					Insira aqui a designação da entidade jurídica registada							
Número do documento: PII01					Título do documento: **Política do Sistema de Gestão da Informação 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 e determinação do papel no PIMS
ISO/IEC 27701:2025	Clause 4.2	Both	Primary	Partes interessadas e requisitos
ISO/IEC 27701:2025	Clause 4.3	Both	Primary	Âmbito do PIMS
ISO/IEC 27701:2025	Clause 4.4	Both	Primary	Estabelecimento e melhoria do PIMS
ISO/IEC 27701:2025	Clause 5.1	Both	Primary	Liderança e compromisso
ISO/IEC 27701:2025	Clause 5.2	Both	Primary	Política de privacidade
ISO/IEC 27701:2025	Clause 5.3	Both	Primary	Papéis e autoridades
ISO/IEC 27701:2025	Clause 6.1.1	Both	Primary	Riscos e oportunidades
ISO/IEC 27701:2025	Clause 6.1.2	Both	Primary	Avaliação de riscos de privacidade
ISO/IEC 27701:2025	Clause 6.1.3	Both	Primary	Tratamento de riscos de privacidade e SoA
ISO/IEC 27701:2025	Clause 6.2	Both	Primary	Objetivos de privacidade
ISO/IEC 27701:2025	Clause 6.3	Both	Primary	Alterações planeadas do PIMS
ISO/IEC 27701:2025	Clause 7.1	Both	Primary	Recursos
ISO/IEC 27701:2025	Clause 7.2	Both	Primary	Competência
ISO/IEC 27701:2025	Clause 7.3	Both	Primary	Sensibilização
ISO/IEC 27701:2025	Clause 7.4	Both	Primary	Comunicações
ISO/IEC 27701:2025	Clause 7.5	Both	Primary	Informação documentada
ISO/IEC 27701:2025	Clause 8.1	Both	Primary	Planeamento e controlo operacional

ISO/IEC 27701:2025	Clause 8.2	Both	Primary	Avaliação operacional de riscos de privacidade
ISO/IEC 27701:2025	Clause 8.3	Both	Primary	Tratamento operacional de riscos de privacidade
ISO/IEC 27701:2025	Clause 9.1	Both	Primary	Monitorização e avaliação
ISO/IEC 27701:2025	Clause 9.2	Both	Primary	Auditoria interna
ISO/IEC 27701:2025	Clause 9.3	Both	Primary	Revisão pela gestão
ISO/IEC 27701:2025	Clause 10.1	Both	Primary	Melhoria contínua
ISO/IEC 27701:2025	Clause 10.2	Both	Primary	Não conformidade e ação corretiva
ISO/IEC 27701:2025	Annex A.1.2.2; Annex A.1.2.3; Annex A.1.2.6; Annex A.1.2.8; Annex A.1.2.9	Controller	Primary	Registos de governação do responsável pelo tratamento
ISO/IEC 27701:2025	Annex A.2.2.2; Annex A.2.2.3	Processor	Primary	Acordo e finalidades do subcontratante
ISO/IEC 27701:2025	Annex A.3.3	Both	Primary	Ligação à política de segurança de PII
GDPR	Article 5(2)	Controller	Supporting	Evidência de responsabilização
GDPR	Article 24	Controller	Supporting	Medidas e política do responsável pelo tratamento
GDPR	Article 26	Joint Controller	Supporting	Disposições entre responsáveis conjuntos pelo tratamento
GDPR	Article 28	Both	Supporting	Governação de subcontratantes
GDPR	Article 30	Both	Supporting	Registos de tratamento
GDPR	Article 32	Both	Supporting	Segurança do tratamento

GDPR	Article 35	Controller	Supporting	Governação de DPIA
ISO/IEC 29100:2020	Clause 4.7; Clause 5.1; Clause 5.11; Clause 5.12	Both	Supporting	Controlos e princípios de privacidade
ISO/IEC 29134:2020	Clause 1; Clause 5.1; Clause 6.2; Clause 6.3	Both	Supporting	Processo e preparação de PIA
ISO/IEC 29151:2022	Clause 4.1; Clause 4.2; Annex A.2	Controller	Supporting	Programa e política de proteção de PII
ISO/IEC 27557:2022	Clause 4; Clause 5.2; Clause 5.3; Clause 5.4.1	Both	Supporting	Integração organizacional do risco de privacidade

1. Âmbito

1.1 Esta política estabelece o Sistema de Gestão da Informação de Privacidade da organização para o tratamento de PII em contextos de responsável pelo tratamento, responsável conjunto pelo tratamento, subcontratante e subcontratante subsequente.

1.2 Esta política aplica-se aos seguintes elementos:

1.2.1 âmbito, contexto, partes interessadas e limites organizacionais do PIMS;

1.2.2 determinação do papel PIMS para atividades de tratamento de PII;

1.2.3 política de privacidade, objetivos de privacidade, avaliação de riscos de privacidade, tratamento de riscos de privacidade e Declaração de Aplicabilidade do PIMS;

1.2.4 governação, monitorização, auditoria interna, revisão pela gestão, não conformidade, ação corretiva e melhoria contínua do PIMS;

1.2.5 informação documentada e evidência necessárias para demonstrar a conformidade e a responsabilização do PIMS.

1.3 Para efeitos desta política, uma alteração material significa qualquer alteração que afete o âmbito do PIMS, as finalidades do tratamento de PII, as categorias de PII, as categorias de titulares dos dados, os locais de tratamento, a atribuição de papéis de responsável pelo tratamento ou subcontratante, a arquitetura de sistemas, os acordos com fornecedores ou subcontratantes subsequentes, o perfil de risco de privacidade, as obrigações legais ou contratuais aplicáveis, ou o âmbito de certificação.

2. Finalidade

2.1 Esta política define os requisitos obrigatórios de governação para estabelecer, implementar, manter, monitorizar e melhorar continuamente o PIMS.

2.2 A finalidade desta política é assegurar que a organização consegue demonstrar uma gestão responsável, baseada no risco e sustentada por evidência do tratamento de PII em todos os papéis PIMS aplicáveis.

3. Objetivos

3.1 Os objetivos desta política são:

3.1.1 definir o âmbito, o contexto, os limites e a aplicabilidade de papéis do PIMS;

3.1.2 atribuir a responsabilização pela governação do PIMS através de papéis PIMS canónicos;

3.1.3 estabelecer objetivos de privacidade e expectativas mensuráveis de desempenho do PIMS;

3.1.4 manter uma Declaração de Aplicabilidade do PIMS para controlos selecionados e excluídos;

3.1.5 integrar a avaliação de riscos de privacidade, o tratamento de riscos de privacidade e a governação de DPIA na operação do PIMS;

3.1.6 assegurar que as obrigações de responsável pelo tratamento, responsável conjunto pelo tratamento, subcontratante e subcontratante subsequente são identificadas antes do início do tratamento;

3.1.7 manter evidência preparada para auditoria para apoiar a preparação para certificação e a melhoria contínua;

3.1.8 evitar papéis, registos, formulários e controlos operacionais desnecessários ou duplicados.

4. Declarações da política

4.1 Estabelecimento, contexto e âmbito do PIMS

4.1.1 [Both] Top Management DEVE aprovar o âmbito do PIMS em REG01 antes da implementação inicial do PIMS e no prazo de 30 dias após qualquer alteração material.

4.1.2 [Both] Privacy Lead / PIMS Manager DEVE documentar em REG01 as questões externas e internas do contexto de privacidade anualmente e no prazo de 30 dias após qualquer alteração material.

4.1.3 [Both] Privacy Lead / PIMS Manager DEVE documentar em REG01 as partes interessadas relevantes e os respetivos requisitos PIMS anualmente e no prazo de 30 dias após qualquer alteração material.

4.1.4 [Both] Privacy Lead / PIMS Manager DEVE manter o resumo das interações dos processos do PIMS em REG01 antes de cada revisão pela gestão.

4.2 Determinação do papel PIMS

4.2.1 [Both] Process Owner / Business Owner DEVE classificar em REG02 o papel PIMS da organização para cada atividade de tratamento de PII antes do início da atividade de tratamento.

4.2.2 [Joint Controller] Vendor / Procurement Owner DEVE documentar em REG08 a atribuição de responsabilidades entre responsáveis conjuntos pelo tratamento antes do início do tratamento conjunto.

4.2.3 [Processor] Vendor / Procurement Owner DEVE documentar em REG08 as instruções de tratamento do cliente para atividades de subcontratante antes da integração do serviço.

4.2.4 [Subprocessor] Vendor / Procurement Owner DEVE documentar em REG08 as instruções do cliente a montante e os acordos de subcontratação subsequente aprovados antes do início da subcontratação subsequente.

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

9. Exceções

9.1 Pedido e aprovação de exceção

9.1.1 [All] Process Owner / Business Owner DEVE documentar em REG12 qualquer exceção solicitada a esta política antes de ocorrer o desvio.

9.1.2 [Both] Privacy Lead / PIMS Manager DEVE avaliar o risco de privacidade de cada exceção solicitada em REG04 antes da aprovação.

9.1.3 [Both] Top Management DEVE aprovar em REG12 exceções que excedam os limiares aceites de risco de privacidade antes da implementação.

9.1.4 [Both] Privacy Lead / PIMS Manager DEVE rever trimestralmente as exceções PIMS ativas em REG12 até ao encerramento.

9.2 Encerramento de exceções

9.2.1 [All] Process Owner / Business Owner DEVE documentar evidência de encerramento da exceção em REG12 até à data de expiração aprovada da exceção.

9.2.2 [Both] Internal Audit / Compliance Reviewer DEVE verificar a evidência de encerramento de exceções expiradas em REG12 durante a auditoria interna planeada seguinte.

10. Aplicação

10.1 Tratamento de não conformidades

10.1.1 [All] Privacy Lead / PIMS Manager DEVE registar em REG12 suspeitas de não conformidade com esta política no prazo de cinco dias úteis após a identificação.

10.1.2 [All] Process Owner / Business Owner DEVE implementar as ações corretivas aprovadas em REG12 até à data limite atribuída após a aprovação da não conformidade.

10.1.3 [All] Top Management DEVE rever as não conformidades maiores do PIMS não resolvidas em REG12 em cada revisão pela gestão.

10.1.4 [All] Internal Audit / Compliance Reviewer DEVE verificar a eficácia das ações corretivas em REG12 no prazo de 30 dias após o encerramento comunicado.

10.2 Escalonamento

10.2.1 [All] Privacy Lead / PIMS Manager DEVE escalar ações corretivas maiores em atraso para Top Management em REG12 no prazo de cinco dias úteis após a data limite.

10.2.2 [All] Top Management DEVE registar decisões sobre ações corretivas maiores em atraso em REG12 no prazo de 15 dias úteis após o escalonamento.

11. Revisão e manutenção

11.1 Revisão da política

11.1.1 [All] Privacy Lead / PIMS Manager DEVE rever esta política em REG12 anualmente e no prazo de 30 dias após qualquer alteração material legal, organizacional, de tratamento, tecnológica ou do âmbito de certificação.

11.1.2 [All] Data Protection Officer / Privacy Advisor DEVE prestar aconselhamento documentado em REG12 antes da aprovação da política quando houver alteração material das obrigações de privacidade.

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 REG03 no prazo de 15 dias úteis após alterações aprovadas à política que alterem o âmbito do PIMS ou a aplicabilidade dos controlos.

11.1.5 [All] Privacy Lead / PIMS Manager DEVE registar em REG11 a comunicação das alterações aprovadas à política no prazo de 30 dias após a publicação.

12. Políticas relacionadas

12.1 Esta política é apoiada pelas seguintes políticas relacionadas:

12.2 PII02 - Política de Papéis, Responsabilidades e Responsabilização de Privacidade

12.3 PII03 - Política de Inventário do Tratamento de PII e Fundamento de Licitude

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

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

12.6 PII12 - Política de Subcontratantes, Subcontratantes Subsequentes e Partilha de Dados

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

12.8 PII15 - Política de Gestão de Incidentes de PII e Violações de Dados

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

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

12.11 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 apoiam.

13.2 ISO/IEC 27701:2025

13.2.1 **Clause 4.1** - Mapeada para a determinação do contexto organizacional, das questões do contexto de privacidade e da aplicabilidade do papel de responsável pelo tratamento ou subcontratante às atividades do PIMS. Addressed by clauses [4.1.2; 4.2.1; 6.1.3].

13.2.2 **Clause 4.2** - Mapeada para a identificação de partes interessadas, titulares dos dados, clientes, autoridades de controlo, subcontratantes, subcontratantes subsequentes e respetivos requisitos PIMS relevantes. Addressed by clauses [4.1.3; 7.2.1; 11.1.1].

13.2.3 **Clause 4.3** - Mapeada para a definição, aprovação, manutenção e alteração do âmbito documentado do PIMS. Addressed by clauses [4.1.1; 6.1.3; 11.1.4].

13.2.4 **Clause 4.4** - Mapeada para o estabelecimento, implementação, manutenção e melhoria dos processos do PIMS e das respetivas interações. Addressed by clauses [4.1.4; 7.1.1; 7.2.1].

13.2.5 **Clause 5.1** - Mapeada para a aprovação por Top Management, os recursos, a revisão de governação e a liderança sobre a eficácia e melhoria do PIMS. Addressed by clauses [4.3.1; 5.1.1; 6.1.1; 8.1.4; 10.1.3].

13.2.6 **Clause 5.2** - Mapeada para a manutenção desta política de privacidade como informação documentada aprovada e para a comunicação de alterações à política. Addressed by clauses [4.3.1; 11.1.1; 11.1.3; 11.1.5].

13.2.7 **Clause 5.3** - Mapeada para a atribuição e comunicação de papéis, responsabilidades e autoridades do PIMS. Addressed by clauses [5.1.1; 5.1.2; 5.1.3; 5.1.4; 5.1.5; 5.1.6; 5.1.7; 5.1.8; 5.1.9].

13.2.8 **Clause 6.1.1** - Mapeada para o planeamento de ações relativas a riscos e oportunidades do PIMS com base no contexto, nos requisitos das partes interessadas, nos objetivos e nos contributos de melhoria. Addressed by clauses [4.1.2; 4.1.3; 4.4.1; 6.1.1; 8.1.1].

13.2.9 **Clause 6.1.2** - Mapeada para a exigência de avaliação de riscos de privacidade antes de tratamento novo ou materialmente alterado e para a manutenção de evidência do risco de privacidade. Addressed by clauses [4.4.1; 5.1.3; 8.2.4; 9.1.2].

13.2.10 **Clause 6.1.3** - Mapeada para o tratamento de riscos de privacidade, a seleção de controlos, a ligação ao programa de segurança da informação e a manutenção da Declaração de Aplicabilidade. Addressed by clauses [4.3.3; 4.3.4; 4.4.3; 7.1.3; 7.1.4; 8.2.2].

13.2.11 **Clause 6.2** - Mapeada para o estabelecimento, medição, monitorização, comunicação e atualização dos objetivos do PIMS. Addressed by clauses [4.3.1; 4.3.2; 8.1.2; 8.1.4].

13.2.12 **Clause 6.3** - Mapeada para alterações planeadas do PIMS e para o controlo de alterações que afetem âmbito, papéis, controlos e informação documentada. Addressed by clauses [4.1.1; 6.1.3; 7.1.1; 11.1.4].

13.2.13 **Clause 7.1** - Mapeada para a determinação e disponibilização de recursos para o estabelecimento, operação, manutenção e melhoria do PIMS. Addressed by clauses [5.1.1; 6.1.1; 7.1.1].

13.2.14 **Clause 7.2** - Mapeada para as expectativas de competência e a evidência que apoia as responsabilidades do PIMS e o desempenho dos papéis. Addressed by clauses [5.1.3; 5.1.8; 11.1.5].

13.2.15 **Clause 7.3** - Mapeada para a sensibilização relativamente à política de privacidade, ao contributo para a eficácia do PIMS e às implicações da não conformidade. Addressed by clauses [11.1.5; 10.1.1; 10.2.1].

13.2.16 **Clause 7.4** - Mapeada para comunicações internas e externas relevantes para a governação do PIMS, alterações à política e escalonamento. Addressed by clauses [6.2.1; 10.2.1; 11.1.5].

13.2.17 **Clause 7.5** - Mapeada para a criação, manutenção, controlo, preparação da evidência e retenção de informação documentada. Addressed by clauses [4.5.1; 4.5.3; 7.1.6; 11.1.4].

13.2.18 **Clause 8.1** - Mapeada para o planeamento, implementação e controlo dos processos operacionais do PIMS e dos processos prestados externamente. Addressed by clauses [4.4.4; 7.1.3; 7.1.5; 7.2.1].

13.2.19 **Clause 8.2** - Mapeada para a realização de avaliações de riscos de privacidade em intervalos planeados e quando sejam propostas ou ocorram alterações significativas. Addressed by clauses [4.4.1; 8.2.4; 9.1.2].

13.2.20 **Clause 8.3** - Mapeada para a implementação de planos de tratamento de riscos de privacidade e a retenção de evidência dos resultados do tratamento. Addressed by clauses [4.4.3; 7.1.3; 8.2.2].

13.2.21 **Clause 9.1** - Mapeada para monitorização, medição, análise, avaliação, métricas e reporte da eficácia do PIMS. Addressed by clauses [8.1.1; 8.1.2; 8.1.4; 8.2.1; 8.2.2; 8.2.3; 8.2.4].

13.2.22 **Clause 9.2** - Mapeada para o planeamento de auditorias internas, amostragem de evidência, resultados de auditoria e revisão independente. Addressed by clauses [5.1.9; 6.2.1; 8.1.3; 9.2.2].

13.2.23 **Clause 9.3** - Mapeada para contributos da revisão pela gestão, revisão do desempenho, resultados da revisão pela gestão e decisões de melhoria. Addressed by clauses [6.1.1; 6.1.2; 8.1.4; 10.1.3].

13.2.24 **Clause 10.1** - Mapeada para a melhoria contínua por meio de revisão pela gestão, métricas, acompanhamento de ações corretivas e manutenção da política. Addressed by clauses [6.1.1; 6.2.2; 10.1.4; 11.1.1].

13.2.25 **Clause 10.2** - Mapeada para o tratamento de não conformidades, ação corretiva, escalonamento, encerramento e verificação da eficácia. Addressed by clauses [4.5.2; 6.2.2; 6.2.3; 10.1.1; 10.1.2; 10.1.4; 10.2.1; 10.2.2].

13.2.26 **Annex A.1.2.2; Annex A.1.2.3; Annex A.1.2.6; Annex A.1.2.8; Annex A.1.2.9** - Mapeada para registos de finalidades de tratamento do lado do responsável pelo tratamento, ligação ao fundamento de licitude, determinação da necessidade de DPIA, atribuição de responsabilidades entre responsáveis conjuntos pelo tratamento e registos de evidência do tratamento. Addressed by clauses [4.2.1; 4.2.2; 4.4.2; 4.5.1; 7.1.2; 8.2.1].

13.2.27 **Annex A.2.2.2; Annex A.2.2.3** - Mapeada para acordos de clientes com subcontratantes, instruções documentadas do cliente e limitações de finalidade do subcontratante. Addressed by clauses [4.2.3; 4.2.4; 5.1.7; 7.1.5].

13.2.28 **Annex A.3.3** - Mapeada para a ligação à política de segurança de PII, a propriedade da linha de base dos controlos de segurança de PII e o estado dos controlos de segurança da informação na Declaração de Aplicabilidade do PIMS. Addressed by clauses [4.3.4; 5.1.4; 7.1.4].

13.3 GDPR

13.3.1 **Article 5(2)** - Mapeada para evidência de responsabilização, aprovação da política, classificação do papel de tratamento, aplicabilidade de controlos, monitorização, auditoria e registos de ações corretivas. Addressed by clauses [4.3.1; 4.5.1; 4.5.2; 6.1.1; 8.1.3].

13.3.2 **Article 24** - Mapeada para medidas de governação do responsável pelo tratamento, aprovação da política, objetivos do PIMS, revisão da eficácia e evidência documentada da responsabilização do responsável pelo tratamento. Addressed by clauses [4.3.1; 4.3.2; 6.1.1; 8.1.4; 11.1.1].

13.3.3 **Article 26** - Mapeada para a determinação e documentação da atribuição de responsabilidades entre responsáveis conjuntos pelo tratamento antes do início do tratamento conjunto. Addressed by clauses [4.2.2; 5.1.7; 7.1.5].

13.3.4 **Article 28** - Mapeada para registos de governação de subcontratantes e subcontratantes subsequentes, instruções de tratamento do cliente e controlo de processos prestados externamente. Addressed by clauses [4.2.3; 4.2.4; 5.1.7; 7.1.5].

13.3.5 **Article 30** - Mapeada para registos das atividades de tratamento, classificação do papel, registos de responsabilização do tratamento e evidência retida para auditabilidade. Addressed by clauses [4.2.1; 5.1.5; 7.1.2; 8.2.1].

13.3.6 **Article 32** - Mapeada para governação da linha de base de segurança de PII, propriedade dos controlos de segurança, estado de implementação da segurança e confirmação de controlos operacionais. Addressed by clauses [4.3.4; 4.4.4; 5.1.4; 7.1.4].

13.3.7 **Article 35** - Mapeada para a determinação da necessidade de DPIA e para a avaliação de riscos de privacidade antes de prosseguir tratamento enquanto responsável pelo tratamento de alto risco ou materialmente alterado. Addressed by clauses [4.4.1; 4.4.2; 5.1.3; 8.2.4].

13.4 ISO/IEC 29100:2020

13.4.1 **Clause 4.7; Clause 5.1; Clause 5.11; Clause 5.12** - Mapeada para a identificação de controlos de privacidade, princípios de privacidade, segurança da informação, conformidade de privacidade, auditoria, evidência e governação de privacidade baseada no risco. Addressed by clauses [4.3.3; 4.3.4; 4.4.1; 4.5.1; 8.1.3; 10.1.4].

13.5 ISO/IEC 29134:2020

13.5.1 **Clause 1; Clause 5.1; Clause 6.2; Clause 6.3** - Mapeada para governação de PIA, determinação de fatores desencadeadores de DPIA, preparação de PIA, critérios de risco de privacidade e evidência documentada de avaliação de riscos de privacidade. Addressed by clauses [4.4.1; 4.4.2; 5.1.3; 8.2.4; 9.1.2].

13.6 ISO/IEC 29151:2022

13.6.1 **Clause 4.1; Clause 4.2; Annex A.2** - Mapeada para requisitos do programa de proteção de PII, identificação de requisitos de proteção de PII, seleção de controlos baseada no risco de privacidade e orientação da política de proteção de PII. Addressed by clauses [4.3.3; 4.3.4; 4.4.3; 7.1.4].

13.7 ISO/IEC 27557:2022

13.7.1 **Clause 4; Clause 5.2; Clause 5.3; Clause 5.4.1** - Mapeada para princípios organizacionais de risco de privacidade, compromisso da liderança, integração do risco de privacidade na governação do PIMS e compreensão do papel da organização no tratamento de PII. Addressed by clauses [4.1.2; 4.2.1; 4.4.1; 4.4.3; 6.1.1].