionais.
Monitoramento e auditoria	Avaliar desempenho, conformidade, riscos, indicadores e eficácia de controles.
Análise crítica e melhoria	Tratar não conformidades, causas, ações corretivas e oportunidades de evolução.

26. DOCUMENTAÇÃO RELACIONADA

Documento/artefato	Finalidade
POL-001	Política de Segurança da Informação.
MR-001	Matriz de Riscos de Segurança da Informação e Privacidade.
SoA / Matriz GAP	Declaração de Aplicabilidade e avaliação de conformidade ISO/IEC 27001 e ISO/IEC 27701.
ROPA	Registro das operações de tratamento de dados pessoais.
Mapa de Dados LGPD	Fluxos, sistemas, origens, destinatários, bases e localizações.
AIPD/DPIA	Avaliações de impacto e salvaguardas para tratamentos de maior risco.
Matriz de Temporalidade	Critérios de retenção, arquivamento, bloqueio e eliminação.
Matriz RACI	Papéis e responsabilidades do SGSI/SGPI.

PCN e PRD	Continuidade de negócios e recuperação de serviços e dados.
Plano de Resposta a Incidentes	Detecção, classificação, contenção, comunicação e aprendizado.
Gestão de Fornecedores	Due diligence, contratos, monitoramento, suboperadores e encerramento.
Procedimentos, SIPOCs e formulários	Detalhamento operacional e registros controlados no ECM.

27. REFERÊNCIAS EXTERNAS

Lei nº 13.709/2018 - LGPD. Acessar referência

ISO/IEC 27701:2025. Acessar referência

ISO/IEC 27001:2022. Acessar referência

Regulamentações da ANPD. Acessar referência

Transferência Internacional de Dados - ANPD. Acessar referência

Comunicação de Incidentes de Segurança - ANPD. Acessar referência

ECA Digital - ANPD. [Acessar referência]

Site institucional da Vert Analytics. [Acessar referência]

Nota sobre normas técnicas

Esta Política contém interpretação executiva própria. Ela não substitui a aquisição e leitura autorizada da ISO/IEC 27701:2025, nem reproduz integralmente requisitos ou orientações protegidas por direitos autorais.

28. GLOSSÁRIO ESSENCIAL

Termo	Definição
ANPD	Agência Nacional de Proteção de Dados.
Controlador	Agente a quem competem as decisões sobre finalidades e meios essenciais do tratamento.
Operador	Agente que realiza tratamento em nome do controlador e segundo suas instruções.
Dado pessoal	Informação relacionada a pessoa natural identificada ou identificável.
Dado pessoal sensível	Dado sobre origem racial ou étnica, convicção religiosa, opinião política, filiação, saúde, vida sexual, genética ou biometria, quando vinculado a pessoa.
DPO/Encarregado	Canal de comunicação e função de apoio à governança de proteção de dados.
Incidente de segurança	Evento confirmado que compromete confidencialidade, integridade, disponibilidade ou autenticidade de dados pessoais.
PII	Personally Identifiable Information; termo internacional equivalente, em contexto, a dados pessoais.
PIMS/SGPI	Sistema de Gestão de Privacidade da Informação.
ROPA	Registro das operações de tratamento de dados pessoais.
Suboperador	Terceiro contratado por operador para tratar dados em nome do controlador.
Titular	Pessoa natural a quem os dados pessoais se referem.
Tratamento	Qualquer operação realizada com dados pessoais, da coleta à eliminação.
Transferência internacional	Transferência ou disponibilização de dados a agente localizado em outro país ou organismo internacional.

ANEXO I - ATUAÇÃO DA VERT ANALYTICS COMO CONTROLADORA

A Vert atua como controladora quando decide a finalidade e os meios essenciais do tratamento. Exemplos típicos estão abaixo e devem ser confirmados no ROPA e nos avisos específicos.

Tratamento típico	Decisão e finalidade
Site, formulários e contato	Gerenciar acesso, solicitações, segurança, comunicação e relacionamento.
Marketing e eventos	Definir públicos, conteúdo, preferências, inscrição e avaliação de campanhas.
Recrutamento e pessoas	Selecionar, contratar, administrar vínculo, benefícios, segurança e obrigações.
Fornecedores e parceiros	Contratar, avaliar, pagar, controlar acessos e cumprir obrigações.
Gestão corporativa	Auditoria, governança, riscos, qualidade, compliance e exercício de direitos.
Segurança dos ambientes	Definir logs, controles de acesso, prevenção, investigação e continuidade.
Produtos próprios	Quando a Vert definir finalidade própria e relação direta com o titular.

Como controladora, a Vert compromete-se a:

- Definir e registrar finalidade, base legal, necessidade, categorias, destinatários e retenção.
- Fornecer transparência adequada e manter canais de atendimento.
- Avaliar riscos, realizar AIPD/DPIA quando apropriado e aplicar privacidade desde a concepção.
- Atender direitos e manter evidências das decisões e respostas.
- Selecionar operadores e transferências com garantias adequadas.
- Comunicar incidentes relevantes à ANPD e aos titulares, quando exigido.
- Revisar tratamentos, eliminar dados e corrigir não conformidades.

ANEXO II - ATUAÇÃO DA VERT ANALYTICS COMO OPERADORA

A Vert atua como operadora quando processa dados pessoais em nome de um cliente controlador, conforme contrato e instruções documentadas. Isso pode ocorrer em soluções de analytics, automação, onboarding digital, biometria, prevenção a fraudes, tratamento documental, suporte, hospedagem ou integração.

Obrigação da operadora	Aplicação na Vert
Instruções	Tratar apenas conforme instruções lícitas e documentadas do controlador; alertar sobre instrução aparentemente incompatível.
Finalidade própria	Não utilizar dados do cliente para finalidade própria incompatível; qualquer papel adicional deve ser definido e legitimado.
Confidencialidade	Limitar acesso a pessoas autorizadas e sujeitas a deveres de confidencialidade.
Segurança	Aplicar medidas proporcionais e manter evidências operacionais adequadas.
Suboperadores	Contratar conforme autorização e impor obrigações equivalentes.
Direitos	Apoiar o controlador na localização, acesso, correção, exclusão, oposição e revisão, conforme contrato.
AIPD e consultas	Fornecer informações necessárias para avaliações e consultas do controlador.
Incidentes	Informar o controlador sem demora injustificada e apoiar avaliação, contenção e comunicação.
Transferências	Observar localização, mecanismos e instruções contratuais.
Auditoria	Disponibilizar informações e permitir verificações proporcionais, preservando segurança de outros clientes.
Encerramento	Devolver ou eliminar dados e cópias conforme instruções, ressalvadas obrigações legais.
Registros	Manter evidências das operações sob sua responsabilidade e cooperação com autoridades por meio do controlador.

Limite de responsabilidade

O controlador permanece responsável por definir finalidade, base legal, transparência, atendimento ao titular e legalidade das instruções. A Vert responde por suas próprias obrigações como operadora e pelos tratamentos em que assuma efetivamente decisões de controladora.

ANEXO III - MATRIZ DE RESPONSABILIDADES: CONTROLADOR, OPERADORA E DPO

Tema	Controlador	Vert como operadora	DPO
Definir finalidade e base legal	Responsável	Segue e valida instruções	Orienta e monitora
Aviso de privacidade ao titular	Responsável	Apoia quando solicitado	Revisa e orienta
Coleta e minimização	Define requisitos	Implementa no serviço	Avalia riscos
Contrato de tratamento	Contrata e instrui	Cumpre e evidencia	Orienta
Atendimento de direitos	Decide e responde	Apoia operacionalmente	Canal e monitoramento
AIPD/DPIA	Coordena	Fornece informações	Orienta e acompanha
Segurança	Define requisitos e supervisiona	Implementa no escopo	Monitora governança
Incidente	Avalia e comunica	Notifica e apoia	Orienta e articula
Suboperador	Autoriza conforme contrato	Seleciona e contrata	Avalia governança
Transferência internacional	Autoriza e define mecanismo	Implementa salvaguardas	Orienta
Retenção e eliminação	Define prazos	Executa instruções	Monitora conformidade
Auditoria e evidências	Supervisiona	Disponibiliza evidências	Acompanha
Comunicação com ANPD	Responsável legal	Apoia por meio do controlador	Canal e orientação

ANEXO IV - GUIA RÁPIDO PARA SOLICITAÇÃO DE DIREITOS

Etapa	Ação	Orientação
1	Identifique o canal	Use dpo@vertanalytics.com.br ou privacidade@vertanalytics.com.br.
2	Explique o pedido	Informe o direito, o contexto, o serviço ou o relacionamento relacionado.
3	Confirme a identidade	Forneça apenas os dados solicitados para validação proporcional e segura.
4	Aguarde a triagem	A Vert verificará se atua como controladora ou operadora e direcionará o tratamento.
5	Receba a resposta	A resposta será enviada por canal seguro, com fundamento e orientações adicionais.
6	Peça esclarecimentos	Caso necessário, o titular pode complementar informações ou contestar a resposta.

Proteção contra fraude

A confirmação de identidade protege o próprio titular. A Vert não solicita senha, token, código de autenticação ou informação desnecessária para atender direitos.

ANEXO V - MATRIZ EXECUTIVA DE ALINHAMENTO LGPD E ISO/IEC 27701:2025

Tema	LGPD	ISO/IEC 27701:2025 - síntese	Evidência esperada
Governança e política	Arts. 6º e 50	Política, liderança, papéis e melhoria	POL-002, RACI, atas e objetivos
Inventário e finalidade	Arts. 6º, 7º, 11 e 37	Operação controlada e registros	ROPA, Mapa de Dados, bases legais
Riscos e impacto	Arts. 38, 46 e 50	Planejamento e avaliação de riscos	MR-001 e AIPD/DPIA
Transparência	Arts. 9º e 18	Comunicação e direitos	Políticas, avisos e registros de atendimento
Controlador e operador	Arts. 5º, 39 e 42-45	Requisitos por papel	Contratos, instruções e anexos I a III

Crianças e adolescentes	Art. 14 e normas aplicáveis	Proteção de titulares vulneráveis	Seção 12, AIPD e design apropriado
Transferência internacional	Arts. 33-36	Controles de terceiros e fluxos internacionais	Contratos, SCCs, avaliações
Segurança	Arts. 46-49	Controles operacionais e incidentes	POL-001, logs, testes e resposta
Fornecedores	Arts. 39 e 46	Gestão de operadores e suboperadores	Due diligence, SLA, auditorias
Retenção e eliminação	Arts. 15 e 16	Ciclo de vida e limitação	Matriz de temporalidade e registros
Monitoramento e auditoria	Art. 50	Avaliação de desempenho	Indicadores, auditorias e análise crítica
Não conformidade e melhoria	Princípio da responsabilização	Ações corretivas e evolução	Planos de ação e verificação de eficácia

29. CONTROLE DE VERSÕES, APROVAÇÃO E VIGÊNCIA

Versão	Data	Elaboração	Aprovação	Descrição
1.0	13/07/2026	Comitê SGSI/ SGPI e DPO	Alta Direção	Reestruturação integral da política pública; integração LGPD, ISO/IEC 27701:2025, ECA Digital, transferências internacionais e anexos de papéis.

Vigência: a partir da aprovação e publicação, permanecendo válida até substituição por versão posterior.

Consulta oficial: site institucional e ECM/ Wiki.Vert. Cópias impressas são consideradas não controladas.

VERT
ANALYTICS

SEU TIME DE
RESULTADOS EM **DADOS**