					Insira aqui a designação da entidade jurídica registada							
Número do documento: PII02					Título do documento: **Política de Papéis, Responsabilidades e Responsabilização em matéria de Privacidade**							
Versão: 1.0		Data de entrada em vigor: 01.01.2025			Proprietário do documento:							
X	Política		Norma		Procedimento		Formulário		Registo		Outro	

Histórico de revisões				
Número da revisão	**Data da revisão**	**Alterações**	**Revisto por**	**Proprietário do processo**

Aprovações			
Nome	**Cargo**	**Data**	**Assinatura**

Alinhada com normas e regulamentos

Norma / Regulamento	Cláusula / Controlo / Artigo	Aplicabilidade	Tipo de cobertura	Comentário
ISO/IEC 27701:2025	Clause 4.1	Both	Primary	Contexto da função PIMS
ISO/IEC 27701:2025	Clause 5.1	Both	Primary	Liderança e responsabilização
ISO/IEC 27701:2025	Clause 5.3	Both	Primary	Papéis, responsabilidades e autoridades do PIMS
ISO/IEC 27701:2025	Clause 7.2	Both	Primary	Competência da função
ISO/IEC 27701:2025	Clause 7.3	Both	Primary	Sensibilização para a função
ISO/IEC 27701:2025	Clause 7.4	Both	Supporting	Comunicação da função
ISO/IEC 27701:2025	Clause 7.5	Both	Primary	Informação documentada da função
ISO/IEC 27701:2025	Clause 8.1	Both	Primary	Propriedade dos controlos operacionais
ISO/IEC 27701:2025	Clause 9.2	Both	Supporting	Função de auditoria independente
ISO/IEC 27701:2025	Clause 9.3	Both	Supporting	Revisão pela gestão da responsabilização
ISO/IEC 27701:2025	Clause 10.2	Both	Supporting	Não conformidade e ação corretiva relacionadas com funções
ISO/IEC 27701:2025	Annex A.1.2.7	Controller	Supporting	Responsabilidade contratual do subcontratante
ISO/IEC 27701:2025	Annex A.1.2.8	Joint Controller	Primary	Papéis e responsabilidades dos responsáveis conjuntos pelo tratamento
ISO/IEC 27701:2025	Annex A.1.2.9	Controller	Primary	Registos de responsabilização

ISO/IEC 27701:2025	Annex A.2.2.2	Processor	Primary	Acordos e instruções de clientes para subcontratantes
ISO/IEC 27701:2025	Annex A.2.2.3	Processor	Supporting	Alinhamento de finalidades do subcontratante
GDPR	Article 5(2)	Controller	Supporting	Evidência de responsabilização
GDPR	Article 24	Controller	Supporting	Responsabilidade e medidas do responsável pelo tratamento
GDPR	Article 26	Joint Controller	Supporting	Acordos entre responsáveis conjuntos pelo tratamento
GDPR	Article 28	Both	Supporting	Governação e instruções de subcontratantes
GDPR	Article 30	Both	Supporting	Registos de tratamento e evidência de responsabilidade
GDPR	Article 37	Conditional	Referenced	Designação de DPO quando aplicável
GDPR	Article 38	Conditional	Supporting	Posição e independência do DPO quando aplicável
GDPR	Article 39	Conditional	Supporting	Tarefas do DPO quando aplicável
ISO/IEC 29100:2020	Clause 4.1; Clause 4.2	Both	Supporting	Intervenientes e papéis no quadro de privacidade
ISO/IEC 29100:2020	Clause 5.12	Both	Supporting	Responsabilização pelo cumprimento da privacidade
ISO/IEC 29151:2022	Clause 6.1.2; Clause 6.1.3	Both	Supporting	Papéis de proteção de PII e segregação
ISO/IEC 27002:2022	Control 5.2	Both	Supporting	Papéis e responsabilidades de segurança da informação

ISO/IEC 27002:2022	Control 5.3	Both	Supporting	Segregação de funções

1. Âmbito

1.1 Esta política define o modelo de funções do PIMS, a estrutura de responsabilização, as regras de atribuição de responsabilidades, as regras de combinação de funções, as expectativas de escalonamento e os requisitos de evidência para a governação da privacidade.

1.2 Esta política aplica-se a pessoal, funções, sistemas, fornecedores, subcontratantes, subcontratantes subsequentes e relações de responsabilidade conjunta pelo tratamento que participem no tratamento de PII, ou o influenciem, no âmbito do PIMS.

1.3 Esta política aplica-se em contextos de responsável pelo tratamento, responsável conjunto pelo tratamento, subcontratante e subcontratante subsequente.

1.4 Esta política não cria novos cargos organizacionais. Define funções canónicas do PIMS que podem ser atribuídas a pessoal ou funções existentes, desde que os requisitos de atribuição da função, competência, independência e conflito de interesses estejam documentados.

2. Finalidade

2.1 A finalidade desta política é assegurar que as responsabilidades do PIMS são claramente atribuídas, compreendidas, comunicadas, evidenciadas, revistas e melhoradas.

2.2 Esta política permite à organização demonstrar responsabilização pela governação da privacidade, pela propriedade do tratamento de PII, pela determinação dos papéis de responsável pelo tratamento e de subcontratante, pela repartição de responsabilidades entre responsáveis conjuntos pelo tratamento, pela gestão de instruções aos subcontratantes, pela responsabilidade de privacidade dos fornecedores, pela revisão independente e pelo escalonamento baseado em funções.

3. Objetivos

3.1 Os objetivos desta política são:

3.1.1 definir as funções canónicas do PIMS utilizadas em todo o conjunto de políticas do PIMS;

3.1.2 assegurar que cada responsabilidade material do PIMS tem uma função responsável atribuída;

3.1.3 apoiar a responsabilização do responsável pelo tratamento, do responsável conjunto pelo tratamento, do subcontratante e do subcontratante subsequente;

3.1.4 permitir a combinação prática de funções em pequenas e médias organizações, controlando simultaneamente conflitos de interesses;

3.1.5 preservar a revisão independente pelo Internal Audit / Compliance Reviewer;

3.1.6 assegurar que as atribuições de funções e as alterações de funções são registadas em objetos de evidência canónicos;

3.1.7 assegurar que os titulares de funções do PIMS recebem comunicação e sensibilização adequadas;

3.1.8 assegurar que lacunas, conflitos e não conformidades relacionados com funções são escalonados e corrigidos.

4. Declarações da política

4.1 Modelo e atribuição de funções do PIMS

4.1.1 [All] Top Management DEVE aprovar o modelo canónico de funções do PIMS em REG01 antes da implementação inicial do PIMS e, posteriormente, anualmente.

4.1.2 [All] Privacy Lead / PIMS Manager DEVE manter as atribuições nominativas de funções do PIMS em REG01 antes da implementação do PIMS e no prazo de 10 dias úteis após alterações de pessoal ou organizacionais.

4.1.3 [All] Privacy Lead / PIMS Manager DEVE documentar o âmbito de responsabilidade e o nível de autoridade de cada função do PIMS atribuída em REG01 antes de a atribuição produzir efeitos.

4.1.4 [All] Process Owner / Business Owner DEVE atribuir um proprietário de tratamento responsável por cada atividade de tratamento de PII em REG02 antes do início da atividade de tratamento.

4.1.5 [All] System Owner / Application Owner DEVE documentar o proprietário do sistema responsável por cada sistema que trate PII em REG02 antes da entrada em produção do sistema.

4.1.6 [All] Vendor / Procurement Owner DEVE documentar o proprietário da relação para cada subcontratante, subcontratante subsequente, partilha de dados com terceiros ou relação de responsabilidade conjunta pelo tratamento em REG08 antes da integração ou da aprovação do acordo.

4.2 Combinação de funções, segregação e independência

4.2.1 [All] Privacy Lead / PIMS Manager DEVE documentar cada combinação de funções do PIMS em REG01 antes de a combinação de funções produzir efeitos.

4.2.2 [All] Top Management DEVE aprovar, em REG01, as combinações de funções que envolvam Privacy Lead / PIMS Manager, Data Protection Officer / Privacy Advisor, Information Security Lead, Incident Response Coordinator ou Internal Audit / Compliance Reviewer antes da atribuição.

4.2.3 [All] Internal Audit / Compliance Reviewer DEVE documentar a independência face ao processo do PIMS em revisão em REG12 antes do início de cada auditoria ou revisão de conformidade do PIMS.

4.2.4 [All] Privacy Lead / PIMS Manager DEVE registar controlos compensatórios para conflitos de segregação inevitáveis em REG12 antes de aprovar uma combinação de funções.

4.2.5 [All] Data Protection Officer / Privacy Advisor DEVE registar preocupações relativas à independência da função ou a conflitos de interesses em REG12 no prazo de cinco dias úteis após a identificação.

[... As secções 4.3–8 não estão incluídas nesta pré-visualização. Adquira o documento completo para aceder ao conteúdo integral. ...]

9. Exceções

9.1.1 [All] Process Owner / Business Owner DEVE solicitar uma exceção de responsabilização de função em REG12 antes de operar uma atividade de tratamento de PII sem uma função atribuída exigida.

9.1.2 [All] Privacy Lead / PIMS Manager DEVE avaliar o impacto e a mitigação de cada exceção de responsabilização de função em REG12 no prazo de 10 dias úteis após o pedido.

9.1.3 [All] Top Management DEVE aprovar exceções de responsabilização de função que excedam 30 dias ou afetem tratamentos de alto risco em REG12 antes de a exceção produzir efeitos.

9.1.4 [All] Privacy Lead / PIMS Manager DEVE definir uma data de expiração não superior a 90 dias em REG12 para cada exceção de responsabilização de função aprovada antes da aprovação.

9.1.5 [All] Privacy Lead / PIMS Manager DEVE encerrar ou reavaliar cada exceção de responsabilização de função em REG12 no prazo de cinco dias úteis após a expiração.

10. Aplicação

10.1.1 [All] Privacy Lead / PIMS Manager DEVE registar atribuições de funções do PIMS em falta, inexatas ou desatualizadas como não conformidades em REG12 no prazo de cinco dias úteis após a identificação.

10.1.2 [All] Top Management DEVE exigir ação corretiva em REG12 no prazo de 15 dias úteis para falhas de responsabilização repetidas ou prolongadas.

10.1.3 [All] Process Owner / Business Owner DEVE impedir a entrada em produção de tratamentos de PII novos ou alterados quando a evidência exigida de função e responsabilização estiver ausente de REG02 ou REG08.

10.1.4 [All] Internal Audit / Compliance Reviewer DEVE verificar a eficácia das ações corretivas para não conformidades de responsabilização de função em REG12 na auditoria agendada seguinte ou no prazo de 60 dias após o encerramento, consoante o que ocorrer primeiro.

11. Revisão e manutenção

11.1.1 [All] Privacy Lead / PIMS Manager DEVE rever esta política anualmente e no prazo de 30 dias após uma alteração material ao modelo de funções do PIMS.

11.1.2 [All] Data Protection Officer / Privacy Advisor DEVE rever as alterações propostas a esta política quanto ao impacto nas funções de privacidade em REG12 antes da aprovação.

11.1.3 [All] Top Management DEVE aprovar alterações materiais a esta política em REG12 antes da publicação.

11.1.4 [All] Privacy Lead / PIMS Manager DEVE atualizar REG01 e REG11 no prazo de 15 dias úteis após alterações aprovadas às funções, responsabilidades ou requisitos de comunicação do PIMS.

12. Políticas relacionadas

12.1 Esta política é suportada pelas seguintes políticas relacionadas:

12.1.1 PII01 - Política do Sistema de Gestão de Informação de Privacidade

12.1.2 PII03 - Política de Inventário de Tratamento de PII e Fundamento de Licitude

12.1.3 PII07 - Política de Avaliação de Riscos de Privacidade e DPIA

12.1.4 PII08 - Política de Privacidade desde a Conceção e por Defeito

12.1.5 PII12 - Política de Gestão de Privacidade de Subcontratantes, Subcontratantes Subsequentes e Terceiros

12.1.6 PII14 - Política de Segurança de PII e Controlo de Acesso

12.1.7 PII15 - Política de Gestão de Incidentes e Violações de PII

12.1.8 PII16 - Política de Formação, Sensibilização e Competência em Privacidade

12.1.9 PII17 - Política de Informação Documentada e Gestão de Evidência do PIMS

12.1.10 PII18 - Política de Monitorização, Auditoria e Melhoria do PIMS

13. Normas e referenciais de referência

13.1 Esta política está mapeada para as seguintes normas e regulamentos. O mapeamento explica como a política apoia os requisitos citados e identifica as cláusulas internas que os implementam ou suportam.

13.2 ISO/IEC 27701:2025

13.2.1 **Clause 4.1** - Mapeada para a determinação do contexto das funções do PIMS, da aplicabilidade ao responsável pelo tratamento e ao subcontratante, da propriedade do tratamento e dos registos de responsabilidade das relações. Addressed by clauses [4.3.5; 5.1.5; 5.1.7; 7.1.2].

13.2.2 **Clause 5.1** - Mapeada para a aprovação por Top Management, supervisão da responsabilização, revisão anual pela gestão, métricas de responsabilização e ação corretiva para falhas de funções. Addressed by clauses [4.1.1; 4.2.2; 5.1.1; 6.1.1; 8.1.6; 10.1.2; 11.1.3].

13.2.3 **Clause 5.3** - Mapeada para a atribuição, documentação, comunicação e manutenção de funções, responsabilidades e autoridades do PIMS, propriedade dos sistemas, propriedade do tratamento, propriedade das relações com fornecedores, propriedade do escalonamento de incidentes e responsabilidade de revisão independente. Addressed by clauses [4.1.2; 4.1.3; 4.1.4; 4.1.5; 4.1.6; 4.4.2; 4.4.3; 5.1.2; 5.1.3; 5.1.4; 5.1.5; 5.1.6; 5.1.7; 5.1.8; 5.1.9].

13.2.4 **Clause 7.2** - Mapeada para evidência de competência e sensibilização específicas por função para responsabilidades do PIMS atribuídas. Addressed by clauses [7.1.4; 8.1.5].

13.2.5 **Clause 7.3** - Mapeada para a sensibilização para responsabilidades do PIMS atribuídas, evidência de aceitação e reporte anual da sensibilização por função. Addressed by clauses [4.5.1; 4.5.2; 7.1.4; 8.1.5].

13.2.6 **Clause 7.4** - Mapeada para a comunicação de atribuições de funções, alterações de funções, escalonamentos e informação de passagem de funções. Addressed by clauses [4.5.1; 4.5.4; 6.1.5; 7.1.6].

13.2.7 **Clause 7.5** - Mapeada para informação documentada sobre atribuições de funções do PIMS, âmbitos de responsabilidade, níveis de autoridade, retenção anual de evidência e manutenção da matriz de funções. Addressed by clauses [4.1.2; 4.1.3; 4.5.3; 7.1.1; 11.1.4].

13.2.8 **Clause 8.1** - Mapeada para a propriedade dos controlos operacionais relativos a atividades de tratamento, sistemas, fornecedores, subcontratantes, subcontratantes subsequentes, relações de responsabilidade conjunta pelo tratamento e controlos de entrada em produção. Addressed by clauses [4.1.4; 4.1.5; 4.1.6; 7.1.2; 7.1.3; 7.1.5; 10.1.3].

13.2.9 **Clause 9.2** - Mapeada para auditoria independente e revisão de conformidade da evidência de atribuição de funções, evidência de combinação de funções, evidência de independência, constatações e encerramento de ações corretivas. Addressed by clauses [4.2.3; 5.1.9; 6.1.4; 8.1.4; 10.1.4].

13.2.10 **Clause 9.3** - Mapeada para a revisão pela gestão da completude das atribuições de funções do PIMS, conflitos de funções, exceções, métricas de responsabilização e resultados da revisão de responsabilização. Addressed by clauses [5.1.1; 6.1.1; 8.1.6; 11.1.1].

13.2.11 **Clause 10.2** - Mapeada para escalonamento, registo de não conformidades, ação corretiva, encerramento de exceções e verificação de eficácia em questões de responsabilização de funções. Addressed by clauses [4.2.5; 4.4.5; 6.1.5; 9.1.5; 10.1.1; 10.1.2; 10.1.4].

13.2.12 **Annex A.1.2.7** - Mapeada para a atribuição e documentação da responsabilidade contratual de subcontratantes e do escalonamento de responsabilidades de terceiros antes da aprovação ou renovação de contratos. Addressed by clauses [4.1.6; 4.4.4; 5.1.7; 7.1.3].

13.2.13 **Annex A.1.2.8** - Mapeada para a documentação da repartição de responsabilidades entre responsáveis conjuntos pelo tratamento e da evidência de responsabilidade da relação antes do início do tratamento em responsabilidade conjunta. Addressed by clauses [4.3.2; 5.1.7; 7.1.3; 8.1.3].

13.2.14 **Annex A.1.2.9** - Mapeada para a manutenção de registos de responsabilização relativos à propriedade do tratamento pelo responsável pelo tratamento, classificação de papéis e propriedade da evidência. Addressed by clauses [4.3.1; 4.3.5; 4.5.3; 8.1.1].

13.2.15 **Annex A.2.2.2** - Mapeada para a responsabilidade por acordos de cliente do subcontratante, propriedade das instruções do cliente e evidência da relação de subcontratação. Addressed by clauses [4.3.3; 5.1.7; 7.1.3; 8.1.3].

13.2.16 **Annex A.2.2.3** - Mapeada para o alinhamento de finalidades e instruções do subcontratante por meio da propriedade das instruções do cliente e da verificação dos papéis de responsável pelo tratamento/subcontratante. Addressed by clauses [4.3.3; 4.3.5; 5.1.7].

13.3 GDPR

13.3.1 **Article 5(2)** - Mapeado para evidência de responsabilização relativa a atribuições de funções, propriedade do tratamento, revisões de funções, não conformidades e constatações de auditoria. Addressed by clauses [4.5.3; 6.1.2; 8.1.1; 10.1.1].

13.3.2 **Article 24** - Mapeado para a responsabilidade do responsável pelo tratamento, propriedade responsável pelo tratamento, supervisão por Top Management, revisão anual e medidas de responsabilização. Addressed by clauses [4.1.1; 4.3.1; 5.1.1; 6.1.1; 8.1.6].

13.3.3 **Article 26** - Mapeado para a documentação da repartição de responsabilidades entre responsáveis conjuntos pelo tratamento e da evidência de responsabilidade da relação antes do início do tratamento em responsabilidade conjunta. Addressed by clauses [4.3.2; 5.1.7; 7.1.3; 8.1.3].

13.3.4 **Article 28** - Mapeado para a repartição de responsabilidades de subcontratantes e subcontratantes subsequentes, propriedade das instruções do cliente, responsabilidade contratual e vias de escalonamento de terceiros. Addressed by clauses [4.3.3; 4.3.4; 4.4.4; 5.1.7; 7.1.3].

13.3.5 **Article 30** - Mapeado para registos de tratamento, propriedade do tratamento, classificação de papéis do PIMS e verificação dos papéis de responsável pelo tratamento/subcontratante. Addressed by clauses [4.1.4; 4.3.1; 4.3.5; 8.1.1].

13.3.6 **Article 37** - Mapeado para a documentação da função Data Protection Officer / Privacy Advisor quando a designação seja aplicável ou atribuída voluntariamente. Addressed by clauses [4.1.2; 4.1.3; 5.1.3; 11.1.2].

13.3.7 **Article 38** - Mapeado para a posição, independência, envolvimento e gestão de conflitos de interesses de Data Protection Officer / Privacy Advisor quando aplicável. Addressed by clauses [4.2.5; 5.1.3; 6.1.3; 11.1.2].

13.3.8 **Article 39** - Mapeado para aconselhamento de privacidade, observações de monitorização, revisão consultiva e revisão do impacto em privacidade relacionado com funções por Data Protection Officer / Privacy Advisor quando aplicável. Addressed by clauses [4.4.1; 5.1.3; 6.1.3; 11.1.2].

13.4 ISO/IEC 29100:2020

13.4.1 **Clause 4.1; Clause 4.2** - Mapeadas para intervenientes do quadro de privacidade e repartição de papéis para titulares dos dados, responsáveis pelo tratamento de PII, subcontratantes de PII, terceiros e classificação de papéis do PIMS. Addressed by clauses [4.1.4; 4.1.6; 4.3.5; 5.1.5; 5.1.7].

13.4.2 **Clause 5.12** - Mapeada para a responsabilização pelo cumprimento da privacidade, evidência de funções, revisão, constatações de auditoria e verificação de ações corretivas. Addressed by clauses [4.5.3; 6.1.2; 8.1.4; 10.1.4].

13.5 ISO/IEC 29151:2022

13.5.1 **Clause 6.1.2; Clause 6.1.3** - Mapeadas para definição de funções de proteção de PII, documentação de funções, comunicação de funções, coordenação entre segurança e privacidade e segregação de funções para proteção de PII. Addressed by clauses [4.1.1; 4.2.1; 4.2.3; 4.2.4; 4.4.2; 5.1.4; 7.1.4].

13.6 ISO/IEC 27002:2022

13.6.1 Control 5.2 - Mapeado para a definição, repartição, documentação, comunicação e manutenção de responsabilidades do PIMS e de segurança da informação. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.2.1; 4.4.2; 4.5.1; 5.1.4; 7.1.1].

13.6.2 Control 5.3 - Mapeado para segregação de funções, aprovação de combinações de funções, revisão independente, controlos de conflitos e verificação de ações corretivas para conflitos de funções. Addressed by clauses [4.2.2; 4.2.3; 4.2.4; 9.1.2; 10.1.4].