Política de Privacy by Design e by Default

Diretrizes obrigatórias para a incorporação da privacidade desde a concepção e por padrão em produtos, sistemas e processos da PX.Center que tratam dados pessoais, abrangendo os sete princípios fundamentais do Privacy by Design, a minimização, a desidentificação, a retenção, a devolução e o descarte.

Código:	*POL-SEG-028*
Área responsável:	*Privacidade*
Data de emissão:	*24/06/2026*
Responsável pela aprovação:	*DPO / CSIP*

1. FINALIDADE/OBJETIVO

Esta política estabelece as diretrizes obrigatórias para a incorporação da privacidade desde a concepção (privacy by design) e da privacidade por padrão (privacy by default) em todos os produtos, sistemas, projetos e processos da PX.Center que envolvam tratamento de dados pessoais.

O documento atende aos controles 7.4 e 8.4 da ISO/IEC 27701:2019, que exigem a adoção de privacidade desde a concepção e por padrão pelo controlador e pelo operador, e ao art. 46, parágrafo 2º, da Lei nº 13.709/2018 (LGPD), que determina a observância de medidas de segurança e privacidade desde a fase de concepção do produto ou do serviço até a sua execução. Esta política deriva da Política de Segurança da Informação (POL-SEG-001), à qual se subordina.

2. ESCOPO/APLICABILIDADE

Aplica-se a todo o ciclo de vida de produtos, sistemas, aplicações, integrações e processos de negócio da PX.Center que tratem dados pessoais, nas situações em que a Organização atue como controladora ou como operadora.

Abrange as fases de concepção, desenvolvimento, testes, homologação, produção, retenção, devolução e descarte, nos ambientes locais e nas nuvens corporativas em uso (os ambientes de nuvem corporativos em uso). Aplica-se igualmente à aquisição de produtos ou serviços e à contratação de fornecedores e prestadores que envolvam programas de software, novas aplicações, tecnologias ou serviços que tratem dados pessoais. Inclui sistemas e funcionalidades baseados em inteligência artificial, na medida em que tratem dados pessoais em qualquer fase do seu ciclo de vida.

Subordina-se à Política de Segurança da Informação (POL-SEG-001) e integra o Sistema de Gestão de Segurança da Informação.

3. USUÁRIOS/PÚBLICO-ALVO

Líder de Tecnologia/Produto, equipes de desenvolvimento e engenharia, Líder de Segurança da Informação, Encarregado de Dados (DPO), Comitê de Segurança da Informação e Privacidade (CSIP), gestores de projeto e terceiros contratados que participem do desenvolvimento, da sustentação ou do teste de produtos e sistemas da PX.Center.

4. DOCUMENTOS DE REFERÊNCIA

- ISO/IEC 27701:2019, controles 7.4 (privacidade desde a concepção e por padrão: controlador) e 8.4 (privacidade desde a concepção, retenção, devolução e descarte: operador)
- ISO/IEC 27001:2022 (Sistema de Gestão de Segurança da Informação)

- Lei nº 13.709/2018 (LGPD), em especial o art. 6º (princípios da adequação e da necessidade), o art. 38 (Relatório de Impacto à Proteção de Dados) e o art. 46, parágrafo 2º
- POL-SEG-001: Política de Segurança da Informação
- POL-SEG-029: Política de Privacidade e Proteção de Dados Pessoais
- POL-SEG-027: Política de Governança em Privacidade
- POL-SEG-005: Política de Descarte Seguro
- POL-SEG-006: Política de Criptografia
- POL-SEG-007: Política de Desenvolvimento Seguro
- POL-SEG-018: Política de Testes e Homologação
- POP-SEG-009: Avaliação de Impacto à Proteção de Dados Pessoais (RIPD)
- POP-SGI-006: Tratamento de Não Conformidades
- INT-SEG-002: Mascaramento de Dados em Ambientes de Teste
- INN-GRR-009: Proteção de Dados Pessoais
- MAN-SGI-001: Manual do SGI
- FOR-17-001: Questionário de Privacy by Design e RIPD

5. DIRETRIZES / REGRAS / CONTROLES

5.1 Os sete princípios fundamentais do Privacy by Design

O Privacy by Design determina que a proteção de dados e a privacidade sejam incorporadas a todo o ciclo de vida dos projetos, produtos e serviços, da concepção ao descarte, com perspectiva preventiva. Sua aplicação observa os sete princípios fundamentais a seguir.

5.1.1 Proativo, não reativo; preventivo, não corretivo: antecipar e evitar eventos invasivos à privacidade antes que ocorram, em vez de aguardar a materialização do risco. Aplicam-se medidas técnicas como anonimização ou pseudonimização, criptografia, garantia de confidencialidade, integridade, disponibilidade e resiliência dos sistemas, verificação e monitoramento da eficácia das medidas e acesso restrito a repositórios internos e externos.

5.1.2 Privacidade como configuração padrão: a privacidade integra os produtos, sistemas e serviços por padrão, sem exigir ação do titular. O titular recebe o produto ou serviço com todas as salvaguardas ativadas desde o início do desenvolvimento, é informado de quais dados são coletados e para qual finalidade legítima, e não lhe cabe adotar ação protetiva para assegurar a privacidade.

5.1.3 Privacidade incorporada ao design: a privacidade é componente elementar da funcionalidade central projetada, e não um acréscimo posterior. Qualquer opção de compartilhamento de dados do titular inicia restrita, e as opções apresentadas não podem ser tendenciosas ao aceite de compartilhamento ou à permissão automática.

5.1.4 Funcionalidade total: soma positiva, não soma zero: incorporar a privacidade a tecnologias, processos e sistemas sem prejuízo da sua funcionalidade plena, acomodando objetivos não relacionados à privacidade de forma que agregue, com documentação dos

interesses envolvidos e busca de soluções multifuncionais que dispensem a renúncia de objetivos legítimos.

5.1.5 Segurança de ponta a ponta: proteção durante todo o ciclo de vida: adoção de medidas robustas de segurança desde o início até o término do tratamento, assegurando a proteção dos dados pessoais em todas as fases do seu ciclo de vida.

5.1.6 Visibilidade e transparência: as práticas de tratamento permanecem visíveis e verificáveis, sustentando a responsabilização e a confiança do titular, em observância aos princípios da LGPD do livre acesso, da qualidade dos dados, da transparência, da não discriminação e da responsabilização.

5.1.7 Respeito pela privacidade do titular: preponderância dos interesses dos titulares, mediante padrões robustos de privacidade, mecanismos para o exercício de seus direitos, acesso facilitado e medidas de segurança que assegurem a confidencialidade, a integridade e a disponibilidade dos dados durante todo o seu ciclo de vida.

5.2 Privacidade desde a concepção (privacy by design)

5.2.1 É obrigatório levantar e registrar os requisitos de privacidade no início de todo projeto, produto ou funcionalidade que trate dados pessoais, antes de qualquer decisão de arquitetura ou de desenvolvimento.

5.2.2 Os requisitos de privacidade integram os artefatos do projeto e seguem o ciclo de desenvolvimento seguro definido na POL-SEG-007. Controles criptográficos aplicam-se conforme a POL-SEG-006.

5.2.3 A área demandante de novo projeto, processo ou serviço que trate dados pessoais preenche o Questionário de Privacy by Design (FOR-17-001) e o encaminha ao DPO e ao CSIP para avaliação dos pré-requisitos antes do início da atividade. A avaliação considera o escopo, o objetivo e a finalidade do tratamento, a natureza dos dados coletados, a base legal adotada, as formas de armazenamento, uso e transferência, o prazo de retenção e a forma de descarte e as medidas de segurança física e lógica aplicadas.

5.2.4 A Avaliação de Impacto à Proteção de Dados Pessoais (RIPD) é obrigatória, conforme o POP-SEG-009 e o art. 38 da LGPD, quando o tratamento puder gerar alto risco aos titulares, incluindo tratamento de dados sensíveis em larga escala, uso de novas tecnologias ou monitoramento sistemático de titulares. Nos demais casos, o DPO avalia e registra a decisão sobre a necessidade da RIPD.

5.2.5 O DPO e o CSIP podem recomendar ajustes, aprovar ou vetar o projeto, ainda que temporariamente, após a análise dos riscos e dos mecanismos de mitigação aplicáveis.

5.2.6 É vedado colocar em produção produto ou funcionalidade que trate dados pessoais sem que os requisitos de privacidade tenham sido implementados e verificados.

5.2.7 Após a implantação, o projeto, processo ou serviço que trate dados pessoais é monitorado quanto ao desenvolvimento e ao desempenho. O monitoramento pós-implantação é realizado, no mínimo, uma vez ao ano e, sempre que necessário, em periodicidade inferior, sob a coordenação do DPO e do CSIP, com vistas à melhoria contínua segundo o ciclo PDCA.

5.3 Privacidade por padrão (privacy by default)

5.3.1 Toda configuração padrão de produto, sistema ou funcionalidade deve ser a mais restritiva em termos de privacidade. Compartilhamento de dados, visibilidade de perfil e coletas adicionais permanecem desativados por padrão e dependem de ação afirmativa do titular.

5.3.2 A coleta de dados pessoais limita-se ao mínimo necessário ao cumprimento da finalidade declarada. É vedado coletar dado pessoal sem finalidade declarada, registrada e legítima, em observância aos princípios da adequação e da necessidade (art. 6º, incisos II e III, da LGPD).

5.3.3 Campos de coleta opcionais devem ser identificados como tais e não podem condicionar o uso do produto quando não forem indispensáveis à finalidade do tratamento.

5.4 Minimização e desidentificação

5.4.1 As equipes de desenvolvimento devem anonimizar ou pseudonimizar os dados pessoais quando a finalidade do tratamento permitir, com prioridade para a anonimização.

5.4.2 A pseudonimização exige a guarda segregada das informações adicionais que permitam a reidentificação, com controle de acesso restrito e registro de uso.

5.4.3 É vedado manter atributos identificadores em bases analíticas ou estatísticas quando a finalidade puder ser atendida com dados desidentificados.

5.5 Retenção e descarte

5.5.1 Dados pessoais são retidos somente pelo prazo necessário ao cumprimento da finalidade do tratamento ou de obrigação legal ou regulatória. Encerrada a finalidade, é obrigatório eliminar ou anonimizar os dados, em conformidade com o controle 7.4 da ISO/IEC 27701:2019.

5.5.2 Os prazos de retenção por categoria de dado pessoal constam de tabela de temporalidade específica. A tabela de temporalidade é mantida e publicada pelo Encarregado de Dados (DPO) e revisada a cada doze meses.

5.5.3 O descarte de dados pessoais e das mídias que os contenham segue os procedimentos de descarte seguro definidos na POL-SEG-005, com registro formal da eliminação.

5.6 Devolução e eliminação ao término de contrato

5.6.1 Nos contratos em que a PX.Center atue como operadora, é obrigatório, ao término da prestação de serviços, devolver ao controlador ou eliminar os dados pessoais tratados, conforme instrução documentada do controlador, em conformidade com o controle 8.4 da ISO/IEC 27701:2019.

5.6.2 A eliminação deve ser comprovada formalmente ao controlador. Cópias de segurança que contenham os dados seguem o mesmo regime de eliminação ao final do seu ciclo de retenção.

5.6.3 A retenção de dados após o término contratual somente é admitida mediante obrigação legal ou regulatória, comunicada formalmente ao controlador.

5.7 Dados pessoais em desenvolvimento e teste

5.7.1 É vedado utilizar dado pessoal real em ambientes de desenvolvimento, teste ou homologação sem mascaramento, aplicado conforme a INT-SEG-002.

5.7.2 Ambientes de teste e homologação observam os controles de segregação e de acesso definidos na POL-SEG-018.

5.8 Inteligência artificial e Privacy by Design

5.8.1 Sistemas, funcionalidades e agentes baseados em inteligência artificial que tratem dados pessoais observam integralmente os sete princípios da seção 5.1 e os controles desta política, desde a concepção do caso de uso.

5.8.2 O preenchimento do Questionário de Privacy by Design (FOR-17-001) é obrigatório para todo caso de uso de inteligência artificial que trate dados pessoais, devendo a avaliação considerar a base legal, a minimização dos dados de treinamento e de inferência, a possibilidade de desidentificação e os riscos de discriminação e de decisões automatizadas.

5.8.3 É vedado utilizar dados pessoais reais em treinamento, ajuste ou avaliação de modelos sem finalidade declarada e legítima e sem desidentificação, quando a finalidade a permitir, aplicando-se o mascaramento da INT-SEG-002 nos ambientes não produtivos.

5.8.4 O tratamento por inteligência artificial que possa gerar alto risco aos titulares, inclusive decisão automatizada com efeito significativo, exige RIPD conforme o POP-SEG-009 e o art. 38 da LGPD, previamente à implantação.

5.9 Uso de redes sociais

5.9.1 O uso de redes sociais é permitido às funções de negócio, especialmente Marketing e Comercial, exclusivamente para finalidades corporativas, sendo vedada a publicação ou o tratamento de dados confidenciais ou de dados pessoais por esse canal.

5.9.2 O uso pessoal de redes sociais nos recursos corporativos é vedado aos demais colaboradores, que não exerçam função de negócio que o justifique.

6. RESPONSABILIDADES

A área de Tecnologia da Informação (TI) é a área responsável por garantir o cumprimento desta política por todas as áreas e departamentos da Organização.

6.1 Líder de Tecnologia/Produto: garantir que os requisitos de privacidade integrem o ciclo de vida de produtos e projetos; assegurar recursos e priorização para a sua implementação; autorizar a entrada em produção somente após a verificação dos requisitos de privacidade. Responde pela disseminação e pelo cumprimento desta política nas áreas da Organização.

6.2 Encarregado de Dados (DPO): orientar as equipes na definição dos requisitos de privacidade; avaliar o Questionário de Privacy by Design (FOR-17-001); avaliar a necessidade e validar as RIPDs conforme o POP-SEG-009; coordenar o monitoramento pós-implantação previsto na seção 5.2.7; manter o ROPA atualizado conforme a POL-SEG-029 e a POL-SEG-027.

6.3 CSIP (Comitê de Segurança da Informação e Privacidade): avaliar, em conjunto com o DPO, os questionários e projetos submetidos; recomendar ajustes, aprovar ou vetar projetos; deliberar sobre riscos residuais e aprovar esta política.

6.4 Líder de Segurança da Informação: definir e validar os controles técnicos de segurança, desidentificação, mascaramento e descarte; verificar a aderência a esta política nas avaliações e auditorias do SGI.

6.5 Equipes de desenvolvimento: implementar os requisitos de privacidade definidos para cada projeto ou funcionalidade; aplicar o mascaramento em ambientes de teste; reportar ao DPO e ao Líder de Segurança da Informação qualquer tratamento de dados pessoais sem requisito de privacidade definido.

6.6 Canal de violações: toda violação ou suspeita de violação desta política deve ser reportada de imediato. As violações relacionadas a privacidade e proteção de dados pessoais são reportadas ao Encarregado de Dados (DPO) pelo e-mail dpo@px.center. As violações relacionadas à segurança da informação são reportadas à área de Segurança da Informação pelo e-mail security@px.center. Os casos são investigados de forma diligente e confidencial e, quando confirmados, ensejam as medidas apropriadas.

O descumprimento desta política sujeita o infrator às medidas disciplinares previstas nas normas internas da PX.Center, sem prejuízo das sanções legais aplicáveis.

7. GESTÃO DE REGISTROS

Os registros decorrentes desta política compreendem: questionários de Privacy by Design (FOR-17-001) preenchidos e avaliados; requisitos de privacidade documentados nos artefatos de projeto; RIPDs elaboradas conforme o POP-SEG-009; evidências de eliminação, devolução e descarte de dados pessoais; registros de mascaramento em ambientes de teste; e registros do monitoramento pós-implantação previsto na seção 5.2.7.

Os questionários, as RIPDs e as demais evidências são armazenados no repositório documental do SGI. Não conformidades relacionadas a esta política são registradas e tratadas na ferramenta corporativa de gestão de não conformidades, conforme o POP-SGI-006. O ROPA é mantido pelo DPO, conforme a POL-SEG-029 e a POL-SEG-027.

8. VALIDADE / GESTÃO DOCUMENTAL

Esta política entra em vigor na data de sua publicação e tem validade indeterminada. A revisão ocorre anualmente ou diante de alteração legislativa, regulatória ou organizacional relevante, mediante aprovação formal do CSIP (Comitê de Segurança da Informação e Privacidade).

9. ANEXOS

FOR-17-001: Questionário de Privacy by Design e RIPD, instrumento de levantamento dos requisitos de privacidade preenchido pela área demandante e avaliado pelo DPO e pelo CSIP, na forma da seção 5.2.3. Os demais registros operacionais referenciados nesta política residem no repositório documental do SGI (questionários, RIPDs e evidências de eliminação e devolução) e na ferramenta corporativa de gestão de não conformidades (não conformidades).

HISTÓRICO DE ALTERAÇÕES

Versão	Data	Criador	Descrição de Alterações
00	16/02/2026	SGI	Criação do documento
01	24/06/2026	SGI	Recodificação para sigla