					Insira aqui a designação da entidade jurídica registada							
Número do documento: PII18					Título do documento: **Política de Monitorização, Auditoria e Melhoria do PIMS**							
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 6.2	Both	Supporting	Medição dos objetivos de privacidade
ISO/IEC 27701:2025	Clause 7.5	Both	Primary	Informação documentada de monitorização, auditoria e melhoria
ISO/IEC 27701:2025	Clause 8.1	Both	Supporting	Monitorização do planeamento e controlo operacional
ISO/IEC 27701:2025	Clause 9.1	Both	Primary	Monitorização, medição, análise 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.1.2.9	Controller	Supporting	Registos de tratamento do responsável pelo tratamento utilizados para auditoria
ISO/IEC 27701:2025	Annex A.2.2.2	Processor	Supporting	Evidência de acordo com subcontratante e cooperação em auditoria
GDPR	Article 5(2)	Controller	Supporting	Evidência de responsabilização
GDPR	Article 24	Controller	Supporting	Medidas do responsável pelo tratamento e revisão da eficácia
GDPR	Article 28	Both	Supporting	Governação de auditoria e

				cooperação com subcontratantes
GDPR	Article 30	Both	Supporting	Registos de tratamento utilizados para auditoria
GDPR	Article 32	Both	Supporting	Testes e avaliação de medidas de segurança
GDPR	Article 39	Conditional	Supporting	Monitorização pelo EPD e aconselhamento de auditoria, quando aplicável
ISO/IEC 29100:2020	Clause 5.12	Both	Supporting	Cumprimento de privacidade, auditoria e supervisão independente
ISO/IEC 29151:2022	Clause 18.2.2; Clause 18.2.3; Clause 18.2.4	Both	Supporting	Revisão da proteção de PII e verificações de conformidade
ISO/IEC 27001:2022	Clause 9.1	Both	Supporting	Monitorização e avaliação de segurança da informação
ISO/IEC 27001:2022	Clause 9.2	Both	Supporting	Apoio à auditoria interna do ISMS
ISO/IEC 27001:2022	Clause 9.3	Both	Supporting	Apoio à revisão pela gestão do ISMS
ISO/IEC 27001:2022	Clause 10.1	Both	Supporting	Apoio à melhoria contínua do ISMS
ISO/IEC 27001:2022	Clause 10.2	Both	Supporting	Apoio a não conformidades e ações corretivas do ISMS
ISO/IEC 27002:2022	Control 5.35	Both	Supporting	Revisão independente da segurança da informação
ISO/IEC 27002:2022	Control 5.36	Both	Supporting	Revisão da conformidade de políticas e normas

ISO 19011:2018	Clause 4; Clause 5; Clause 6; Clause 7	Both	Supporting	Princípios, programa, condução e competência de auditoria de sistemas de gestão

1. Âmbito

1.1 Esta política define os requisitos da organização para monitorização, medição, análise, avaliação, auditoria interna, revisão pela gestão, tratamento de não conformidades, ações corretivas e melhoria contínua do PIMS.

1.2 Esta política aplica-se ao seguinte:

1.2.1 todos os processos, controlos, políticas, registos, objetos de evidência, sistemas, fornecedores, subcontratantes, subcontratantes subsequentes e acordos de partilha de dados no âmbito do PIMS;

1.2.2 os contextos da organização como responsável pelo tratamento, responsável conjunto pelo tratamento, subcontratante e subcontratante subsequente;

1.2.3 a monitorização consolidada do desempenho do PIMS, dos objetivos de privacidade, do estado de implementação dos controlos, das constatações de auditoria, das não conformidades, das ações corretivas, das ações de revisão pela gestão e das ações de melhoria;

1.2.4 a evidência retida em REG12 e a evidência de origem de suporte retida em REG01 a REG11.

1.3 Esta política não substitui os requisitos de monitorização operacional definidos noutras políticas do PIMS. Estabelece o ciclo consolidado de avaliação de desempenho, auditoria, revisão e melhoria do PIMS.

1.4 Para efeitos desta política, uma não conformidade maior do PIMS significa uma falha que afete materialmente o âmbito do PIMS, os objetivos de privacidade, a responsabilização pelo tratamento de PII, o tratamento de riscos de privacidade, os direitos dos titulares dos dados, a segurança do tratamento, a governação de subcontratantes ou subcontratantes subsequentes, a preparação para violações, a integridade da evidência documentada, o âmbito da certificação ou a repetição da falha do mesmo requisito num período de 12 meses.

1.5 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 funções de responsável pelo tratamento ou de subcontratante, a arquitetura do sistema, os acordos com fornecedores ou subcontratantes subsequentes, o perfil de risco de privacidade, as obrigações legais ou contratuais aplicáveis, o âmbito da auditoria, o método de monitorização ou o âmbito da certificação.

2. Finalidade

2.1 A finalidade desta política é assegurar que a organização avalia o desempenho do PIMS, verifica a conformidade do PIMS, identifica não conformidades, corrige fragilidades de controlo e melhora continuamente o PIMS com base em evidência objetiva.

2.2 Esta política permite à organização demonstrar que as atividades de monitorização, auditoria, revisão pela gestão e melhoria do PIMS são planeadas, independentes quando exigido, baseadas em evidência, tempestivas e rastreáveis a funções responsáveis e a objetos de evidência canónicos.

3. Objetivos

3.1 Os objetivos desta política são:

3.1.1 definir um processo consolidado de monitorização e medição do PIMS;

3.1.2 assegurar que os objetivos de privacidade e o desempenho dos controlos do PIMS são medidos com base em evidência documentada;

3.1.3 estabelecer um programa de auditoria interna do PIMS baseado no risco;

3.1.4 preservar a independência e a objetividade nas atividades de auditoria do PIMS;

3.1.5 assegurar que a revisão pela gestão recebe contributos completos e atuais sobre o desempenho do PIMS;

3.1.6 assegurar que as não conformidades são registadas, avaliadas, corrigidas e verificadas;

3.1.7 assegurar que as ações corretivas são acompanhadas até ao encerramento e revistas quanto à eficácia;

3.1.8 identificar fragilidades recorrentes e oportunidades de melhoria;

3.1.9 apoiar a preparação para certificação e a gestão responsável de evidência;

3.1.10 evitar a duplicação de métricas operacionais já definidas em políticas relacionadas do PIMS.

4. Declarações da política

4.1 Quadro de monitorização e medição do PIMS

4.1.1 [Both] The Privacy Lead / PIMS Manager MUST definir o programa consolidado de monitorização do PIMS em REG12 antes da operação inicial do PIMS e, posteriormente, anualmente.

4.1.2 [Both] The Privacy Lead / PIMS Manager MUST definir o método de medição, a frequência, a fonte de evidência, a meta e a função responsável por cada métrica do PIMS em REG12 antes do início do ciclo de medição.

4.1.3 [Both] The Process Owner / Business Owner MUST fornecer trimestralmente ao Privacy Lead / PIMS Manager contributos de monitorização das atividades de tratamento de PII provenientes de REG02.

4.1.4 [Both] The Information Security Lead MUST fornecer trimestralmente ao Privacy Lead / PIMS Manager contributos sobre o estado dos controlos de segurança de PII provenientes de REG03.

4.1.5 [Both] The Vendor / Procurement Owner MUST fornecer trimestralmente ao Privacy Lead / PIMS Manager contributos sobre o estado de garantia de subcontratantes, subcontratantes subsequentes, partilha com terceiros e fornecedores provenientes de REG08.

4.1.6 [All] The Incident Response Coordinator MUST fornecer mensalmente ao Privacy Lead / PIMS Manager contributos sobre tendências de incidentes de privacidade e violações provenientes de REG10, bem como no prazo de 10 dias úteis após o encerramento de um incidente maior.

4.1.7 [Both] The Privacy Lead / PIMS Manager MUST consolidar trimestralmente os resultados de monitorização do PIMS em REG12.

4.2 Programa de auditoria interna do PIMS

4.2.1 [All] The Internal Audit / Compliance Reviewer MUST preparar anualmente em REG12 um programa de auditoria interna do PIMS baseado no risco antes do primeiro ciclo de auditoria do PIMS planeado.

4.2.2 [All] The Internal Audit / Compliance Reviewer MUST definir em REG12 o objetivo, os critérios, o âmbito, o método, a base de amostragem e o prazo de reporte de cada auditoria do PIMS antes do início do trabalho de campo da auditoria.

4.2.3 [All] The Internal Audit / Compliance Reviewer MUST registar em REG12 as verificações de independência do auditor e de conflito de interesses antes de cada atribuição de auditoria.

4.2.4 [All] The Privacy Lead / PIMS Manager MUST disponibilizar a informação documentada controlada do PIMS e a evidência de registos solicitadas através de REG12 no prazo de 10 dias úteis após um pedido de auditoria aprovado.

4.2.5 [Both] The Internal Audit / Compliance Reviewer MUST testar o estado de implementação dos controlos aplicáveis do PIMS face a REG03 durante cada auditoria do PIMS.

4.2.6 [Both] The Internal Audit / Compliance Reviewer MUST registar em REG12 a amostra selecionada de evidência de tratamento de PII durante cada auditoria do PIMS.

4.2.7 [All] The Internal Audit / Compliance Reviewer MUST registar os resultados da auditoria do PIMS em REG12 no prazo de 15 dias úteis após a conclusão da auditoria.

4.2.8 [All] The Privacy Lead / PIMS Manager MUST designar em REG12 os responsáveis pelas ações corretivas relativas a constatações de auditoria do PIMS aceites no prazo de 10 dias úteis após a aceitação dos resultados da auditoria.

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

9. Exceções

9.1 Exceções de monitorização, auditoria e melhoria

9.1.1 [All] The Process Owner / Business Owner MUST solicitar em REG12 qualquer exceção a esta política antes de ocorrer o desvio.

9.1.2 [All] The Privacy Lead / PIMS Manager MUST avaliar em REG12 o impacto de cada exceção solicitada na privacidade, certificação, auditoria e ação corretiva no prazo de 10 dias úteis após o pedido.

9.1.3 [All] The Data Protection Officer / Privacy Advisor MUST registar aconselhamento em REG12 antes da aprovação de qualquer exceção que afete obrigações legais, direitos dos titulares dos dados, compromissos de AIPD, obrigações de auditoria de clientes ou tratamento de alto risco.

9.1.4 [All] Top Management MUST aprovar em REG12 as exceções que afetem a conclusão do calendário de auditoria, a revisão pela gestão, não conformidades maiores, o âmbito da certificação ou o tratamento de alto risco antes de a exceção produzir efeitos.

9.1.5 [All] The Privacy Lead / PIMS Manager MUST definir em REG12 uma data de expiração não superior a 90 dias para cada exceção aprovada de monitorização, auditoria ou melhoria.

9.1.6 [All] The Privacy Lead / PIMS Manager MUST encerrar ou reavaliar em REG12 cada exceção de monitorização, auditoria ou melhoria no prazo de cinco dias úteis após a expiração.

10. Aplicação

10.1 Aplicação dos requisitos de monitorização, auditoria e melhoria

10.1.1 [All] The Privacy Lead / PIMS Manager MUST registar em REG12 como não conformidade um ciclo de monitorização não realizado, uma auditoria do PIMS não realizada, uma revisão pela gestão em atraso, evidência de auditoria em falta, uma ação corretiva em atraso ou uma ação de melhoria em atraso no prazo de cinco dias úteis após a identificação.

10.1.2 [All] The Internal Audit / Compliance Reviewer MUST registar em REG12 a severidade das constatações de auditoria antes da emissão do relatório de auditoria.

10.1.3 [All] Top Management MUST exigir em REG12 ação corretiva para cada não conformidade maior do PIMS no prazo de 10 dias úteis após o escalonamento.

10.1.4 [All] The Process Owner / Business Owner MUST impedir a entrada em produção ou a submissão de garantia externa para tratamento de alto risco quando a evidência de ação corretiva exigida esteja em falta em REG12 antes da entrada em produção ou submissão.

10.1.5 [All] The Privacy Lead / PIMS Manager MUST escalar para Top Management em REG12 os incumprimentos recorrentes de prazos de monitorização ou de ação corretiva no prazo de cinco dias úteis após a segunda ocorrência num período de 12 meses.

10.1.6 [All] The Internal Audit / Compliance Reviewer MUST verificar em REG12 o encerramento da ação de aplicação na auditoria seguinte agendada ou no prazo de 60 dias após o encerramento comunicado, consoante o que ocorrer primeiro.

11. Revisão e manutenção

11.1 Revisão e manutenção da política

11.1.1 [All] The Privacy Lead / PIMS Manager MUST rever esta política em REG12 anualmente e no prazo de 30 dias após uma alteração material aos requisitos de monitorização, auditoria, revisão pela gestão, ação corretiva ou certificação do PIMS.

11.1.2 [All] The Internal Audit / Compliance Reviewer MUST rever anualmente em REG12 a eficácia do programa de auditoria do PIMS após a última auditoria agendada para o ano operacional do PIMS.

11.1.3 [All] The Data Protection Officer / Privacy Advisor MUST rever em REG12 as alterações a esta política com significado para a privacidade antes da aprovação.

11.1.4 [All] Top Management MUST aprovar em REG12 as alterações materiais a esta política antes da publicação.

11.1.5 [All] The Privacy Lead / PIMS Manager MUST atualizar REG01 e REG03 no prazo de 15 dias úteis após alterações aprovadas a esta política que alterem o âmbito do PIMS ou a aplicabilidade de controlos.

11.1.6 [All] The Privacy Lead / PIMS Manager MUST registar em REG11 a comunicação das alterações aprovadas a esta política no prazo de 30 dias após a publicação.

12. Políticas relacionadas

12.1 Esta política é suportada pelas seguintes políticas relacionadas:

12.2 PII01 - Política do Sistema de Gestão da Informação de Privacidade

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

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

12.5 PII04 - Política de Aviso de Privacidade e Transparência

12.6 PII05 - Política de Gestão de Consentimento e Preferências

12.7 PII06 - Política de Gestão dos Direitos dos Titulares dos Dados

12.8 PII07 - Política de Avaliação de Riscos de Privacidade e AIPD

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

12.10 PII09 - Política de Recolha, Utilização, Divulgação e Partilha de PII

12.11 PII10 - Política de Retenção, Apagamento e Eliminação de PII

12.12 PII11 - Política de Exatidão e Qualidade de PII

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

12.14 PII13 - Política de Transferência Internacional de PII

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

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

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

12.18 PII17 - Política de Gestão de Informação Documentada e Evidência 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 suporta os requisitos citados e identifica as cláusulas internas que os implementam ou suportam.

13.2 ISO/IEC 27701:2025

13.2.1 **Clause 6.2** - Mapeada para a definição, medição, reporte e revisão dos objetivos do PIMS e das métricas de desempenho do PIMS. Addressed by clauses [4.1.2; 4.3.4; 8.1.1].

13.2.2 **Clause 7.5** - Mapeada para a manutenção de informação documentada relativa a resultados de monitorização, programas de auditoria, resultados de auditoria, evidência de revisão pela gestão, não conformidades, ações corretivas e ações de melhoria. Addressed by clauses [4.1.7; 4.2.4; 4.2.7; 4.3.1; 4.4.1; 7.1.8; 11.1.1].

13.2.3 **Clause 8.1** - Mapeada para a operação do ciclo planeado de monitorização, auditoria, ação corretiva e melhoria do PIMS como parte do controlo operacional do PIMS. Addressed by clauses [4.1.1; 4.2.1; 7.1.1; 7.1.6].

13.2.4 **Clause 9.1** - Mapeada para a definição do que é monitorizado e medido, a consolidação dos resultados de monitorização, a avaliação do desempenho do PIMS e a manutenção de evidência de medição. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.1.4; 4.1.5; 4.1.6; 4.1.7; 8.1.1; 8.1.2; 8.1.4; 8.1.7].

13.2.5 **Clause 9.2** - Mapeada para a manutenção do programa de auditoria interna, planeamento de auditoria, verificações de independência do auditor, amostragem de evidência, resultados de auditoria e seguimento de constatações de auditoria. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.2.5; 4.2.6; 4.2.7; 8.1.3; 10.1.2].

13.2.6 **Clause 9.3** - Mapeada para o planeamento da revisão pela gestão, revisão do desempenho do PIMS, revisão de tendências de auditoria e ações corretivas, aprovação de saídas e decisões de recursos. Addressed by clauses [4.3.1; 4.3.2; 4.3.3; 4.3.4; 4.3.5; 4.3.6; 6.1.7].

13.2.7 **Clause 10.1** - Mapeada para a identificação, aprovação, implementação e acompanhamento de oportunidades de melhoria contínua para a adequação, suficiência e eficácia do PIMS. Addressed by clauses [4.3.7; 4.5.1; 4.5.2; 4.5.3; 4.5.4; 4.5.5; 4.5.6; 7.1.6].

13.2.8 **Clause 10.2** - Mapeada para o registo de não conformidades, análise de causa raiz, planeamento de ações corretivas, implementação de ações corretivas, verificação da eficácia, escalonamento e aplicação. Addressed by clauses [4.2.8; 4.4.1; 4.4.2; 4.4.3; 4.4.4; 4.4.5; 4.4.6; 4.4.7; 4.4.8; 10.1.1; 10.1.3; 10.1.6].

13.2.9 **Annex A.1.2.9** - Mapeada para registos de tratamento do responsável pelo tratamento utilizados como fontes de evidência para monitorização, amostragem de auditoria e métricas de atualidade do inventário de tratamento. Addressed by clauses [4.1.3; 4.2.6; 8.1.7].

13.2.10 **Annex A.2.2.2** - Mapeada para evidência de acordo com subcontratante, auditoria de clientes, resposta de garantia e cooperação do subcontratante acompanhada através de processos de garantia de fornecedores e clientes. Addressed by clauses [4.1.5; 5.1.7; 7.1.5; 8.1.8].

13.3 GDPR

13.3.1 **Article 5(2)** - Mapeado para evidência de responsabilização relativa a monitorização, auditoria, revisão pela gestão, ação corretiva e melhoria contínua. Addressed by clauses [4.1.7; 4.2.7; 4.3.2; 4.4.2; 4.5.1].

13.3.2 **Article 24** - Mapeado para medidas de governação do responsável pelo tratamento, revisão da eficácia, revisão pela gestão, ação corretiva e evidência documentada de melhoria. Addressed by clauses [4.3.4; 4.3.5; 4.3.6; 4.5.2; 10.1.3].

13.3.3 **Article 28** - Mapeado para evidência de subcontratantes, subcontratantes subsequentes, auditorias de clientes, garantia de terceiros e cooperação de fornecedores. Addressed by clauses [4.1.5; 5.1.7; 7.1.5; 8.1.8].

13.3.4 **Article 30** - Mapeado para registos de tratamento utilizados como evidência de monitorização, amostragem de auditoria, completude de objetos de evidência e atualidade do inventário de tratamento. Addressed by clauses [4.1.3; 4.2.6; 8.1.7].

13.3.5 **Article 32** - Mapeado para a monitorização e avaliação do estado dos controlos de segurança de PII, evidência de controlos técnicos e evidência de eficácia relacionada com segurança. Addressed by clauses [4.1.4; 4.2.5; 5.1.4; 7.1.4; 8.1.2].

13.3.6 **Article 39** - Mapeado para aconselhamento de privacidade, observações de monitorização, apoio à auditoria e revisão de tendências de cumprimento em matéria de privacidade pelo Data Protection Officer / Privacy Advisor, quando aplicável. Addressed by clauses [5.1.3; 6.1.6; 9.1.3; 11.1.3].

13.4 ISO/IEC 29100:2020

13.4.1 **Clause 5.12** - Mapeada para verificação do cumprimento de privacidade, auditorias internas ou independentes, controlos internos, mecanismos de supervisão e evidência de avaliação de riscos de privacidade. Addressed by clauses [4.2.1; 4.2.3; 4.2.7; 4.5.1; 6.1.6; 8.1.7].

13.5 ISO/IEC 29151:2022

13.5.1 **Clause 18.2.2; Clause 18.2.3; Clause 18.2.4** - Mapeadas para revisão independente da segurança da informação relacionada com PII, conformidade com políticas e normas, e revisão técnica de conformidade para proteção de PII. Addressed by clauses [4.2.3; 4.2.5; 7.1.4; 8.1.2; 10.1.6].

13.6 ISO/IEC 27001:2022

13.6.1 **Clause 9.1** - Mapeada para contributos de monitorização e avaliação de segurança da informação que suportam a medição do desempenho do PIMS e o estado dos controlos de segurança de PII. Addressed by clauses [4.1.4; 8.1.2].

13.6.2 **Clause 9.2** - Mapeada para apoio de auditoria interna do ISMS ao planeamento de auditorias do PIMS, evidência de auditoria, resultados de auditoria e conclusão do programa de auditoria. Addressed by clauses [4.2.1; 4.2.2; 4.2.7; 8.1.3].

13.6.3 **Clause 9.3** - Mapeada para entradas e saídas da revisão pela gestão relativas à supervisão integrada do desempenho do PIMS e da segurança da informação. Addressed by clauses [4.3.1; 4.3.2; 4.3.5; 4.3.6].

13.6.4 **Clause 10.1** - Mapeada para a melhoria contínua do PIMS e do ambiente de controlo de segurança da informação de suporte. Addressed by clauses [4.5.1; 4.5.2; 4.5.6].

13.6.5 **Clause 10.2** - Mapeada para o tratamento de não conformidades, planeamento de ações corretivas, implementação de ações corretivas e verificação da eficácia. Addressed by clauses [4.4.2; 4.4.4; 4.4.6; 4.4.7; 10.1.1].

13.7 ISO/IEC 27002:2022

13.7.1 Control 5.35 - Mapeado para revisão independente, verificações de independência do auditor, teste de evidência de auditoria e verificação independente da eficácia de ações corretivas. Addressed by clauses [4.2.3; 4.2.5; 4.4.7; 10.1.6].

13.7.2 Control 5.36 - Mapeado para revisão de conformidade do PIMS e das políticas de segurança da informação, estado de implementação dos controlos e evidência de conformidade com normas. Addressed by clauses [4.1.4; 4.2.5; 4.5.3; 8.1.2].

13.8 ISO 19011:2018

13.8.1 **Clause 4; Clause 5; Clause 6; Clause 7** - Mapeadas para princípios de auditoria, gestão do programa de auditoria, condução de auditoria, reporte de auditoria baseado em evidência, seguimento de auditoria e expectativas de competência do auditor para auditorias do PIMS. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.2.6; 4.2.7; 4.4.7; 5.1.9; 11.1.2].