

Política de Governança em Privacidade

Estrutura de governança em privacidade da PX.Center

Código:	<i>POL-SEG-027</i>
Área responsável:	<i>Privacidade</i>
Data de emissão:	<i>24/06/2026</i>
Responsável pela aprovação:	<i>DPO / CSIP</i>

1. FINALIDADE/OBJETIVO

Esta política estabelece a estrutura de governança em privacidade da PX.Center, estendendo o Sistema de Gestão de Segurança da Informação (SGSI), instituído pela POL-SEG-001 (Política de Segurança da Informação) e pelo MAN-SGI-001, para um Sistema de Gestão de Privacidade da Informação (PIMS), em conformidade com os controles 5.2, 5.6, 6.2 e 6.3 da ISO/IEC 27701:2019, com a Lei 13.709/2018 (LGPD) e em integração com a ISO/IEC 27001:2022.

O documento define papéis, instâncias de decisão e mecanismos de planejamento e controle operacional que asseguram o tratamento de dados pessoais conforme as bases legais e os princípios da LGPD. Esta política deriva da Política de Segurança da Informação (POL-SEG-001), à qual se subordina.

2. ESCOPO/APLICABILIDADE

O PIMS abrange todos os processos da PX.Center que tratam dados pessoais, nas condições de controladora e de operadora, em todas as unidades, ambientes tecnológicos e relações com terceiros. A definição pela PX.Center como entidade de referência abrange os demais CNPJs do grupo, dispensando documento específico por entidade. Estão incluídos os sistemas, ativos de informação e serviços em nuvem que suportam o ciclo de vida do dado pessoal: coleta, uso, armazenamento, compartilhamento e eliminação.

Esta política aplica-se em conjunto com a POL-SEG-029 — Política de Privacidade e Proteção de Dados Pessoais, norma-base de tratamento de dados pessoais da Organização. 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

Direção, Encarregado de Dados (DPO), membros do CSIP (Comitê de Segurança da Informação e Privacidade), Líder de Segurança da Informação, gestores de área e todos os colaboradores e terceiros que tratam dados pessoais em nome da PX.Center.

4. DOCUMENTOS DE REFERÊNCIA

- Lei 13.709/2018 (Lei Geral de Proteção de Dados Pessoais, LGPD)
- ISO/IEC 27701:2019 (controles 5.2, 5.6, 6.2 e 6.3)
- ISO/IEC 27001:2022
- POL-SEG-001: Política de Segurança da Informação
- MAN-SGI-001: Manual do SGI
- POL-SEG-029 — Política de Privacidade e Proteção de Dados Pessoais
- POL-SEG-002: Política de Gestão de Incidentes

- POL-SEG-017: ciclo de treinamento e conscientização
- POP-SEG-009: Avaliação de Impacto à Proteção de Dados Pessoais
- POP-SGI-006: Tratamento de Não Conformidades
- INN-GRR-009: Proteção de Dados Pessoais

5. DIRETRIZES / REGRAS / CONTROLES

5.1 PIMS COMO EXTENSÃO DO SGSI

A PX.Center estende o SGSI estabelecido pela POL-SEG-001 e pelo MAN-SGI-001 para um PIMS, em conformidade com o controle 5.2 da ISO/IEC 27701:2019. O escopo do PIMS cobre todos os processos que tratam dados pessoais, tanto na condição de controladora quanto na de operadora. Os requisitos da ISO/IEC 27001:2022 são interpretados com a extensão de privacidade: onde a norma menciona segurança da informação, leia-se segurança da informação e privacidade. É vedado tratar dados pessoais fora do escopo do PIMS.

5.2 PAPÉIS DE PRIVACIDADE

Em conformidade com o controle 6.3 da ISO/IEC 27701:2019, a PX.Center mantém papéis formais de privacidade. O Encarregado de Dados (DPO) é designado pela Direção por ato formal, com a função exercida mediante contrato com serviço especializado de Encarregado de Dados (Encarregado como serviço), serviço especializado de Encarregado como serviço, e o contato divulgado no canal dpo@px.center. O DPO exerce as atribuições do art. 41 da LGPD:

aceita reclamações e comunicações dos titulares, presta esclarecimentos e adota providências; recebe comunicações da ANPD; orienta colaboradores e contratados sobre as práticas de proteção de dados pessoais. Opera o canal do titular dpo@px.center, com prazo de resposta de 15 dias úteis, e mantém o Registro das Operações de Tratamento de Dados Pessoais (ROPA). Os gestores de área respondem pelo tratamento de dados pessoais nos processos sob sua gestão, mantêm as informações do ROPA de seus processos atualizadas e comunicam ao DPO toda mudança de finalidade, base legal ou compartilhamento.

O CSIP é a instância deliberativa de privacidade da Organização: aprova normas, arbitra conflitos de interpretação, delibera sobre riscos residuais e acompanha o desempenho do PIMS em reunião mensal.

5.3 PLANEJAMENTO E CONTROLE OPERACIONAL DO PIMS

Em conformidade com o controle 5.6 da ISO/IEC 27701:2019, o DPO mantém o ROPA atualizado, sendo obrigatório registrar toda nova operação de tratamento antes do início da operação. Todo novo projeto, produto ou serviço que envolva o tratamento de dados pessoais deve acionar a avaliação de impacto à proteção de dados pessoais (RIPD) antes de avançar para a implantação, conforme o modelo definido no POP-SEG-009, sob responsabilidade do gestor de área demandante com apoio do DPO.

Tratamentos com potencial de alto risco aos direitos dos titulares exigem a conclusão dessa avaliação previamente à implantação. Após a implantação, os tratamentos avaliados são

submetidos a monitoramento pós-implantação, com revisão periódica conduzida pelo DPO em conjunto com os gestores de área, de modo a verificar a manutenção das condições de conformidade e a eficácia dos controles. Incidentes que envolvam dados pessoais seguem a POL-SEG-002, com etapa adicional obrigatória: o DPO avalia e documenta a necessidade de comunicação à ANPD e aos titulares afetados, conforme o art. 48 da LGPD.

Não conformidades de privacidade são registradas e tratadas no ferramenta corporativa de gestão de não conformidades, conforme o POP-SGI-006.

5.4 HIERARQUIA NORMATIVA DE PRIVACIDADE

Em conformidade com o controle 6.2 da ISO/IEC 27701:2019, a estrutura normativa de privacidade obedece a uma hierarquia em que esta política rege a governança do PIMS; a POL-SEG-029 — Política de Privacidade e Proteção de Dados Pessoais é a norma-base de tratamento de dados pessoais, abrangendo direitos dos titulares, bases legais e transferência internacional; e as normas derivadas, como a INN-GRR-009 e o POP-SEG-009, detalham controles específicos por meio de procedimentos, instruções e normas internas.

Conflito entre normas é resolvido pela norma de nível superior, cabendo ao CSIP deliberar sobre os casos omissos.

5.5 DILIGÊNCIA DE TERCEIROS OPERADORES

A PX.Center mantém processo formal de diligência de terceiros operadores que tratam dados pessoais em seu nome, com aplicação de questionário de conformidade em privacidade previamente à contratação e durante a vigência contratual. A diligência verifica a aderência do operador às obrigações da LGPD e às exigências de segurança da informação aplicáveis, e seus resultados subsidiam as decisões de contratação e a manutenção dos vínculos com terceiros.

5.6 CONSCIENTIZAÇÃO EM PRIVACIDADE

O conteúdo de privacidade e proteção de dados pessoais integra o ciclo de treinamento e conscientização regido pela POL-SEG-017. A participação é obrigatória na admissão e nas reciclagens periódicas; os gestores de área asseguram a participação de suas equipes.

5.7 USO DE REDES SOCIAIS

O uso de redes sociais em nome da PX.Center é permitido às funções de negócio de Marketing e Comercial, restrito às finalidades institucionais e comerciais e vedada a divulgação de dados confidenciais ou de dados pessoais. Aos demais colaboradores é proibido o uso pessoal de redes sociais nos ativos e ambientes da Organização. A publicação de qualquer conteúdo que envolva dados pessoais observa as bases legais da LGPD e as diretrizes desta política e da POL-SEG-029.

5.8 ANÁLISE CRÍTICA DO PIMS

O CSIP realiza análise crítica anual do PIMS, avaliando a adequação do escopo, o estado do ROPA, os incidentes com dados pessoais, os resultados de avaliações de impacto, as não conformidades registradas no ferramenta corporativa de gestão de não conformidades, as

solicitações de titulares e as mudanças na legislação ou em orientações da ANPD. O CSIP registra em ata as decisões e os planos de ação resultantes.

6. RESPONSABILIDADES

A Tecnologia da Informação (TI) é a área responsável por garantir o cumprimento desta política e responde pela apuração de violações às suas disposições, com canal de contato dpo@px.center para questões de privacidade e LGPD e security@px.center para questões de segurança da informação.

A Direção aprova esta política, designa formalmente o DPO, provê os recursos necessários ao PIMS e responde pelo compromisso da Organização com a LGPD.

O Encarregado de Dados (DPO) exerce as atribuições do art. 41 da LGPD, mantém o ROPA, opera o canal do titular, conduz a interlocução com a ANPD e reporta o desempenho do PIMS ao CSIP.

O CSIP delibera sobre privacidade, aprova as normas derivadas, realiza a análise crítica anual do PIMS e acompanha a execução dos planos de ação.

O Líder de Segurança da Informação integra os controles do SGSI à proteção de dados pessoais, apoia a resposta a incidentes que envolvam dados pessoais e mantém alinhamento técnico com o DPO.

Os gestores de área respondem pelo tratamento de dados pessoais em seus processos, mantêm as informações do ROPA atualizadas, acionam a avaliação de impacto (RIPD) quando aplicável e asseguram a conscientização de suas equipes.

7. GESTÃO DE REGISTROS

Os registros do PIMS residem nos seguintes repositórios:

- ROPA: sob custódia do DPO.
- Atas do CSIP, versões desta política e avaliações de impacto (POP-SEG-009): repositório documental do SGI.
- Não conformidades de privacidade: ferramenta corporativa de gestão de não conformidades.
- Registros de atendimento ao titular recebidos via dpo@px.center: sob custódia do DPO.
- Evidências de treinamento em privacidade: conforme a POL-SEG-017.

É obrigatório preservar a integridade dos registros, com acesso restrito por necessidade de conhecimento, e mantê-los disponíveis para auditorias internas e externas do SGI.

8. VALIDADE / GESTÃO DOCUMENTAL

Esta política entra em vigor na data de sua publicação, com validade por prazo indeterminado. O CSIP revisa o documento anualmente ou diante de mudança relevante na legislação, em orientações da ANPD, na estrutura organizacional ou no escopo do PIMS. O descumprimento desta política sujeita o infrator às medidas disciplinares previstas nas normas internas da PX.Center.

9. ANEXOS

Não há anexos. Os registros operacionais do PIMS residem nos sistemas indicados na seção Gestão de Registros (ferramenta corporativa de gestão de não conformidades e repositório documental do SGI).

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